Online Social Networks, Radical Business Transparency and Ethical Climate: A Conceptual Governance Framework

by

Gerry Comninos

submitted in accordance with the requirements for

the degree of

DOCTOR OF BUSINESS LEADERSHIP

at the

SBL

GRADUATE SCHOOL OF
BUSINESS LEADERSHIP

UNISA

SCHOOL OF BUSINESS LEADERSHIP

UNIVERSITY OF SOUTH AFRICA

Supervisor: Prof Angelo Nicolaides

Co-Supervisor: Prof Anton Grobler

DECLARATION

Name: Gerry Comninos

Student number: 79169767

Degree: DOCTOR OF BUSINESS LEADERSHIP

Online Social Networks, Radical Business Transparency and Ethical Climate: A Conceptual Governance Framework

I declare that the above thesis is my own work and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete references.

I further declare that I submitted the thesis to originality checking software and that it falls within the accepted requirements for originality.

I further declare that I have not previously submitted this work, or part of it, for examination at Unisa for another qualification or at any other higher education institution.

23 January 2024

TABLE OF CONTENTS

ABBREVIATIONS

OSN	-	Online Social Network Platform
OSNs	-	Online Social Network Platforms
SNS	-	Social Networking Sites
APA	-	American Psychological Association
ECQ	-	Ethical Climate Questionnaire
OPLIS	-	Online Privacy Literacy Scale
SeBIS	-	Security Behaviour Intentions Scale
RSES	-	Rosenberg Self-Esteem Scale
OSES	-	Online Self-Efficacy Scale
BSMAS	-	Bergen Social Media Addiction Scale
SME	-	Small Medium Enterprise
IT	-	Information Technology
FBM	-	Fogg Behaviour Model

TERMS OF ASSOCIATION

Online awareness – The awareness of various factors that may influence behaviour when engaging with OSNs.

WRITING NUMBERS VERSUS NUMERALS

APA style was followed, where words were used for numbers below ten and numerals for ten and above numbers. Numerals were used for all numbers referencing a chapter section, clause or page number. All numbers reported as a percentage were in numerals.

LIST OF FIGURES

Unless specified, all sources and diagrams are by the author.

LIST OF TABLES

TITLE

“Online Social Networks, Radical Business Transparency and Ethical Climate: A Conceptual Governance Framework.”

ABSTRACT

This research study aims to examine the factors influencing responsible engagement when interacting with online social networks (OSN) to provide the building blocks of a conceptual governance framework addressing the paradigm shift from traditional Corporate Transparency to the notion of Radical Transparency.

The literature review validates measuring levels of responsible OSN engagement by surveying the frequency usage of business-friendly OSN platforms relative to social-based OSN platforms. The research delves into behavioural science, online privacy and ethical climate within the organisation. The literature identified three cases namely; awareness of online behaviour, the competency levels of online privacy literacy, and the work culture and ethical environment. The literature further identified validated survey response scales toward gauging factors influencing responsible levels of OSN engagement specifically; 1.) Online self-awareness accounts for the employee's online self-efficacy and online self-esteem using the Online Self-Efficacy Scale (OSES) and the Rosenberg self-esteem scale (RSES), respectively, 2.) Online privacy literacy accounting for the employee's awareness and competency in evasive action toward privacy and security risk using an adapted version of the online privacy literacy scale (OPLIS), 3.) Online organisational awareness accounts for the perception by the employees of the ethical climate within the organisation using an online adapted ethical climate questionnaire (ECQ). In addition, observable behavioural mediating factors were accounted for using the Security Behavioural Intentions Scale (SeBIS), the Bergen social media addiction scale (BSMAS) and OSN engagement habits. A qualitative study of 29 in-depth executive management interviews was conducted and complemented with a quantitative study of N1=328 respondents from organisations in the financial and health sectors. Of the N1=328 respondents, N2=234 completed the ethical climate questionnaire (ECQ).

The qualitative and quantitative findings show that through frequency usage, OSN usage in the business environment is directed primarily towards business communication with limited social use. In addition, the qualitative and quantitative studies highlight the role of online self-awareness, privacy literacy, and organisational awareness associated with responsible OSN behaviour. However, both studies identify the key influencing factor associated with responsible OSN engagement, that

being positive behavioural intent to exercise online security and privacy and to be vigilant about the perils of OSN addiction.

A governance framework to mitigate exposure against reputational risk while encouraging employees to be online brand ambassadors in both business and private OSN engagement is recommended. Key to such a governance framework is fostering an organisational online ethos and culture by providing training in online privacy through a well-defined set of policies and processes while developing online self-awareness through a code of conduct.

CHAPTER 1 : RESEARCH INTRODUCTION

1.1 RESEARCH INTRODUCTION AND BACKGROUND

Are OSNs redefining the business landscape? To what extent are OSNs transforming business transparency? At what point does the individual's right to freedom of speech threaten the organisation's reputational risk? These are some key questions revolving around the topic to be addressed.

1.1.1 *Defining Online Social Networks*

It would thus be pertinent to define what exactly is meant by the term 'Online Social Network'. The term Online Social Networks can be referred to as social networking sites or social media. The following section will clarify the definition of the term Online Social Networks for the purpose of this study which incorporates the elements from both social networking sites and social media. References in current literature (Heirman *et al.*, 2016; Mwaba, Saini and Abratt, 2017; Koch, Gerber and De Klerk, 2018; Ahani and Nilashi, 2020) refer to the definition by Boyd and Ellison (2007) in the paper that defines Social Network Sites. This seminal article identifies a social network site (SNS) by three key elements, namely, (i) an application that is a web-based user network enabling you as a user to construct a public or semi-public profile of yourself as part of this network, (ii) the ability to connect to other profiles within this network, and (iii) disclosure of a list of your connections to your connected profiles enabling them to interconnect (Boyd and Ellison, 2007).

Obar and Wildman (2015) define social media in general as "Web 2.0" Internet-based applications. Obar and Wildman emphasise user-driven content and interaction as a crucial element of social media in keeping with the Boyd and Ellison characterisation fundamentals. The term online social networks is often used as a more comprehensive definition that encompasses all Web 2.0 applications that facilitate users to create and communicate content by sharing with other users from a user or group profiles (Bouadjenek, Hacid and Bouzeghoub, 2016; Penni, 2017; Soga *et al.*, 2020).

For this research, OSNs is referred to as Web 2.0-based applications that are used on computing devices connected to the Internet, facilitating the connection and interaction of user-generated content by individual users or groups that are represented by user profiles (Adibi and Okocha, 2019; Vagianos and Zafiropoulos, 2021). An OSN is a configuration of connected social human interactions using a mobile or web application (Obar and Wildman, 2015).

The introduction of OSNs, often called social media or Social Networking Sites (SNS), has radically and forever changed how we as humans communicate in the last three decades. The emergence of OSNs has redefined the nature of internal business communication interaction of stakeholders and external communication between organisations, clients, suppliers, and the general public.

This has created a new paradigm in interactive communication that has changed the rules of communication engagement. All communication is now recorded, leaving it exposed, only to be activated by the send button, potentially reaching an array of communities of recipients. These recipients, in turn, can similarly resend or forward this message to other communities, which can proliferate to reach an exponentially growing number of recipients in minutes. This results in what can be defined as radical transparency. This study is paramount to the awareness of the potential reach and the associated unintended potential harm that a single send activation may have caused. This awareness is a critical factor in behaviour towards responsible engagement when using OSNs.

This study aims to identify factors that make the employee aware of the notion of radical transparency and how such factors influence the employees’ propensity to act responsibly when engaging in OSNs.

1.1.2 *Current Use of OSNs*

OSNs have become an integral part of the modern-day culture in communication, whether on a personal, social group or business level. OSNs increasingly represent our personal identity within all our social and business circles and society en masse (Clark, Algoe and Green, 2018; Heidari, Salimi and Mehrvarz, 2020). Following the current trend of OSNs, in future years, any individual, group or organisation that does not have an OSN profile may be deemed to be non-existent and beyond the confines of community social networks (Wang et al., 2016; Gould and Nazarian, 2018; Tan et al., 2018). When considering communication by an individual employee within the organisation, OSNs are a communication medium that can enable them to connect with other users in the following three broad categories, namely:

- Personal social communication.
- Business communication.
- Receiving and broadcasting news and “Going viral”.

1.1.3 *Personal social communication*

On a personal level, users may think of connecting with old friends and sharing photographs and information. Such a connection is predominantly the social sharing of relevant information. On this level, it has more to do with the broadcast of the personal well-being and events associated with oneself, your friends and your family. This type of communication often varies depending on the user’s appetite to share life events and to be viewed across this medium. Some may share accounts of detailed events, such as having partaken in a sporting event (Prado-Gascó et al., 2017) or social activities, such as uploading images of themselves with friends detailing a food dish or a cocktail ordered whilst dining (Mendini, Pizzetti and Peter, 2019). Others may share notable events, such as the birth of a child. Some may share a noteworthy achievement of a family member or friend (Humphreys, 2018). Then some regularly log on to their user profile to share a birthday wish of another or a ‘like’ of an event or opinion announced by a connection. A recent study alludes to how moral emotions expressed using OSNs in a social context lead to moral contagion (Brady *et al.*, 2017).

1.1.4 *Business communication*

As a business tool, OSNs enable a fast, economical and effective way of directly interacting with potentially just under half the world’s population as of 2020 (Tankovska, 2021b). OSN engagement facilitates increased brand awareness, measured through current and potential customers (Quesenberry and Coolsen, 2019). Engagement with OSNs can be a gateway to increased website traffic. Brands and organisations can partner with influencers, enhancing product reputation and boosting sales (Arora et al., 2019; Campbell and Farrell, 2020). The reach of OSNs can assist with reputation management and crisis communication.

The uptake of users on OSNs has forced companies to allocate resources that enhance their social media footprint. For example, in March 2012, AllFacebook.com ranked Coca-Cola as the most popular company on Facebook, with 41 million likes (AllFacebook.com, 2015). In 2021 Samsung, ranked seventh as the most popular brand worldwide in 2020 by Forbes (Swant, 2020), took the number one spot on Facebook with close to 160 million followers. Coca-Cola follows this in second place, with more than 105 million Facebook followers in 2021 (Tankovska, 2021a).

In addition to assessing online consumer popularity, the OSN provides a media platform where a company's employees, business partners, competitors and customers can comment on how and what they buy. These stakeholders can also express their thoughts concerning the company. This is where OSNs become a platform that essentially blends personal communication, business interaction, news feeds and updates.

1.1.5 *Receiving and broadcasting news and "Going viral."*

It is about sharing news and political views by sharing topical articles, images, satire, and videos from a political perspective. According to a 2020 survey of adults by Statista in South Africa, Kenya, Argentina, Chile, Greece and Bulgaria, more than 70% of adults get their local and world news from OSNs. This was evident in the role OSN platforms played in the Fees Must Fall (#FMF) movement in South Africa which was initiated at the University of the Witwatersrand (Wits), going viral spreading rapidly to other universities and colleges throughout South Africa (Daniels, 2016). This is in contrast to the less than 40% of adults in more affluent European countries such as the UK, Germany and France who may use OSNs for local and world news (Watson, 2020). In a Pew Research Centre survey, 86% of Americans use mobile digital devices to get their news from OSNs (Shearer, 2021). The power of this medium has become evident; for example, when a video clip of an incident such as road rage, a physical altercation or a political protest is shared, it may go viral within seconds. "It's gone viral" is a phrase that has now been integrated into our daily vocabulary and has become a key indicator of the success of a news article or advertising campaign (Himelboim and Golan, 2019; Jenkins and Nielsen, 2020). When navigating the social norms and practices within social networks, one realises all too soon that by simply clicking on a 'like' or 'share' symbol on a post, whether it be a photograph, video clip or article, one is participating in the spread of a viral commentary. Within a split second, not only depending on the OSN, your opinion could be broadcast to the entire reach of your extended social network but may also be permanently recorded on the OSN used. The expression of moral emotions on OSNs such as Twitter by influential persons, whether business or political, on threads of a social movement often go quickly viral (Brady *et al.*, 2017). This was evident in the financial sector when the Standard Bank economist Chris Hart was accused of an alleged ‘racist’ tweet which went viral and became a major trending social media topic (BusinessTech, 2016). A tweet by a healthcare professional from Cape Town allegedly advising on breast-feeding went viral creating controversy in the healthcare sector prompting the need for social media guidelines for health practitioners (Noakes, 2017).

1.1.6 *Radical Transparency*

This power of immediate dissemination not only lends itself to transparency but forces its hand to the notion of radical transparency accurately described in the Naked Corporation: How the Age of Transparency Will Revolutionize Business (Tapscott and Ticoll, 2012), where transparency within OSNs is now being redefined as Radical Transparency (Heemsbergen, 2016; Beal and Strauss, 2008; Tapscott and Williams, 2013). For the purpose of this study radical transparency is defined as the transformation from controlled transparency to the self-enabling viral nature of information dissemination facilitated through the open structure of OSNs, where direct messaging can instantaneously be broadcast to a broad audience (Pino and Zafra, 2019). Radical transparency provides greater insight into the ethics and values of an organisation and the conduct of a business relating to its stakeholders, both good and bad. Not only can OSNs help us see how a business positions its products and services, but we can now also see how a company treats its employees, partners and suppliers, customers, competitors and even countries.

The notion of radical transparency has not been formally or scientifically defined but has emerged from blogs and other OSNs (Baraibar, 2013). Radical transparency allows modern organisations to enter into a direct continuing discourse with their customers, employees and other stakeholders through technologies such as OSNs (Pino and Zafra, 2019).

1.1.7 *The Need for an OSN Governance Framework*

An in-depth analysis of the findings of 132 papers from selected information systems journals between 1997 and 2017 discussing and exploring the risks and benefits of OSNs found that only five studies between 2010 and 2016 examined the governance of transparency in public administration and political contexts, warning that policymakers from the organisation are advised to include external stakeholder in the development of an OSN governance framework (Kapoor et al., 2018).

The impact of this social phenomenon necessitates establishing the pitfalls and vulnerabilities to the modern-day organisation through engagement with OSNs. Numerous studies in the form of quantitating and qualitative research that has been undertaken in Germany and Australia have revealed the concern from shareholders and other stakeholders about the control by an organisation of all stakeholders, in particular, employee-customer OSN engagement without any form of validation, guidance or approval from the organisation (Macnamara and Zerfass, 2012). In addition, studies have shown that employees find the terms of service and privacy policies of OSNs overwhelming and too lengthy to bother with (Oeldorf-Hirsch and Obar, 2019). This translates into a loss of control of the organisations' public communication. This has created an immense challenge regarding governance for any organisation trying to regulate and control the engagement across all OSNs (Zerfass, Fink and Linke, 2011). From an African perspective however, a recent empirical study found that the penetration of the OSN platform Facebook is associated with a positive effect on governance dynamics (Asongu and Odhiambo, 2019).

1.1.8 *Ethical Climate*

The ethical behaviour of the stakeholder, particularly the employee, is determined by the organisation's ethical climate (Teresi *et al.*, 2019). The notion of ethical climate was initially introduced by Schneider (1975:474) as an unchanging, psychologically meaningful, and shared perception employees embrace concerning their organisation's ethical procedures and policies (Schneider, 1975). In 1987 Victor and Cullen introduced the term 'ethical climate', which they described as the operational environment in which the employees within the organisation consider acceptable or unacceptable regarding behaviour while in the workplace (Victor and Cullen, 1988).

A culture that provides employees with a physical, moral code in the shape of a code of conduct relates to the types of decisions and behaviours that are considered to be acceptable or not. Failing to adhere to acceptable conduct could be considered to be unethical. Increased awareness of questionable practices in the workplace was further developed with the idea of employee social identity adherence. Companies would deem acceptable behaviour through the notion of additional support and reward for ethically superior behaviour (Guerci et al., 2015; Pagliaro et al., 2018).

1.1.9 *Ethical Climate versus Ethical Culture*

Ethical climate is the shared awareness of what is morally acceptable in the organisation, translating to what constitutes ethical or unethical behaviour (Chouaib and Zaddem, 2013). Ethical culture is the shared awareness of how the organisation's work environment is set or enabled to comply with what constitutes unethical and ethical behaviour (Treviño and Brown, 2004). Whereas ethical climate may be seen as more of what is fundamental to the underlying ethics within the organisation, ethical culture may be seen as ethically technically practical, thus a more pragmatic approach (Kaptein, 2020). This research aims not to debate the nuances of ethical climate versus ethical culture as a construct and refer to ethical climate as a reflection of the organisational awareness of expected conduct for ethically responsible behaviour. Elements of this research will invariably cross the contentious divide between what scholars may define as ethical climate or ethical culture and will, for the purposes of this research, the two terms are used interchangeably.

When evaluating the organisation's ethical climate as a reflection of the organisation's workplace culture concerning business transparency when engaging with OSNs (Capriotti, Zeler and Camilleri, 2021), we need to explore the diversity of work culture and ethics of the different generations in developing a governance framework as a guide to OSN engagement (Hess, 2019).

1.2 THE PROBLEM STATEMENT

The last decade has seen forced a paradigm shift in traditional Corporate Transparency to the emergence of the notion of Radical Transparency through the engagement of online social network platforms (OSNs). This radical departure has left the organisation's communication channels, traditionally controlled by marketing and public relations, now potentially open to every employee's voice with an online social network profile. Irresponsible indifferent or malicious online behaviour, whether it be intended or unintended leave the nature of OSNs open to security and confidentiality breaches that may result in both reputational risk and litigation. This highlights a theoretical gap for the need to explore and identify factors currently being researched such as an online awareness in self-efficacy and self-esteem, in both a personal and organisational capacity, and a lack of familiarity with online privacy (Masur, Teutsch and Dienlin, 2018). This leads to online engagement vulnerable to factors such as a lack of vigilance, indifference and addiction (Zivnuska *et al.*, 2019b; Andreassen, Pallesen and Griffiths, 2017; Osatuyi and Turel, 2018a). This further underlines a gap for the practical need to incorporate factors that influence online behaviour to promote a work culture of responsible engagement, as part of the policies and procedures of a conceptual governance framework as guidance to address the exposure echoed in the literature by the idea of a 'loss of control'.

1.3 THE AIM

The research assesses the levels of loss of control reported in the literature through having determined the levels of responsible behaviour by the stakeholder when engaging with OSNs. The research analyses and assesses the influence of critical factors regarding online self-awareness, online behaviour, online privacy literacy and work culture reflected in the organisation's ethical climate. This assessment acts as a foundation of the key elements considered in the development of a governance framework for responsible OSN engagement within the organisation.

1.4 RESEARCH OBJECTIVES

1.4.1 *Primary Objective*

To research and establish the factors to develop a conceptual governance framework as part of the work culture reflected in the organisation's ethical climate to promotes responsible OSN engagement by employees of an organisation where the protection of consumer data is a critical privacy imperative, to mitigate the perceived loss of control through the notion of radical transparency.

The objectives of the research study would be:

1.4.2 *Theoretical Objectives*

1) To critically review the literature to explore what is understood by the notion of radical transparency relating to OSNs and to identify behavioural factors influencing organisations' responsible and abusive OSN engagement.

1.4.3 *Empirical Objectives*

2) Explore the perceptions of behaviour and adherence to current governance, policies and guidelines of employee OSN engagement in the selected industries through a series of interviews of executive management from selected industries.
3) To gauge the opinions and perceptions of a sample of employees from selected industries towards factors that influence responsible behaviour when engaging in OSNs.
4) To gauge employees' levels of awareness towards psychological and external factors affected by manipulated impulsive behaviour, habits, and OSN addiction on responsible OSN engagement.
5) To gauge the perceived effect of individual employees' online privacy literacy and security intentions on responsible OSN engagement.
6) To gauge the perceived influence of the employees' awareness of the ethical climate within the organisation on responsible OSN engagement.
7) To develop a conceptual governance framework for responsible engagement on OSNs.
8) To provide the groundwork for further research into the factors influencing OSN engagement.
9) To present recommendations that may contribute towards higher levels of responsible engagement within organisations.

1.5 THE RESEARCH QUESTIONS

1.5.1 *Prevailing Question*

What influencing factors when engaging on OSNs, form the foundation in developing a conceptual governance framework, that promotes responsible behaviour reflected in the organisation's ethical climate to mitigate the notion of radical transparency?

1.5.2 *Specific Research Questions*

1) What are factors that have been researched that influence responsible and abusive OSN engagement within the organisation?
2) What are the opinions and perceptions of the executive management in the selected industries on responsible OSN engagement and adherence to current

government policies and procedures?

3) To what degree does each influencing factor identify and promote responsible OSN engagement?
4) To what degree does the level of the individual employee’s online privacy literacy and security intentions influence responsible OSN engagement?
5) To what degree does the level of awareness of psychological and external factors such as purposely manipulated impulsive behaviour by OSN organisations, habits and OSN addiction influence responsible OSN engagement?
6) To what degree does the employee’s awareness of the ethical climate within the organisation influence responsible OSN engagement?
7) How are the factors that influence and promote responsible OSN engagement reflected in the ethical climate of the selected organisations?
8) What recommendations should be made to the organisations for responsible OSN engagement?

1.6 MOTIVATION FOR THE RESEARCH UNDERTAKEN

The researcher has been an information technologist in the financial services and healthcare sectors. Client and transactional information confidentiality and privacy are part of the organisation's foundation as a business concern. As part of the X-Generation, the onset of OSNs raises a severe concern for the researcher regarding reputational risk exposure vulnerable to the fragility of both reckless unintended or intended information dissemination through the irresponsible engagement of OSNs within an organisation. Insight gained in researching these sectors where the need for protecting client and patient privacy and confidentiality is critical should apply to organisations and institutions in any other sectors that need to maintain privacy and confidentiality. This study will often refer to the two selected sectors when referring to the findings. The study is not concerned with the disparate business functions of these sectors. The study is concerned, with the need for privacy and confidentiality of clients and patients as a minimum benchmark (Ferlito and Mametja, 2021). The findings and the development of a conceptual governance framework can be generalised to other appropriate sectors.

1.6.1 *Need for the Study*

The adoption and integration of the radical paradigm shift of the OSN technological platform in our everyday lives may already seem familiar to most of us. However, much of our social and business structure is still based on traditional western social norms and values regarding communication where the use of lean media is still regard as more effective than rich media (Ishii, Lyons and Carr, 2019). Where the use of lean media emulates personal communication that was once restricted within your physical personal social network, it has now expanded to that of broadcast communication, where all communication is interweaved and shared within other disparate social networks and accurately recorded on the world wide web (Friemel and Bixler, 2018). This leaves our traditional habits and norms of communication vulnerable to the scrutiny of any one person connected to the global interconnectivity of OSNs (Carlsson, 2019). This has already led to extensive research on the effect that OSNs have on personal, professional, academic, political, and business and health services communication (Anstey Watkins *et al.*, 2018; Kahne and Bowyer, 2018; Negriff and Valente, 2018; Yu et al., 2020).

From a corporate governance perspective, control of the consequences above, where the immediate and intensive interactive nature of OSNs has created a more complex risk profile, is categorised in academic literature with the use of phrases such as “Loss of control” and “Out of control” (Linke and Zerfass, 2013a; Macnamara *et al.*, 2016; Williams and Hausman, 2017). Control of communication exchange and information dissemination, whether organisational or private, as representation from the employee or any stakeholder shifts from being predominantly controlled by a formal PR function potentially to that of an individual stakeholder engaging with any OSN. This leaves the employee or any organisation stakeholder potentially accountable as a custodian of company information that may be exchanged when engaging on OSNs. Furthermore, the employee is seen as a representative of the organisation whenever they engage in an OSN, whether for organisational or private reasons.

Due to social media’s highly interactive, uncontrollable, complex nature, today’s organisations are continually facing emerging new risks regarding a) the content disseminated both organisational and private, b) transgressing compliance and legal regulations (Uhunoma and Asekhauno, 2021), and c) reputational risk attained by threatening the perception and image of the organisation or institution (Williams and Hausman, 2017; Roy *et al.*, 2020).

Being accountable to the organisation whilst engaging in OSNs necessitates appropriate behaviour regarding controlling the content exchanged and being accountable for the privacy settings on the OSN (Crossler and Bélanger, 2019). The ethical climate of the organisations reflects the behaviour of employees in an organisation. An organisation's ethical climate is upheld by a mutual adoption of morally responsible behaviour between peers that uphold the organisation's ethos and ultimately serve as a control mechanism when engaging in OSNs (Blome and Paulraj, 2013; Chouaib and Zaddem, 2013; Pagliaro et al., 2018). Ethical climate, however, reflects work culture and does not account for behavioural traits driven by external influences and interventions beyond the workplace. Factors such as privacy invasion and habit-forming manipulation techniques employed by the organisations that own the OSNs need to be surveyed, observed and explored. Personal and social influences include self-esteem, self-efficacy, and the propensity toward habit-forming addictions. Knowledge and awareness of these factors, particularly understanding the importance of protecting oneself regarding privacy settings, are key to responsible engagement on OSNs. Extensive research of the literature on how OSN organisations use behavioural science for their monetary benefit and the effect that self-knowledge, self-concept and self-awareness play in OSN engagement needs to be conducted to understand how to drive a work culture that guides the employee toward responsible behaviour.

The shift to online representation of the organisational image through either formal or casual engagement on OSNs depends on the responsible usage of OSNs. There is thus a need to explore the dependency of the responsible use of OSN engagement by each employee or stakeholder associated with the organisation, which is what this study undertakes. The interactive nature of OSN communication between primary stakeholders (employees) and secondary stakeholders (customers or suppliers) should prompt this study to consider all stakeholders, whether they be primary or secondary. The key focus of this study is the primary stakeholder as a direct representative of the organisation whose perceptions and behaviour are assessed. Crucial to such exploration are employees' perceptions of the use of OSNs and the actual use and habits when engaging in OSNs (Nyangeni, Du Rand and Van Rooyen, 2015). This dependency on responsible OSN engagement needs to be addressed as part of the organisation's governance framework (Sievert and Scholz, 2017; Helberger, Pierson and Poell, 2018).

1.6.2 *Scholarly contribution*

This study explores the possible factors that influence and are associated with the behavioural traits of OSN engagement, both in the work environment and private life. The study identifies these factors in terms of constructs that can be observed using validated scales that, if needed, can be adapted. This study gauges the identified factors influencing behaviour towards responsible OSN engagement. The qualitative and quantitative findings show that OSN usage in the business environment is directed primarily towards business communication with limited social use. The research revealed the importance that higher levels of online self-awareness, online privacy literacy, and online organisational awareness are associated responsible OSN behaviour.

The study contributes by identifying the key factor influencing associated with responsible OSN engagement, that being positive behavioural intent to exercise online security and privacy and to be vigilant about the perils of OSN addiction.

In light of the findings, the study recommends a governance framework to encourage responsible behavioural intent when engaging with others on OSN platforms. The framework should include an awareness and training programme promoting an online ethos and culture, online self-awareness and online privacy and security competency. The organisations selected for this study adhere to the benchmark of professional standards and norms concerning business transparency, privacy and confidentiality.

1.7 THESIS CHAPTER OUTLINE

1.7.1 *Chapter 1 Research Introduction*

This chapter introduces research that was done. Defining OSNs and the use thereof is introduced. This is followed by introducing two key concepts in OSN engagement: business and radical transparency and OSN governance and associated legal framework. Key to this chapter is the problem statement research questions with the aims and objectives. The researcher presents an outline of the research and research methodology conducted to address the problem statement, research questions, aims and objectives.

1.7.2 *Chapter 2: Literature Review*

The literature review explores the business concepts in the research question, namely, radical transparency and governance and ethical climate in the context of OSNs in detail. In addition, the literature review examines key factors that influence the behaviour of OSN engagement, namely:

- the generation the user has been born into,
- behavioural science and the psychological vulnerabilities of the user,
- measures to ensure communication privacy and trust when engaging with OSNs; and
- the user’s awareness of the organisation's ethical climate reflects how to navigate ethical issues resulting in what would be deemed the correct and responsible behaviour whilst engaging on OSNs.

1.7.3 *Chapter 3: Research Methodology*

A mixed research methods approach through both qualitative and quantitative methods (Babbie, Wagner III and Zaino, 2015; Creswell and Creswell, 2018; Saunders, Lewis and Thornhill, 2019) is used to collect both qualitative and quantitative data. A deductive approach to the research is adopted, with prior knowledge and theory underlying the research. The reason for a convergent mixed-methods approach is to gain an integrated, holistic view of OSN engagement within the organisation (Plano Clark, 2019). From a company management's top-down organisational hierarchy perspective, phenomenological qualitative methods are employed to understand the perceptions and experiences. A quantitative research method determines OSN engagement regarding actual usage, behavioural awareness concerning user privacy settings, self-efficacy, and the perceptions of organisational behavioural disposition when engaging with OSNs. A bottom-up approach using all employees, including management, is employed. Finally, a merging analysis will interrelate the quantitative results with the quantitative insights and perspectives in the form of a suggested governance framework.

1.7.3.1 The Selected Industries, Target Population, Sample and Unit of Analysis

The industries selected are the financial and healthcare sectors since the researcher has work experience as an IT specialist and has experience predominantly in the financial and healthcare sectors in South Africa. The researcher intends to use a purposeful convenience sample where the target population is the entire workforce within the selected organisations, comprising approximately 2000 employees. The unit of analysis is the stakeholder that works and is representative of the organisation, from executive management to all employees, including casual or contract workers.

1.7.4 *Chapter 4: Findings*

This chapter discusses the findings from both qualitative and quantitative research. A comprehensive explanation of the methods and software tools used to dissect and evaluate the findings to a meaningful result is presented.

1.7.5 *Chapter 5: Discussion, Conclusion with, Recommendations for Further Research*

This chapter further analyses the meaning, importance, and relevance of the findings in terms of the research objectives and the context of the literature review. This chapter provides a conclusion to the interpretation of the findings culminating in the foundations of a governance framework for responsible OSN engagement. This chapter ends with recommendations for further research.

1.7.6 *Annexures*

An annexure will contain the quantitative research instrument used in this study.

1.7.7 *Ethical Clearance*

Besides being a non-negotiable requirement for university research, the nature and sensitivity of the conducted research in this study make ethical clearance of paramount importance. Therefore, this chapter addresses all possible precautions undertaken to conduct the research ethically while maximizing the value of the contribution while minimizing any possible risk of harm.

CHAPTER 2 : LITERATURE REVIEW

2.1 OVERVIEW

Chapter 1 introduces the subject matter fundamental to this research and defines what is referred to in this research as OSNs and the characteristics of current usage. Key concepts in the title, problem statement and research questions are briefly introduced. The literature attests to subject matter that is not only complex but rapidly evolving daily. Unravelling a social phenomenon's social adoption and technological complexities and redefining how we as humans interact within a couple of decades are bound to be convoluted, navigating through social, psychological, behavioural, technological, and ethical business elements. To assist in navigation, the researcher uses a graphical map to tie up the various elements, see Figure 2.1. In achieving the first research objective, namely, critically reviewing the literature to identify factors that influence responsible and abusive OSN engagement within the organisation, the literature follows three general themes.

Theme one briefly restates the definition of OSNs used in this study and then discusses the current general usage of OSNs. This will then be followed by the specific use of media information through OSNs globally and in South Africa.

Theme two explores the research concepts introduced in chapter one with an in-depth discussion leading to the idea of ethical work culture of responsible engagement.

Theme three investigates the factors that influence OSN engagement. The literature review first looks at the influence of generation and identifies and discusses three key factors influencing responsible engagement. First, the psychological impact and behavioural science lead to the derivation of the construct of online self-awareness as an influencing factor. Second is text and rich media communication privacy and trust leading to the derivation of the construct of online privacy literacy as an influencing factor. The third is the organisation's ethical climate leading to the derivation of the construct of online organisational awareness as an influencing factor.

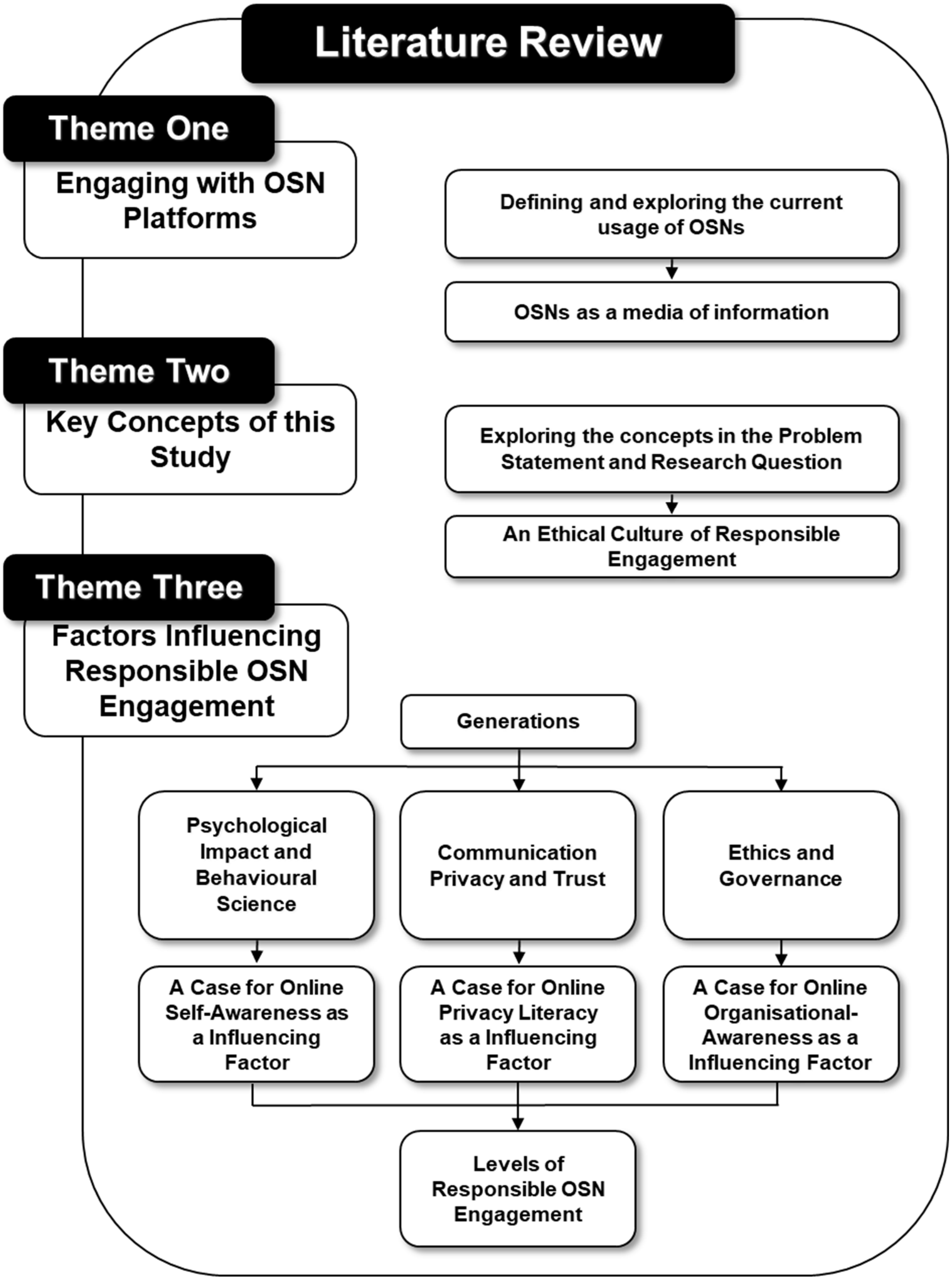

Literature Review
Theme One
Engaging with OSN Platforms
Defining and exploring the current usage of OSNs
OSNs as a media of information
Theme Two
Key Concepts of this Study
Exploring the concepts in the Problem Statement and Research Question
An Ethical Culture of Responsible Engagement
Theme Three
Factors Influencing Responsible OSN Engagement
Generations
Psychological Impact and Behavioural Science
Communication Privacy and Trust
Ethics and Governance
A Case for Online Self-Awareness as a Influencing Factor
A Case for Online Privacy Literacy as a Influencing Factor
A Case for Online Organisational-Awareness as a Influencing Factor
Levels of Responsible OSN Engagement

Figure 2.1 Literature Review Overview

2.2 THEME ONE: ENGAGING WITH OSN PLATFORMS

Engaging with OSNs allows individuals or groups of individuals to communicate in an online community. Conversation are conducted on individual OSN platforms such as Twitter, Facebook, WhatsApp, Instagram, and LinkedIn, or using email. OSN platforms allows businesses to remain in constant contact with the ecosphere of an organisation such as suppliers, distributors, customers, competitors, government agencies, environmental lobbyists and other relevant stakeholders.

2.2.1 *Defining Online Social Networks (OSNs)*

OSNs use the Internet Web 2.0 technology platform to enable connections that can be referred to as "Links" that facilitate the interaction of individuals, both informal and formal groups such as a family, circles of friends, clubs or organisations that can be referred to as "Nodes." These Nodes and Links form social structures called online social networks, where the nodes can stay connected.

As discussed in the introduction, the literature consistently refers to three characteristics defined by Boyd and Ellison (2007) to categorise a social media platform as a Social Networking Site (SNS), namely:

- Being able to define a User Profile.
- Being able to "Friend" or connect to other user profiles.
- Disclosure of your friends or connections to connected user profiles.

In keeping with the Boyd and Ellison characterisation fundamentals, Obar and Wildman (2015) emphasises that user-driven content and interaction is a crucial elements of OSNs when using a mobile or web app for social and business interactions (Soga *et al.*, 2020). The prominent South African and worldwide OSNs with their user sizes are found in Figure 2.2 and Figure 2.4.

2.2.2 *Online Social Network Usage*

For this research, the OSNs selected are based on South African and worldwide OSN usage, as shown in Figure 2.2, Figure 2.3 and Figure 2.4. From a geographical and user perspective, Facebook dominates the globe; see Figure 2.5.

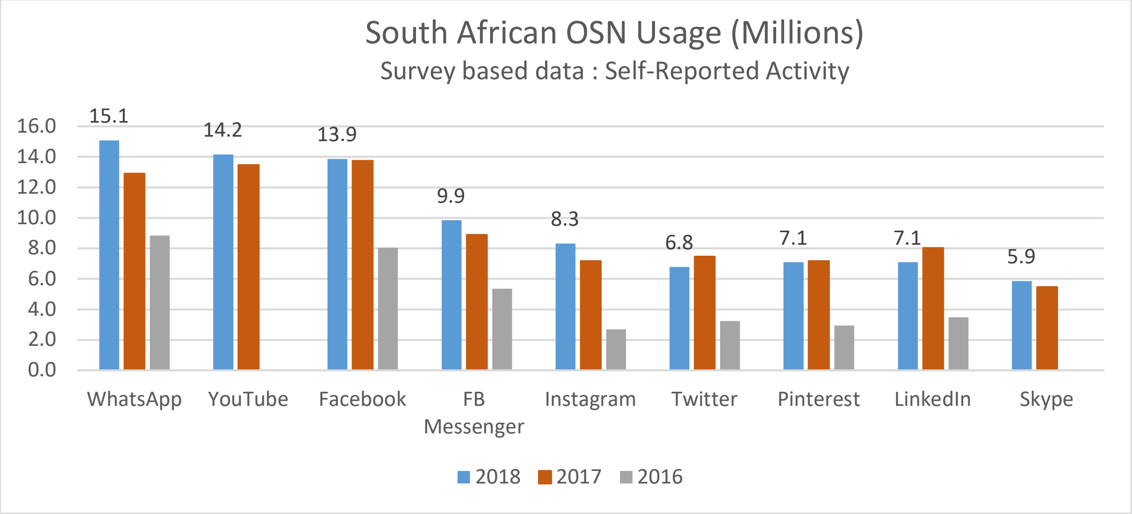


Figure 2.2. Online Social Network Usage in South Africa 2016 – 2018

Figures represent survey-based data of self-reported activity

Source: (We are Social and Hootsuite, 2016; We Are Social and Hootsuite, 2017; We Are Social and Hootsuite., 2018).

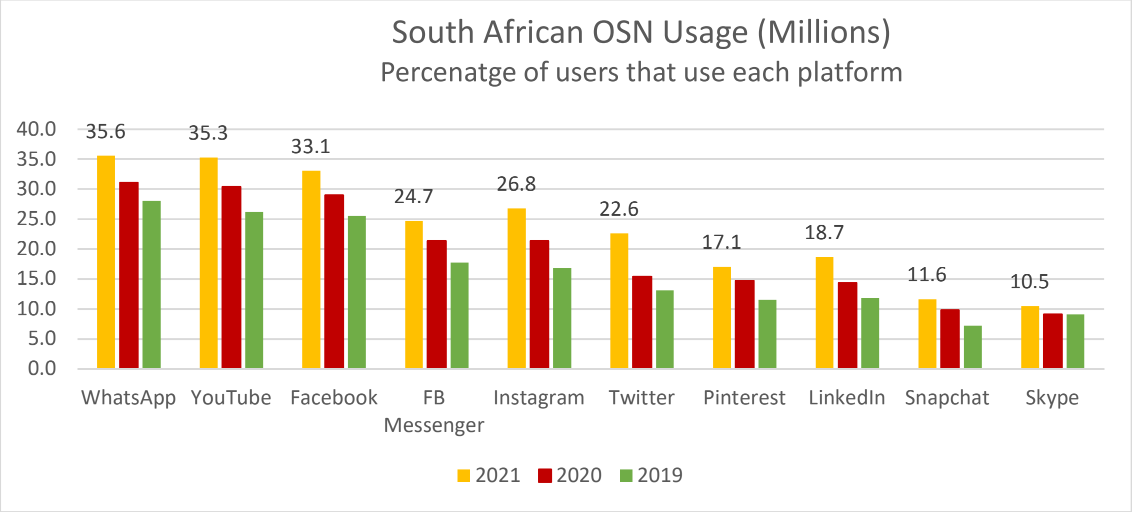


Figure 2.3. Online Social Network Usage in South Africa 2019 – 2021

Figures represent percentage of users that use each platform

Source: (We are Social and Hootsuite, 2019; We Are Social and Hootsuite, 2020; We Are Social and Hootsuite., 2021)

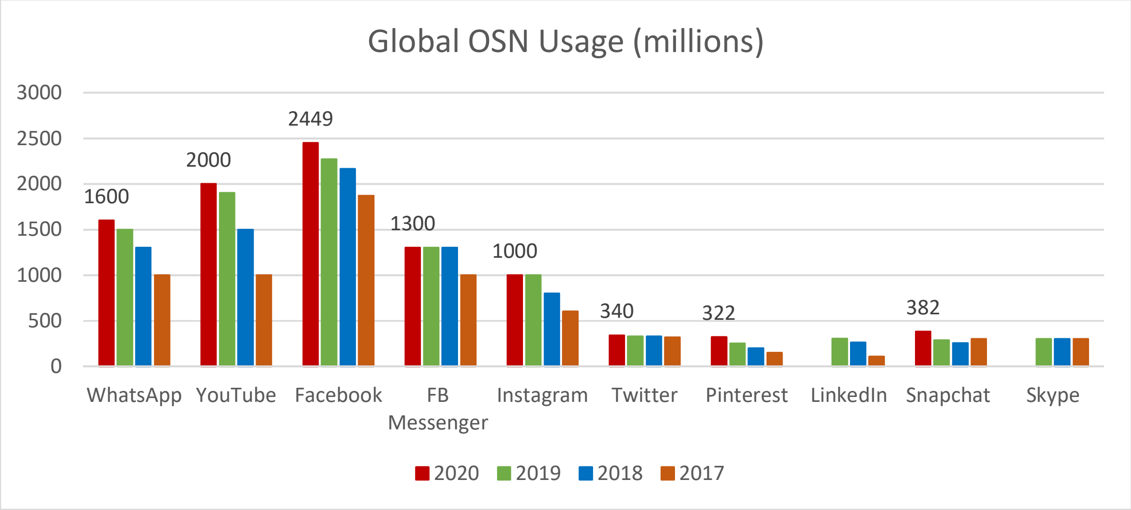


Figure 2.4. Online Social Network Usage World Wide 2017 – 2020.

Source: (We Are Social and Hootsuite, 2017, 2018, 2019, 2020).

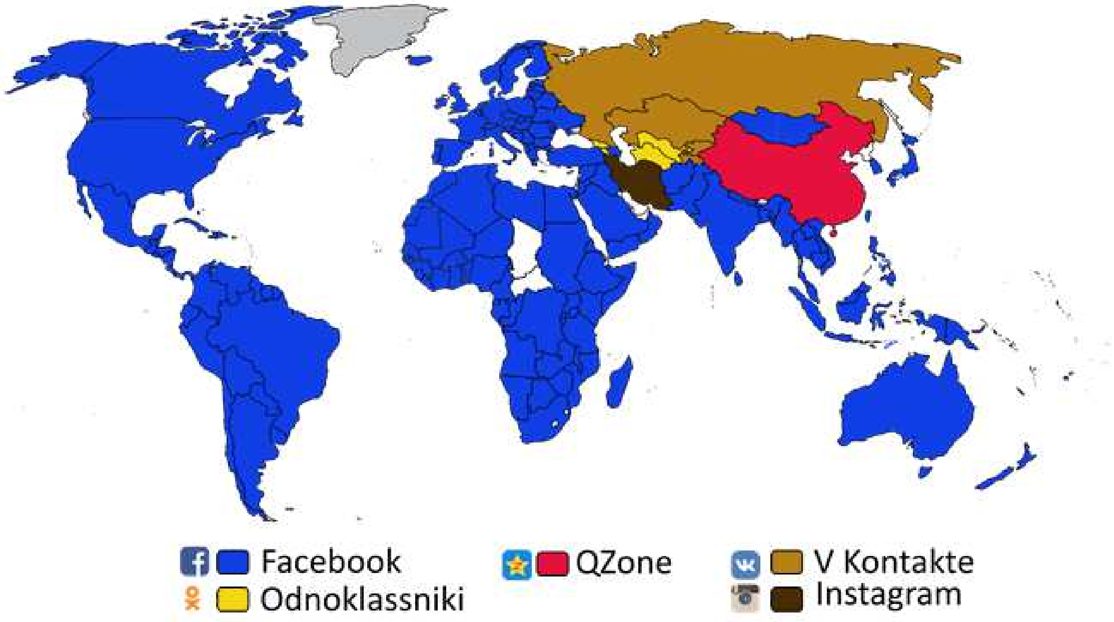


Figure 2.5. World Map of online social networks as of January 2019.

Source: (Cosenza, Alexa and Similarweb.com, 2019).

2.2.3 *OSNs as a Media of Information*

Communication using an OSN can take the form of two types of messages. The first is a private message, equivalent to texting (SMS) or instant messaging (IM) directly from one user to another user, where the content of the message is kept between the message sender and message recipient. This type of communication may be equivalent to direct face-to-face communication between two people or in the form of a private written letter or email between two people (Nguyen *et al.*, 2022).

The second form of the message is a group message or broadcast to a defined group of user profiles or self-declared followers of a user profile. Users of such a group can interact in what is referred to as a group chat. Creating a group of user profiles is a key distinguishing characteristic of an OSN. This type of messaging system differentiates between a peer-to-peer messaging system and a group or forum chat messaging system of an OSN (Kaufmann and Peil, 2020).

The instant real-time Mobile Instant Messaging (mIM) protocol, as a low-cost technological platform, has become a key factor in collaborative and information exchange communication within the organisation, both on an individual and group level, changing the way we exchange information and communicate (Ogara, Koh and Prybutok, 2014; Yuan and Wu, 2020).

Since its introduction in 1992, although surpassed by mIM generating 50 billion messages a day, SMS still generated 21 billion messages a day in 2014 (Deloitte, 2014). In comparison, six years later, in 2020, the following estimates were derived from the various constantly changing sources of commercial statistical data such as Statista, ‘Hootsuite and We Are Social and others. As of October 2020, globally, 79% of employees used a mobile messaging platform such as SMS or mIM to communicate with other employees at least once a week (Kemp, 2020). As of January 2019, 41 million mIM messages were sent per minute, equating to 59 billion per day, an increase of 18% since 2014 (Clement, 2019). Text messaging using the SMS platform was approximately 16 million per minute, equating to 23 billion per day and an increase of 10% since 2014 (Morreale, 2017; Dobrilova, 2020; Domo, 2020). The global distribution of text messaging is illustrated in Figure 2.6.

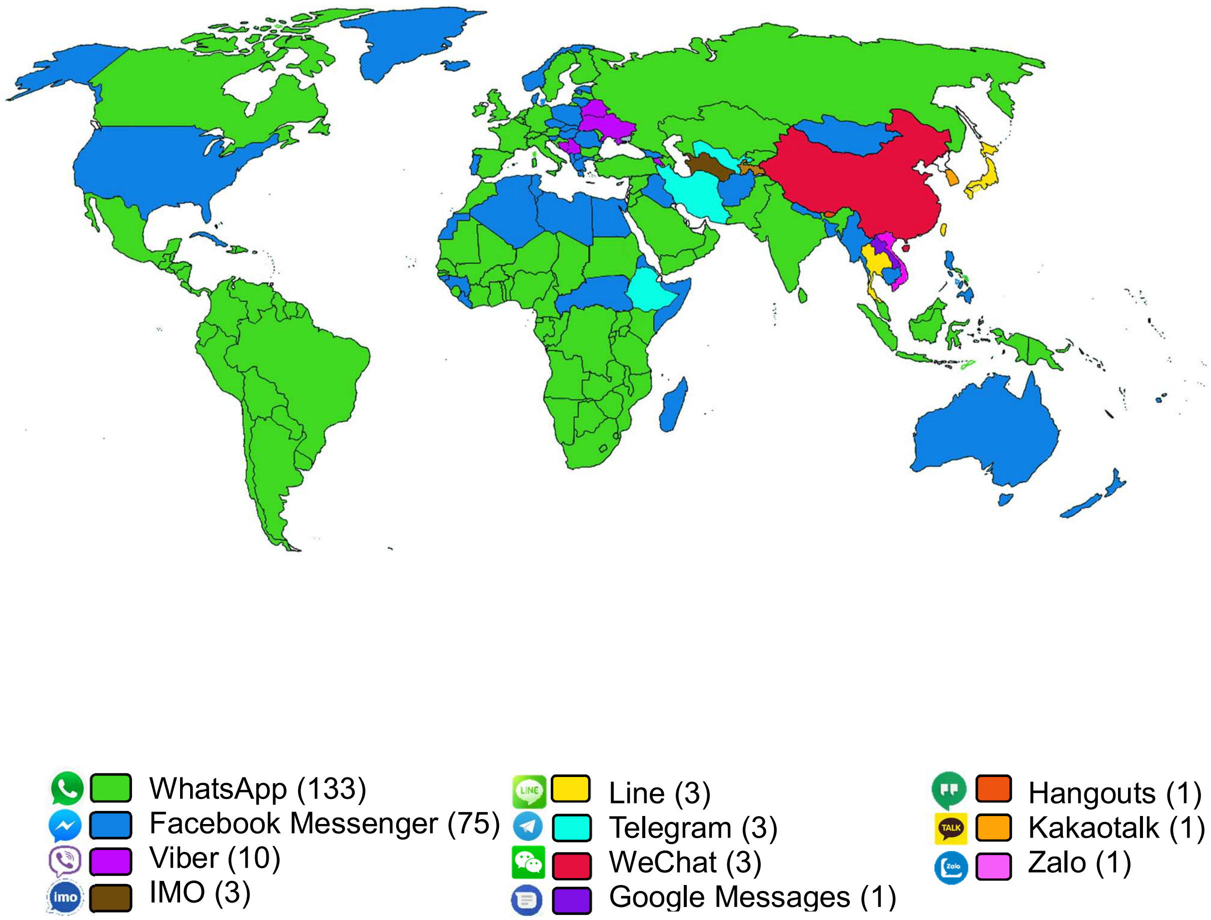


Figure 2.6 Distribution of Messaging OSNs as of January 2019

Note: Numbers in parentheses represent the number of countries/territories messaging app is ranked top.

Source: (C. Smith, 2019; Clement, 2019b; Jessica Clement, 2020a; We Are Social and Hootsuite, 2019).

From a usability perspective, mIM apps merge text messaging and mobile social networks. This can be attributed to the proliferation of smartphones that boast 'Over the Top (OTT) mIM apps that stream media of the Web 2.0 platform, where apps such as Facebook Messenger and WhatsApp are popular in the Western World WeChat in China, see Figure 2.6. As of August 2020, there are close to 42 million messages shared by WhatsApp users alone (Clement, 2020). These OTT messaging apps, particularly WhatsApp, Facebook-Messenger, WeChat and Line, carry the key features of an OSN as defined by Boyd and Ellison (2007).

Within the context of the defined criteria in this research, WhatsApp falls into the category of an OSN. Whether it be classified as messaging media or social media, or an OSN, WhatsApp is becoming the prominent mIM app used for messaging text and exchanging social multimedia content and has been seen to be increasing work performance through the exchange of information, planning and coordination throughout the world (Fiadino et al., 2015; Terkan and Celebi, 2020)

2.3 THEME TWO: KEY CONCEPTS OF THIS STUDY

The research question concerns three key business management concepts regarding behavioural intentions toward responsible OSN engagement. These are the management of responsible OSN engagement through appropriate governance and the organisation's legal framework to help eliminate the threat of the notion of radical transparency when practising business transparency. A brief introduction of each concept follows.

2.3.1 *Radical Transparency*

Business transparency is a key foundation of business ethics (Shum et al., 2019) and prevents corrupt behaviour (Bertot, Jaeger and Grimes, 2012). As defined in the introduction, the transformation to radical transparency is associated with transforming the self-enabling viral nature of information dissemination (Pino and Zafra, 2019). The facility of OSNs that enables immediate direct messaging that can instantly be transformed into broadcast messaging makes further business analysis and radical transparency relevant to this study.

2.3.2 *OSN Governance and Legal Framework*

On the 1st of June 2021, the President of the Republic of South Africa signed the Cybercrimes Act 1 into law. This act addresses cybercrimes, such as the unauthorized access of data, cyber extortion, password hacking and cyber fraud as a violation punishable by fine or imprisonment or both (Snail ka Mtuze and Musoni, 2023). In addition, user-generated online content is regulated by the amended Films and Publications Act (Ongeso, 2022). The legal perspective is further divided into the rights of the individual's (employee's) rights to privacy and freedom of speech and the rights and interests of the organisation (employer). A well-structured policy regarding engagement with OSNs is now a must for all employers. From governance and legal perspective, OSNs have advanced rapidly when it comes to terms and conditions of use and prohibitions; however, there is still a large amount of uncertainty as to how the courts will rule in many cases, which is pre-empting companies to put measures and policies in place to mitigate risk (van den Berg and Struwig, 2020). The main legal risks associated with OSNs include defamation, the protection of intellectual property, a breach of privacy and security and other unsolicited media breaches leading to reputational harm. The need and challenge of the governance of OSNs may be best summarised as follows:

> *“Today, regulators and the courts are being asked to address a broad and diverse range of challenges social media pose to law and policy. Privacy, speech rights, intellectual property, antitrust, government surveillance, employer surveillance of employees, protection of children and older minors and consumer protections are prominent among the issues being addressed (Obar and Wildman, 2015).”*

When engaging on an OSN, the user is accountable for any original comment or information published from their user identification, usually defined as their profile (Kaupins and Park, 2011). This accountability is determined by the user’s behaviour when engaging with OSNs, whether intentional or unintentional, responsible or irresponsible (Gray, 2001). The affordances of OSNs toward transparency, openness and accountability necessitate responsible behaviour when engaging with OSNs (Sivarajah, Irani and Weerakkody, 2015; Stamati, Papadopoulos and Anagnostopoulos, 2015). Therefore, guidance accompanying company policies and procedures for responsible behaviour within the organisation requires an analysis of the building blocks of a governance framework for communication paradigm shift in through the use of OSN platforms in South African organisations (van den Berg and Struwig, 2020; Ferlito and Mametja, 2021).

2.3.2.1 Ethics within the communication paradigm shift on OSN platforms

When considering the adoption of an ethical code within the communication paradigm shift on OSN platforms, users can fall prey to adopting and accepting the values and culture of the organisation that owns OSN. All too often, users are happy to accept the suggested default settings of the OSN, playing into the hands of the organisations that own OSNs (Capurro, 2013), giving the organisation permission to interrogate and use the employee’s personal and organisational data. However, the user is accountable for their freedom of choice and ethically to follow the values defined within the user's professional and personal ethical code (Rascão, 2020; Yang, 2020).

The need to maintain stringent ethical codes is embedded within the professional standards defined in both the financial services and healthcare sectors, necessitating an awareness of the potential dangers and pitfalls of engaging with OSNs. Additionally, over time engagement demands repeated risk assessments of current trends, potential security breaches and new features in the continual evolution of OSNs (Morgan, 2011).

2.3.2.2 The Phenomena

OSNs dominate modern-day communication across generations in our personal social circles and business environment. What may initially have seemed a novel platform for communication has become essential in communicating with others. Coupled with this novel communication platform is an invasion of both business and our private lives. The unforeseen impact of the nature of this technological communication platform on our daily lives needs careful scrutiny or as articulated by Danah Boyd, who initially identified the key elements of an OSN or a social networking site:

> *"While these tools are not the first genre of technology designed to enable social interaction, they have been taken up around the globe at an unprecedented speed, revealing the extraordinary nature of the social media phenomenon. For this reason alone, it is imperative to analyze the phenomenon of social media."* (Boyd, 2015).

This unpredictable adoption of technology poses questions, as highlighted by Carroll, Brown and Buchholtz (2018), concerning the social and ethical implications and repercussions of OSNs (Carroll, Brown and Buchholtz, 2018), particularly Facebook and Twitter, MySpace, LinkedIn, Pinterest, etc.

2.3.2.3 Data and Knowledge

"We are drowning in data yet thirsting for knowledge" the futurist John Naisbitt's infamous quote from Megatrends: Ten New Directions Transforming Our Lives (Naisbitt, 1984) is today just as relevant as when it was first published in 1982. Today's technology platforms have enabled data gathering, recording, and classification on a scale never seen before in human history. By 2011 IBM had already claimed that at least 90% of the world’s data had been gathered and recorded (IBM, 2011; Nunan and Di Domenico, 2013). This has led to the notion of “Big Data”, which is the processing and analysis of massive data sets from various systems sources to reveal patterns and associations that enable the development of business strategies and decisions. Big data are distinguished by what was initially known as the three V’s, namely, Volume, Velocity and Variety (Price and van der Walt, 2013; Carroll, 2014) to what is now referred to as the four Vs with the addition of Veracity (Zikopoulos *et al.*, 2015:8).

2.3.2.4 The use of Information Technology (IT) and the Stakeholder

A general premise of this research is for organisations to adhere to a code of business ethics in the information age or the 4IR, in particular, engagement with OSNs. For this research, information technology (IT) is defined as using any electronic-based technology to access, generate, store, and communicate information.

The start of the 21st century saw the rapid development of the use of electronic media in the interaction of social networks on what is now the OSN. Companies spend billions of dollars using social networking to market and sell to potential customers. The pervasive nature of this thriving business opportunity, it can be argued, is driven by technology determinism. Put simply, whatever the ongoing boundaries of technology are, they will continually change as people and society adapt to those boundaries, which will then again be redefined. Rapid advances in technology often have adverse side effects on society. The concept of ‘technology determinism’ is often associated with ‘ethical lag’.

The dominance for the drive of progress fuelled by the profit that renders an absence of foresight during the rapid growth in e-commerce often leaves e-commerce and OSNs vulnerable to what is considered unethical business practices. Practices include online scams, access to private and confidential company and personal information, cyber-bullying, and piracy (Mannhardt, Petersen and Oliveira, 2019; Semantha *et al.*, 2020). This is echoed as reported in the MIT Technology Review in an interview with Edith Ramirez, the chairwoman of the Federal Trade Commission (FTC), as recently as October 2016, saying that “protecting consumer privacy cannot become an afterthought as the technological landscape grows more complex” (Orcutt, 2016a; Berto, 2019; Thilakarathne, 2020).

This highlights the ongoing issues around ethics and e-commerce, namely the economic divide of who has access to the Internet (Orcutt, 2016b; Spooner, 2016; Nyahodza and Higgs, 2017), the protection of intellectual property through illegal downloads, and privacy (UNODC, 2013; Carroll, Brown and Buchholtz, 2018). The access to privacy, mainly personal information, United States of America (US) differs regarding access to adult content versus content for all ages. One of the primary concerns in the US has been adult content and access to the personal information of children within the age group of 13 years and younger, which requires informed consent. Although the Children's Online Privacy Protection Act (Federal Trade Commision, 2013) revised and passed with amendments in 2013 applies to all, it allows companies to apply the use of cookies without consent on personal computers.

A primary concern in this research is business transparency and the invasion of consumer privacy by others (Isaac and Kang, 2019; Angelopoulos *et al.*, 2020; Robertson, 2020). This is a concern in the South African health sector where the need of familiarity with OSNs platform by practitioners is becoming imperative in communication with patients (Grobler and Dhai, 2016; Kubheka, Carter and Mwaura, 2020).

2.3.2.5 Engaging in E-Commerce and Consumer Privacy

Transacting in e-commerce renders the consumer vulnerable to cybercrime manifested in a host of unethical privacy intrusion and exploitation practices. OSNs being vulnerable to cybercrime is key to a governance framework linking use of Information Technology (IT) and the stakeholder and should include precautions against elements such as the collection and gathering of personal information and use thereof without consent and phishing lures in spam mail, ransomware attacks and others discussed in this section. The criminal activities linked to cybercrime range from petty and mischievous scams to cyber espionage (Marinos and Lourenço, 2018) to organized attacks crippling multinationals and governments (UNODC, 2013; Carroll, Brown and Buchholtz, 2018). Not only are such commercial transgressions against the consumer invasive, but once committed, the potential damage may be irrecoverable and leave the consumer susceptible to possible further lethal attack. It is almost impossible to recover or maintain one's personal information as private and confidential once it is electronically transferred to unauthorised hands. The permanent nature of recorded electronic data are that, not only will it be stored and accessible to others for the rest of your life, but it will also outlive you.

The collection and gathering of personal information and use thereof without consent have become a grave violation of privacy (Robertson, 2020). The dangers of invasive techniques such as using cookies to keep track of consumers as repeat customers are not fully understood by users when accepting them for ease of transacting with an e-commerce website (Carroll, Brown and Buchholtz, 2018). Other more invasive methods, such as a barrage of unsolicited emails or text messages in the form of spam, when first emerged and proved to be highly disruptive and exasperating (Orcutt, 2016a).

Using “phishing lures” in spam mail entices the user to click on a web link to infect the unsuspecting user (Acohido, 2010). This infected mobile device or computer can now be used as a bot linking it to a command-and-control server. This compromised computer now takes on the identity of a bot and then becomes part of a network of bots which, with other compromised workstations, is known as a botnet (Acohido and Swartz, 2008). Phishing is not restricted to emails but is flourishing on OSNs such as Facebook and Twitter (Verkijika, 2019). Spam has been developed as a sophisticated malware distribution technology enabling fraudulent activities (Parsons *et al.*, 2019). The distribution of malware as a botnet infrastructure of compromised computers is a key element of what is taken on a “living” form of a malicious self-sustaining cyber-attack organism (OECD, 2008). Attacks are often kept purposefully small to avoid detection.

Recently, there has been a proliferation of ransomware attacks, where a company and personal data are encrypted by the perpetrator and will only be unencrypted for a ransom payment to be paid in cryptocurrency (Novinson, 2019). Having suffered an onslaught of ransomware attacks in 2017, the UK National Health Service was put on alert in the latter part of 2020 for Russian-based ransomware Ryuk (Scroxton, 2020).

The era of being able to identify phishing emails by intentional typos and the lure of being selected to partake in an elaborate financial scheme where a small investment will supposedly return millions, or you suddenly find that you are the recipient of a large inheritance or grant is fading and being replaced with a far more sophisticated form of phishing identified as spearphishing (Allodi *et al.*, 2020). Spearphishing emails are professionally crafted by highly organized and sophisticated criminal syndicates that use both advanced espionage and technological techniques to send an email that appears legitimate to come from a trusted colleague within your organisation (Grimes, 2015).

The collection and use of personal information are considered a severe invasion of privacy by many western-style democracies. Legislation to protect this privacy is continually evolving (Federal Trade Commission, 2019; Georgiadou, De By and Kounadi, 2019; Mcquinn and Castro, 2019). The European Union has made significant advances with the right-to-be-forgotten campaign (Floridi *et al.*, 2015) led by top academic philosophers. These included Luciano Floridi and multinationals like Google, where, through a ruling by the Court of Justice of the European Union (CJEU) in 2014, individuals have a “right to delist” any URL linking web pages with news articles or blogs that may contain irrelevant, inappropriate, harmful, or dated information about them (Kirkwood, 2020).

In August 2016, Microsoft followed Google’s initiative to comply with this European ruling (Sawers, 2016). The right to privacy has recently been highlighted in the refusal of Apple to allow the FBI to access the personal password of suspected San Bernardino terrorists as an invasion of personal privacy. This stance was backed by other companies such as Google and Microsoft (Grimes, 2016). The FTC recommends “best practices” companies should follow concerning protecting consumer privacy (Federal Trade Commission, 2019). The three key elements within this suggested privacy framework are privacy by design, simplified consumer choice and transparency.

There have been recent developments and ways businesses are approaching protecting the privacy of their consumers. Companies like Walt Disney and Novartis are revising their privacy policies, particularly moving away from the notoriously lengthy privacy policies we have become accustomed to. The effectiveness of shorter privacy policies versus longer ones is currently being researched (Gluck *et al.*, 2016) regarding awareness. Major corporations are now appointing a Chief Privacy Officer (CPO) whose job is to protect consumer and employee privacy. Data breaches such as the 2015 breach at Ashley Madison (Zetter, 2015) and Yahoo (Khandelwal, 2016) companies are now being forced to clamp down and tighten their data security regarding customer and employee data. In the case of the Ashley Madison breach, victims are reportedly still being threatened through personalised blackmail (Doffman, 2020).

In South Africa, the protection and right to privacy are clearly defined in chapter 8, under the protection of personal information, of the South African Electronic Communications and Transactions Act (2002) where unless legally required to do so and any gathering, handling, divulging or broadcasting of personal data need written permission.

The Protection of Personal Information Act 4 of 2013 (POPIA) has been effected from 1 July 2021, explicitly regulating the processing of personal information (DLA PIPER, 2020). This personal information has become especially vulnerable to persons engaging in the OSNs. OSNs such as Facebook, LinkedIn, and many others have become targets for data theft (LinkedIn, 2016; Price, 2019; Queenie, 2019). This data are sold to hackers through hacker forums and eBay-type sites, usually in batches that could fetch a $200 per 1000 set of personal credentials, including an OSN username and password (Acohido, 2010; Carroll and Buchholtz, 2018).

2.3.2.6 OSNs and Techno Moral Lag

The idea of techno moral lag is highlighted by the contemporary philosopher James Garvey (2016) in his book "*The Persuaders*", where he analyses the justification of using technology to aid possible dubious persuasive practices by the marketers of large corporates and governments down to retail outlets (Garvey, 2016). The period whereby legislation lags behind technological innovation where regulation is falling behind the technologies they govern (Murdoch, 2021; Brown and Marsden, 2023) is what the researcher refers to as "Techno Moral Lag".

As is explored in detail in section 2.6, the persuasive contentious idea of libertarian paternalism in the form of gentle nudges to a more manipulative ominous shove in the form of the affirmed collaborative psychological practice of brain hacking (O'Brolchain and Gordijn, 2015; Ienca and Haselager, 2016; Cooper, 2017) by teams of technologists, software developers and behavioural psychologists, persuasive methods through the use of OSNs on an unknowing public for financial reward may be morally off course (Boren, 2015; Carabantes, 2021). The adoption of our accepted moral standards in maintaining our individual human rights of freedom of thought and choice lags behind technology (Garvey, 2016).

As with the examples of legislation lagging approximately 70 years and ten years behind driving under the influence or driving while talking while holding a mobile phone, respectively, legislative measures in protecting organisation information and representation and the stakeholders' rights to individual freedom seem a long way from being implemented, let alone understood. Not having proper legislation emphasises the need to develop a robust governance framework in guiding the discretion of the stakeholder concerning moral behaviour when engaging with OSNs. This makes the evaluation of the ethical climate reflecting company culture within the organisation to the appropriate use of OSNs crucial and relevant to the proposed research.

2.3.3 *Business Transparency*

Transparency has become a prominent factor in corporate governance in establishing business ethics and good business practice (Carroll, Brown and Buchholtz, 2018). The need for transparency (Clark, 2012) is shown in academic literature and spans across all profit and non-profit organisations, from the government to the public and private commercial sectors (Bandsuch, Pate and Thies, 2008)

International conglomerates have a concerted drive to build and establish trust through the transparency of their supply chains assuring their customers, for example, that there are no hidden shortcuts compromising quality (Bonanni and Bateman, 2019). Thus, trust appears to be the key mechanism that propagates the use of an OSN to connect (Saeidi, 2020) and share personal information with others (Salehan and Kim, 2012). As in most social and business practices, we connect and associate with those we trust because we expect them to be transparent when communicating with us (Kirby, 2012; Haesevoets et al., 2019). As stated in a contemporary definition of Business Transparency from Forbes:

> *"Business transparency is the process of being open, honest, and straightforward about various company operations. Transparent companies share information relating to*

> *performance, small business revenue, internal processes, sourcing, pricing, and business values* (Kappel, 2019)*."*

An analysis of the notion of transparency in communication from the academic literature over the last two decades and the importance of transparent communication in the workplace as an ethic allied to corporate trust *(Haesevoets et al., 2019)*.

The lack of transparency in an organisation tends to manifest in a lack of trust and confidence from both the public and the stakeholders regarding the organisation's business practices and ethics (Rawlins, 2008b, 2008a; Schleifer, Fiorini and Auld, 2019). Over the past two decades, the academic literature has advocated transparency by an organisation as a key factor in propagating trust and restoring the trust of all stakeholders, particularly employees and the all-important public citizens. In addition, governments frequently use information and communication technology (ICT) to improve transparency (Porumbescu, Cucciniello and Gil-Garcia, 2020; Tejedo-Romero and Araujo, 2020).

However, within the last decade studies have shown that gaining trust through transparency, particularly by the government using ICT, depends on the media used (Grimmelikhuijsen, 2012; Porumbescu, 2015). Moreover, the proliferation of OSNs available to the government to push information to its citizens to increase transparency, as seen in a recent study, emphasises the role of presentation and not content alone while navigating the emerging vulnerable perils of OSNs (Berto, 2019; Porumbescu *et al.*, 2019).

It is recommended that commentary through OSNs must be managed by government with circumspection with direct purpose when engaging with the wider public (Feeney and Porumbescu, 2020). This implies that, when using OSNs regarding transparency in both the commercial world and in government, presentation, vigilance, and data protection must be adhered to (Kirchner and Razmerita, 2019; Angelopoulos et al., 2020).

2.3.3.1 Radical Transparency "The Joker in the Pack."

The phenomenon of OSNs potentially leaks and reveals unsuspecting organisation data to numerous users' eyes given a computer screen or holding a mobile device. In addition, corporate scandals are frequently exposed and reported globally on OSNs through personal accounts of private interaction turned to and exposed on open forums or a group broadcast, often exposing confidential information (Horn *et al.*, 2015; Gottschalk and Benson, 2020).

As mentioned in the introduction, radical transparency has yet to be formally or scientifically defined from an academic perspective. Researching the literature, there are diverse notions of the term radical transparency. Early in the development of Web 2.0, as the Internet merged with media, radical transparency was linked to the idea that “No contentious action would go unnoticed and unpublicized (Hammond, 2001).” Some argue that radical transparency is involuntary transparency solely by external factors through newly developed technologies resulting in the non-controlled exposure of information. This is debated to be in contrast to transparency which is controlled voluntary disclosure (Birchall, 2014; Heemsbergen, 2016). Others argue that the concept of radical transparency has materialised from blogs and other OSNs (Baraibar, 2013). Here, radical transparency further advanced the need to reveal all tied to an online world where your reputation is not only easy to find but unavoidably visible, whether perceived positively or negatively (Thompson, 2007). The argument is that the age of secrecy no longer exists. Therefore, radical transparency is defined and directed more to use OSNs on the Web 2.0 technology protocol, including blogs and websites, to communicate directly with clients and other organisational stakeholders. From an organisational perspective, radical transparency is emphasised in Elisa Baraibar’s thesis (Baraibar, 2013), stressing the need for today’s organisations to incorporate and moderate their social exposure and nuances in all stakeholder relationships (Pino and Zafra, 2019). In this way, radical transparency could be seen to promote open dialogue of opposing ideas to attain a collaborative solution instead of pandering to their own opinion (Gino, 2017). Radical transparency allows modern organisations to enter into a direct continuing discourse with their customers, employees and other stakeholders through OSNs, enabling a collaborative reach beyond the capabilities of traditional corporate communication (Pino and Zafra, 2019).

The concept of radical transparency for this study is defined as a fundamental notion of involuntary or voluntary transparency driven by the transformation to digital accessibility of networked information previously privy only to those who had physical access to a confidential filing system (Hammond, 2001). Radical transparency is thus seen to have been born from the disruptive and invasive media platforms used to disseminate involuntary information disclosure that may often be tied to political incentives (Heemsbergen, 2013). Furthermore, it understands the fine line between private and public information, which today's organisation struggles to define, often frequently resulting in an overlooked context of inevitable digital transformation and unwanted exposure (Baraibar, 2013; Gino, 2017; Pino and Zafra, 2019).

2.3.3.2 The Case for Radical Transparency

The nature of digital media provides immediate accessibility to networked information and enables the further proliferation of this information to the outer limits of any online virtual network and, in doing so, radicalizes the transparency of previously protected confidential information. This type of radical transparency was clearly demonstrated in 2006 when Iceland launched WikiLeaks (Sifry, 2011). Danah Boyed, known for her seminal work in defining SNS, cautions against this act of information propagation that may be both intentional and unintentional. Critical to the debate around radical transparency is the notion of unintentional involuntary disclosure of information and behaviour. This leaves the discussion open about whether an organisation or individual disclosed information is either consensual or involuntary, thus rendering the latter disclosure beyond their control.

2.3.3.3 Radical Transparency and OSNs

It can be argued that digitally recorded text and the ease with which it can be communicated to one or more recipients, and the ease with it then be copied and/or forwarded to other recipients and the effects thereof, was not something that was initially anticipated. Thus, the capability to use mobile devices and web-based messaging systems is a key driver in both intentional and unintentional radical transparency.

It can be argued that radical transparency, is in part as a result of the emergence of OSNs. Every text that is sent follows a permanent text audit trail, but in doing so, the message can be copied and then forwarded. If need be, the message can be copied as a screenshot and then forwarded. Forwarding, whether as a direct message, a group chat or a broadcast message, results in the content of the message being instantly available to either one, a group or a myriad of users connected via an OSN (Ringel, 2019; Heimstädt and Dobusch, 2020). The phenomena of radical transparency, whether through the ubiquitous email or other OSNs or emerging technologies such as Big Data, have been a disruptive technological force in the business for the last decade (Brown, Chui and Manyika, 2011; Roberts, 2012).

2.4 THEME THREE: FACTORS INFLUENCING RESPONSIBLE OSN ENGAGEMENT

In keeping with the first objective, the literature review turns to factors that may influence behaviour associated with OSN engagement. When commencing the literature review in 2016, the researcher considered factors influencing the behaviour of OSN engagement by using a research study of employees by using an online questionnaire. The study considered the theory of planned behaviour and social practice, resulting in the influence of perceived behavioural control and subjective norms when interacting with others (Piazza *et al.*, 2019; Kumar *et al.*, 2020).

This was done by communicating self-concept to others through trust and privacy concerns when engaging with the OSN Facebook (Bitter, Grabner-Kräuter and Breitenecker, 2014). A further qualitative study results in a list of factors within the four categories, namely, technological, organisational, social, and individual, that influence employee engagement with OSNs as part of work function (Chin, Evans and Choo, 2015). These studies and a recent literature review of research from 2010 to 2018 on perceived risk engaging with OSNs identifying social, technological, motivation, behavioural, trust, and privacy factors (Busalim, Che Hussin and Iahad, 2019), were used to identify the following general categories. These may influence employee and other stakeholder behaviour when engaging with OSNs within the organisation, addressing research question one and, in part, the prevailing research question.

- **Generational and demographic factors**
  Considering the generational effect as a backdrop to these factors would be prudent.
- **Behavioural, Psychological and Self-concept**
  The psychological factors of communication are nuances rooted in the human psyche (Meshi, Tamir and Heekeren, 2015; Turel and Qahri-Saremi, 2016).
- **Technological Communication Privacy and Trust**
  Understanding and being aware of the technological security and privacy

vulnerabilities of OSNs (Philipp K Masur, Teutsch and Trepte, 2017b).

- **Organisational behavioural influences**
  It is being aware and conforming to the online culture within the organisation (AlKalbani, Deng and Kam, 2015; Attrill, 2016).

These influence factors are explored regarding possible constructs that may guide a gauge regarding the observed levels of responsible OSN engagement within the organisation.

2.5 THE GENERATIONS AND ASSOCIATED TECHNOLOGY UPTAKE

A designated period during which common traits forged by events and circumstances are common to the people living during that time defines a generation. Those in the same generations will typically experience similar challenges, beliefs and shared memories as one generation matures into the next, so make the readjusted approach and resulting behaviours to new events and circumstances. However, those of a specific age grouping in one generation do not share the same circumstance and experiences as someone of the same age in a previous generation due to the adoption of new innovations and technologies (Widagdo *et al.*, 2021).

Since the advent of the microprocessor, there has been a rapid development of technology in distinct phases. The 1960s, 70s and 80s saw tremendous advances in each phase of computation, software development and business automation. The eighties spawned the era of public connectivity and the Internet, whilst the nineties saw the Internet mature and the onset of digital mobility. Finally, the start of the new millennium converted digital mobility to mobile accessibility in conjunction with the advent of the smartphone and cloud computing, transforming humans into digital omnivores, likening to cyborgs sporting digital wearables (Malwade *et al.*, 2018; Jin *et al.*, 2020; Hawkridge, 2022; Papakonstantinou *et al.*, 2022).

To understand the differences between the various generations, we need to consider their upbringing and the world culture and events that have shaped their attitudes and opinions during their developmental stages.

With the rapid technological changes, the general categories of generations are now being further sub-categorised. Digital thought leaders like Marc Prensky, Dan Tapscott and Larry Rosen had coined the terms ‘Digital Immigrants’ and ‘Digital Natives’ (Prensky, 2001), ‘Net-Generation’ (Tapscott, 2009), and ‘The iGeneration’ (Rosen, 2010).

2.5.1 *Digital Immigrants and Digital Natives*

Digital natives have grown up with OSNs as a de facto communication medium and are thus often unfamiliar with the formalities and nuances of the traditional communication mediums of the sixties, seventies and eighties. Digital immigrants have had to migrate from using traditional 19th and 20th-century communication mediums to adapting to the new communication medium of OSNs. For digital immigrants, the perspective of this initially somewhat unfamiliar technological platform of OSNs is seen as a social phenomenon. For digital immigrants, OSNs are accepted as a social communication mechanism that is continually evolving, where work communication is now interweaved with social communication and banter. (Weber, Fulk and Monge, 2016; Nevin and Schieman, 2021).

Before the ‘digital natives’ who were not born digitally connected, the living generations had to make a cognitive paradigm shift to function in the new digital world. As a result, they have migrated from a non-connected world to one where being digitally connected is the new ‘norm’ and have thus become ‘digital immigrants’.

In Prensky’s view, although the ‘digital immigrant’ has adapted to the digital age, and as is the case with any immigrants, they still tend to live their inherent identity by creating a disparate environment. The digital natives appear to function best when they are socially networked online are motivated by instant gratification, and communicate through instant and text messaging. An African study, where students from the university of the Eastern Cape in South Africa, was done to investigate the capacity of South African millennials regarding the nuances of digitisation as part of their upbringing, to adapt to becoming digital citizens unlike first world millennials. The study shows that having grown up with limited exposure to connectivity and access to digital devices, living in the connected digital age has its challenges. It shows that the African digital literate university-going millennials may lack soft skills such as online etiquette and expertise in online security and privacy (Takavarasha, Cilliers and Chinyamurindi, 2018).

Each generation's experience and adoption of OSNs is very different (Berezan *et al.*, 2018; Calvo-Porral and Pesqueira-Sanchez, 2019; Herrando, Jimenez-Martinez and Martin-De Hoyos, 2019). This study broadly defines the generation bands based on a combination of research papers and prominent authors on the subject (Jorgensen and Bradley, 2003; Howe and Strauss, 2007; Cox, 2019). The focus of this study covers all the generations employed by the selected organisations to be researched, namely, the Baby Boomers, Generation X and the Millennial Generation (Statista, 2021a).

2.5.2 *The X Generation*

The literature consistently states that people growing up between 1946 and 1964 are termed the Baby Boomer generation. However, those born from 1965 until 1979 fall into "Generation X" (Gen-Xer), a term generally ascribed to Coupland's (1991) “Generation X: Tales for an Accelerated Culture”, where "X" suggests a nebulous, possibly confused generation with Gen-Xer’s being the least defined category of generations.

The X generation experienced a world where physically large; expensive computers transitioned to the concept of personal computing. In addition, the X generation has experienced the transition from communication through landlines and postal mail to fax and email and, by the turn of the millennium, has had to adapt to the concept of socially interacting and communicating through OSNs (Kraus, 2017).

2.5.3 *The Net Generation (Y Generation, Millennials)*

The eighties gave rise to Generation Y, referring to anyone born from 1980 to 1999. This generation, however, is also referred to as the "Millennials", initiating them as the first internet-connected cyber-generation. The "Net Generation", a term coined by Don Tapscott (Tapscott, 2009), described the impact of the World Wide Web on the development of the Millennials. “The Net Generation”, now cited in recent literature (Leung, 2013; Qibtiyah and Beriansyah, 2019), refers to the birth range from 1977 to 1997, marginally shifted from 1975 to 1995. The Net generation has now fully adapted to the transition from workstation-based apps to mobile smartphone apps such as OSNs. They have accepted that software updates to the functionality and usability of OSNs happen without the users’ consent or knowledge, highlighting a concern regarding responsible engagement with OSNs (Sheppard and Vibert, 2019). To this end a study conducted in South African schools showed that 92% of teachers feel cyber-safety should form part of the curriculum (Kritzinger, 2016).

2.5.4 *The iGeneration (Z Generation, Zoomers)*

The Z-Generation, born in an overlap period with the millennials at the turn of the century, has grown up where the Internet is no longer viewed as a feature but as an integral and essential way of life. Harry Rosen has coined them as the "iGeneration", where the "individualized" "i" is seen as synonymous with Apple Inc.'s "i" in iPod, iPhone, iTunes and the iPad while simultaneously associated with the "I" in Internet connectivity (Rosen, 2010; Rosen, Whaling, Rab, Carrier, and Cheever, 2013; Rosen, 2014). In addition, the iGeneration is characterised by the need for social confirmation of self-acceptance and status by the number of followers and the number of 'Likes' on OSNs they engage in (Cipolletta, Malighetti and Cenedese, 2020).

Table 2.1 20th Century Categories of Generations

<table>
<tr><th colspan="3">Digital Immigrants Before 1981
(Prensky, 2001)</th><th colspan="2">Digital Natives After 1982
(Prensky, 2001)</th></tr>
<tr><td colspan="3" rowspan="2">Adopters of the World Wide Web
Prefer Personal Interaction
Combine Old with New of, doing things
i.e. Books, News Papers, Landlines and mobile
Prefer single-task, Procedural and Logical Problem Solving</td><td><b>Net Generation</b>
<b>1977 – 1997</b>
(Tapscott, 1998)</td><td><b>iGeneration</b>
<b>1990 – 1999</b>
(Rosen, 2010)</td></tr>
<tr><td colspan="2"><b>Millennials</b>
<b>1982 – 2005</b>
(Howe and Strauss, 2007; Brosdahl and Carpenter, 2011)</td></tr>
<tr><th>Silent Generation
1923 - 1944</th><th>Baby Boomers
1945 - 1961</th><th>Generation X
1961 – 1981</th><th>Generation Y
1975 - 1995</th><th>Generation Z
1995 - 2015</th></tr>
<tr><th colspan="5">Major Technological Innovations</th></tr>
<tr><td>Automobile</td><td>Television</td><td>Personal Computer</td><td>Internet / Smartphone</td><td>Big Data Machine Learning</td></tr>
<tr><th colspan="5">Preferred Communication Method</th></tr>
<tr><td>Formal Written Letter</td><td>Line Telephone</td><td>SMS Texting Email</td><td>Social Media Instant Messaging</td><td>Mobile Wearables</td></tr>
<tr><th colspan="5">Communication</th></tr>
<tr><td>Face-to-face</td><td>Face-to-face
Telephone</td><td>Texting
Email</td><td>Social Media
Instant Messaging</td><td>FaceTime</td></tr>
<tr><th colspan="5">Influential Events and Innovations</th></tr>
<tr><td>World War II
Rationing
Gender Roles</td><td>Cold War
Post War
Boom
Sexual Revolution
Moon Landings
Woodstock Teenagers</td><td>End of Communism
Live Aid
Personal Computer
Word Processors
Spreadsheets
Broken Marriages</td><td>9/11 event
Play Station
Internet
Social Media
Google
Wikipedia</td><td>Subprime Meltdown
Climate Change
Mobile Technology
Wearables
Arab Spring
Cloud Computing
Big Data
Deep Learning</td></tr>
</table>

Additional Sources are used in chart compilation (Robinson, 2016).

Note: There is no standard for when a particular generation begins and ends. Thus, dates have been approximated using the literature to show overlaps.

2.6 THE PSYCHOLOGICAL IMPACT OF OSNS AND BEHAVIOURAL SCIENCE

Researchers have been using behavioural science with specific reference to the dual system theory (Kahneman, 2012) to explain the unplanned and inhibited behaviours that are evident in the use of OSNs (Turel and Qahri-Saremi, 2018). Furthermore, OSN platform organisations are using advances in behavioural science theory, such as framing and nudging to incorporate behavioural triggers (Hirschprung, Toch and Schwartz-Chassidim, 2017). To gain insight into the behavioural complexities associated with OSN usage, a review of the implications and impact of behavioral science and OSN use is explored.

Behavioural Science is about exploring and understanding the factors that influence human behaviour. Part of the purpose of exploring behavioural science can be two-fold. Firstly, as a discipline, use the knowledge gained on what influences or coerces people to help them with prevention and intervention. Secondly, to use the knowledge gained to influence or coerce people for profit, whether through marketing, fear-mongering, distributing fake news, campaigning and other more subtle suggestion techniques such as nudging (Thaler and Sunstein, 2008). The difference between influence and coercion is about the freedom associated with whether a person feels they have a choice in a prescribed behaviour or treatment (Olsen, 2003).

Recent findings highlight the impact of psychological vulnerabilities and mental health problems when engaging with OSNs, such as digital dementia, sleeping disorders and mobile attachment anxiety (Frost and Rickwood, 2017). Progress made in the field of behavioural science over the past five decades by Daniel Kahneman. He was awarded the Nobel Prize in Economics in 2002, together with Amos Tversky, in the research of heuristics, biases, and framing culminated in the theory of the two-system approach in the decision-making process referred to as the Reflective and Impulsive Social Behaviour or the Dual Process system of reasoning.

Harvard law professor Cass Sunstein who served as the Administrator of the White House Office of Information Affairs, refers to the age of behaviour in “Nudge theory: the psychology and ethics of persuasion” (Sample, 2017) as work done in the 1970s and 1980s exploring the rationality of people. Research in this field explores the rational thought exercised in people's choices and judgements (Thaler and Sunstein, 2008). It is noted that people tend to deviate from what is seen to be realistically rational and will instead opt for unrealistically optimistic choices. This demonstrates that a person's behavioural choices are often risk-prone rather than risk-averse.

This work prompted the idea of using subtle interventions that encouraged short-term behaviour that would improve people's health, increase longevity and enhance general well-being in the long term, rather than leaving people to seek short-term gratification by engaging in what may appear as carefree reckless behaviour. For example, when it comes to personal finances, it was noted that people would sacrifice a savings plan for immediate short-term spending. Regarding health, people would opt for the convenience and instant pleasure of fast foods rather than seeking a healthier diet, thereby promoting longevity.

2.6.1 *Reflective Impulsive Theory: Two Systems of Cognitive Processes*

The advances in the behavioural sciences led to the classification of people's thought processes into two systems, simply defined as system one and system two, known as Reflective Impulsive Theory, also known as and referred to in the literature as the 'Dual-System' theory (Kahneman, 2012; Sunstein, 2013; Michaelson and Steeves, 2020; Turel and Serenko, 2020).

System one works intuitively, being prone to reactive behaviour like infatuation (falling in love), seeking instant pleasure, and being irrationally fearful. System one is characterised by processing available choice information automatically and intuitively, leaving decision-making based on heuristics that make decisions prone to conscious and unconscious biases.

System two, on the other hand, is deliberative and reflective and processed in the human brain's prefrontal cortex. System two is characterised by processing choice information through the conscious effort of information analysis, deduction and calculation (Kahneman, 2012; Kannengiesser and Gero, 2019).

As discussed previously, the addictive nature and compulsive use of OSNs can be problematic. This may be due to an organisation's stakeholders' often rash, impulsive, precarious, and detrimental use of OSNs. Such behaviour may lead to privacy abuses, careless, politically insensitive commentary, sexual, racial and gender-based remarks, and harassment on posts and posting of sensitive company information (Tarafdar *et* *al.*, 2015; Wellisz, 2016). Recent research shows that impulsive behaviour when engaging in OSNs can result from embedded differences related to the Dual-System theory and circumstantial external stimuli (Turel and Bechara, 2017).

A study by Reppler (Davis, 2011) revealed an alarming occurrence of profanities associated with impulsivity on Facebook walls. Forty-seven per cent of Facebook users make use of the words regarded as profanities, such as, in order of frequency of occurrence, “The F-word”, “Sh*t”, and “B*tch” posted on their Facebook walls.

The study by Turel and Bechara (2017) reveal distinctive possible correlations between motor impulsivity and lack of sleep, which result in dangerous and harmful behaviour such as texting while driving, deviant interpersonal behaviour such as gossiping, and the use of profanities when engaging with OSNs.

In the same study, younger and lower Grade Point Average (GPA) score survey participants exhibited a greater propensity towards dangerous and possibly harmful behaviour through OSN engagement. This could be linked to an under-developed prefrontal cortex or possibly relate to younger people being less likely to have work and parental responsibilities, thus having more leisure time on their hands (Turel and Bechara, 2016).

2.6.2 *Nudging Theory*

A prominent note was taken of the Nudging Theory following the publication of Sunstein and Thaler’s book, *Nudge: Improving Decisions About Health, Wealth, and Happiness* Thaler and Sunstein (2008, p. 6) Here they define a nudge as follows:

> *“A nudge, as we will use the term, is any aspect of the choice architecture that alters people's behaviour in a predictable way without forbidding any options or significantly changing their economic incentives. To count as a mere nudge, the intervention must be easy and cheap to avoid. Nudges are not mandates. Putting fruit at eye level counts as a nudge. Banning junk food does not.”*

This follows their 2003 paper where they counter-argue the intuitive idea that ‘libertarian paternalism’ is seen as an oxymoron by reason that, when facing a choice where the options are not well ordered or structured, choices could be based on framing effects rather than a product of their environment, rendering preferences possibly meaningless (Sunstein and Thaler, 2003). Paternalism can be defined by imposing regulations and deemed values that would be seen to protect an individual's self-interest by introducing a cost if not followed or a reward if followed. Simply stated, it "makes people" go in a direction they originally neither intended to nor wanted to go. It is an intervention of a person's liberty, justified for the sake of their welfare (Dworkin, 1983).

Sunstein further distinguishes paternalistic interventions as more aggressive, 'hard' paternalism and less aggressive, 'soft' paternalism, where the cost associated with not following a hard paternalist regulation may be prison or a fine. In contrast, soft paternalism is enforced through a warning, disclosure policy or prescribed terms and conditions (Sunstein, 2014). This is where the words "making people" in the researcher's simply stated definition of paternalism may still be appropriate. Recent literature has varying views on nudging as a positive influence on society or whether nudging is prone to manipulating society (Renaud and Zimmermann, 2018; Schmidt and Engelen, 2020). This can be associated with the foundational work of variable schedule of rewards theory known as the Hook Model by the behavioural psychologist Burrhus Frederic Skinner (Skinner, 1957), which is covered in more detail in the discussion of brain hacking. As stated in The Economist (Houston, 2013):

> *"Libertarian paternalism" is nothing but a profoundly confusing, completely superfluous synonym for anti-paternalism."*

In libertarian (the freedom of choice) paternalism, even though it may be exercised using a pointed or encouraged directive, it remains a nudge, which maintains a person's choice to opt-out of such a directive. Nudging is thus not necessarily seen as coercive, but it could be argued to be manipulative (Callard, 2015; Nys and Engelen, 2016; Wilkinson, 2013b) or, as argued regarding the use of nudging when powered by Big Data, could be 'secretly' coercive and manipulative (Sætra, 2019).

2.6.3 *Framing*

Framing is a nudge that presents words and concepts in an alternative way intended to shift people's perceived frame of reference (Thaler and Sunstein, 2008; Choe *et al.*, 2013). For example, people will often have immediate feelings for certain words or concepts such as "cost" or "hard work" based on their biases and preconceived notions that may trigger an unconscious feeling of avoidance because they are associated with a possible lifestyle compromise. A framing nudge can evade this trigger associated with unconscious emotional responses by instead associating positive or at the least neutral connotations through more appealing words or by making them view a concept from an angle or perspective that, in essence, still addresses the same question or statement eliciting a different response or choice to be affected by them.

Typical examples using framing would refer to the amount required for purchase as an investment rather than a cost, implying the idea of acquiring an asset instead of incurring liability or that the effort required is rewarding rather than hard work.

In the context of OSNs, framing relates to influencing the user through persuasive visuals towards making more preferable choices or, as in the paper, *Nudging people away from privacy-invasive mobile apps through visual framing* (Choe *et al.*, 2013) would influence the user to consider selecting mobile apps that have better and less invasive privacy settings. This approach is based on the framing effects discussed by Tversky and Kahneman (1981), where framing is used to guide or influence people's decisions in how resultant choices and options are stated.

It is important to note that the literature emphasises the positive outcomes of nudging through framing, typically quoting examples of persuading a patient to seek medical treatment or choose a healthier lifestyle (Thaler and Sunstein, 2008; Voyer, 2015). This emphasis may seek to justify liberal paternalism as an approach utilised by health and governmental organisations where framing is often purported to result in beneficial outcomes. The ethics of whether liberal paternalism is contradictory in its nature is still keenly debated, as is whether or not paternalism as such is to be accepted as an ethical notion (Vallgarda, 2012). A recent study in Argentina, where over 100 000 Twitter users were analysed, found that users are collectively engaging with OSN's frame tweets by accepting or discarding hashtags with associated keywords (Aruguete and Calvo, 2018). A similar study revealed a causal link between Facebook posts influencing news intermedia framing (Lo, Lam and Cheung, 2021). It is further deduced that framing can be used as an instrument of control (Tversky and Kahneman, 1981).

2.6.4 *Nudging Using Reflective Impulsive Theory*

2.6.4.1 System one nudge

A system one nudge is used to activate our automatic reactive thinking. This type of nudge typically uses emotive images to direct a person's thinking towards or away from a product, service or activity. A well-known example is using graphic images of lung cancer on cigarette packets to nudge people not to smoke (Alemanno, 2012). Another well-known example is the fly in the urinal at Amsterdam's Schiphol Airport (O'Hanlon, 2010). In an attempt to circumvent the sanitation problem created by careless urinating behaviour often exhibited by men, Amsterdam's Schiphol Airport found that notices and signs encouraging better hygiene habits had little effect employed a subtle nudge. The now well-known nudge was to etch the image of a common household fly at the bottom of the urinal, tempting men to aim at something whilst urinating, resulting in an 80% decrease in urine spillage (Yeung, 2012). One nudge system can often be successfully self-imposed, illustrated by placing an overweight image of yourself on the refrigerator door, discouraging you from overeating.

The lack of strategic foresight, when engaged in system one decisions, relies on good or bad habits and when running in an unconscious 'autopilot mode' makes it particularly susceptible to manipulation. Successful manipulation of system one is driven by an immediate appeal and instant gratification (Sunstein, 2016). In the context of OSNs, instant gratification can lead to an addictive habit that can be exploited through manipulation.

2.6.4.2 System two nudge

System two is characterised by processing choice information through the conscious effort of information analysis, deduction and calculation (Kahneman, 2012). A system of two nudges is used to appeal to your cognitive aptitude and may either encourage or deter you from buying a product or service or participating in some or other activity or behaviour. This type of nudge uses a person's ability to reason with the information presented to them. This may be in the form of a simple warning, or it may use informative statistics. System two will employ framing techniques in how information is structured and presented. A system of two nudges may be designed to either take advantage of a person's unconscious biases and prejudices or help them decide against these biases and prejudices through reason.

The more calculating strategic nature, which acts through carefully considering all available information when deliberating on making a decision, requires far more covert schemes for successful manipulation. Such schemes include mental trickery, deliberately supplying false information, or deliberately hiding information. In the context of the design of the menu options presented in an OSN, there may be manipulation on the part of the software company, which can control what options are presented and what options are omitted.

2.6.5 *Fogg and OSN Manipulation*

The Persuasive Technology Lab at Stanford was established and operated by the experimental psychologist B.J. Fogg who first defined the term "Captology" (Computers as Persuasive Technologies) as a new area of study that fuses the interaction of computer science and behavioural psychology, which has now become to be known as "behaviour design". Software developers borrow principles and techniques from behaviour design, also known as the Fogg behaviour model (FBM) (Fogg, 2009b, 2009a), to build OSNs that nudge the user toward forming habits that lock the user into spending more time and effort on the OSN than usual resulting in wasting time.

The behavioural technique of Pavlovian psychology is likened to the conditioning behaviour used when training pets, as in rewarding a dog when correctly following a command. Using nudging to condition human behaviour when spending extended periods on an OSN is the basis of how the FBM operates, driven by the following three simultaneous conditions as seen in Figure 2.7, namely:

1. Want: The user must have an immediate desire to perform an action.
2. Ability: The opportunity to perform the desired action must be available to the user with little or no perceived cost.
3. Prompting: The user must be prompted by what is termed a "Trigger" to perform the desired action in this context.

In Fogg's own words, the most important sentence in the FBM is, "Put hot triggers in the path of motivated people." This methodology has been implemented in most OSNs today, and although it may appear invisible to users, it is apparent in their now-assumed normal interactive behaviour. This is evident from the emails received that prompt you to purchase an item immediately or the mobile applications that grab your attention and games that keep your eyes glued to your mobile device screen. Typical examples of using the trigger of a reward in line with the FBM methodology are the “like”, “share”, or “retweet” buttons.

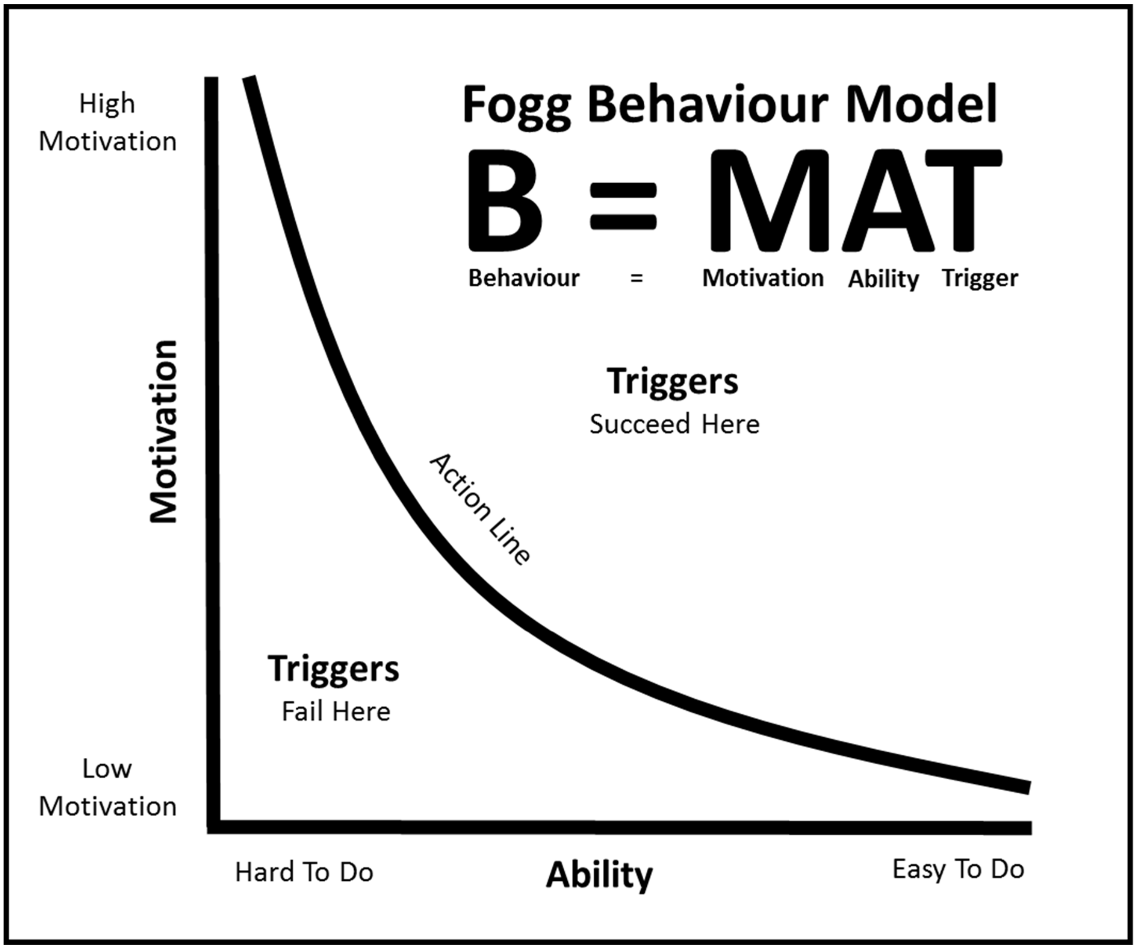
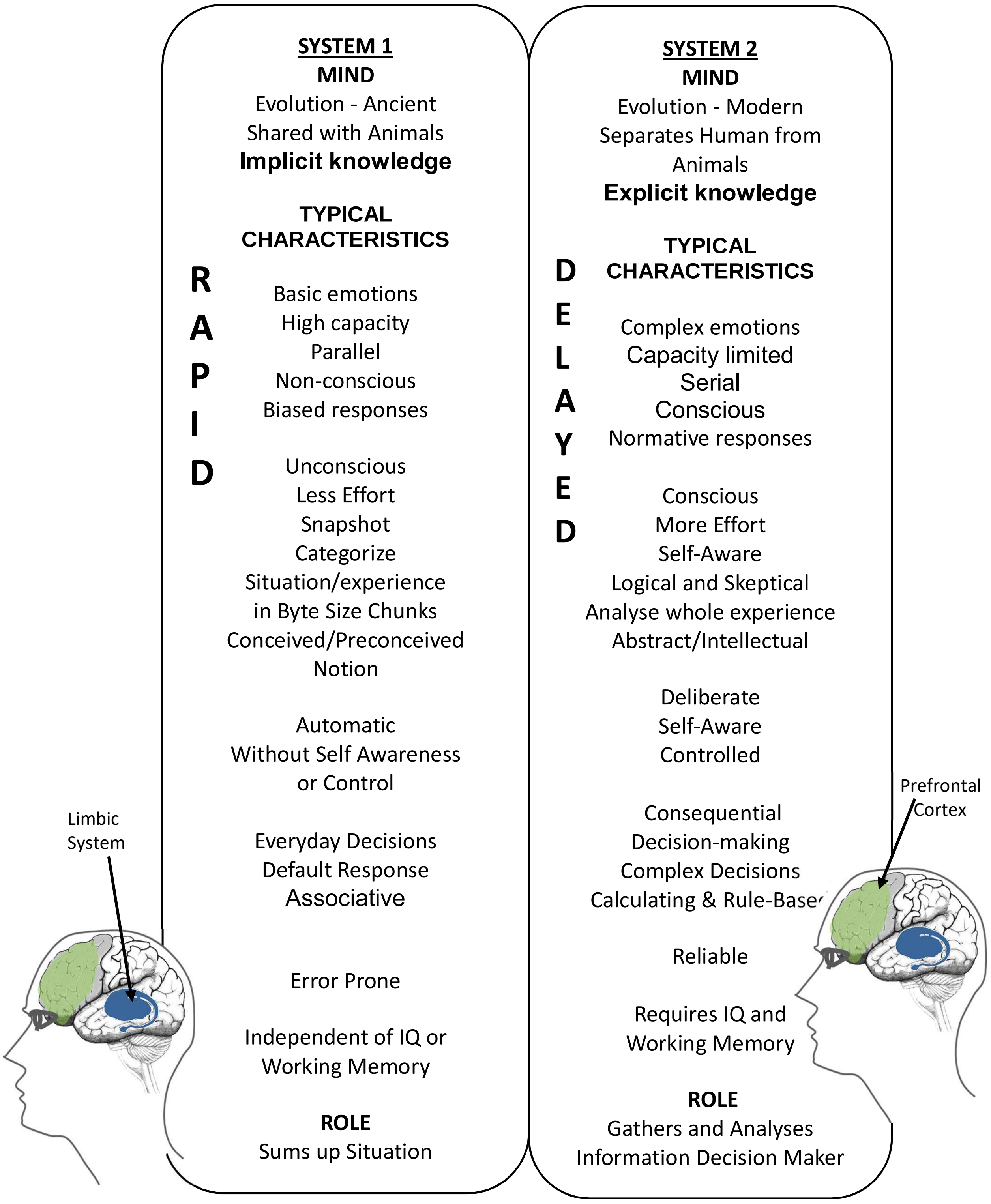


Figure 2.7. Fogg behaviour model

Source (Fogg, 2016)



SYSTEM 1
MIND
Evolution - Ancient
Shared with Animals
Implicit knowledge

TYPICAL CHARACTERISTICS

RAPID

Basic emotions
High capacity
Parallel
Non-conscious
Biased responses

Unconscious
Less Effort
Snapshot
Categorize
Situation/experience
in Byte Size Chunks
Conceived/Preconceived
Notion

Automatic
Without Self Awareness
or Control

Everyday Decisions
Default Response
Associative

Error Prone

Independent of IQ or
Working Memory

ROLE
Sums up Situation

SYSTEM 2
MIND
Evolution - Modern
Separates Human from
Animals
Explicit knowledge

TYPICAL CHARACTERISTICS

DELAYED

Complex emotions
Capacity limited
Serial
Conscious
Normative responses

Conscious
More Effort
Self-Aware
Logical and Skeptical
Analyse whole experience
Abstract/Intellectual

Deliberate
Self-Aware
Controlled

Consequential
Decision-making
Complex Decisions
Calculating & Rule-Base

Reliable

Requires IQ and
Working Memory

ROLE
Gathers and Analyses
Information Decision Maker

Figure 2.8.Graphic Summary of System One and System Two

When a user receives a “like”, displayed as the prominent “thumbs up” icon on Facebook or a “heart” on Twitter, they feel an acknowledgement of social connection and approval. The user feels rewarded by the acknowledgement of their online social behaviour. This will typically start a pattern of seeking to be rewarded on a repeated basis. This behavioural pattern then starts propagating the formation of a user habit (Soror *et al.*, 2015) that is ultimately desired by the owner of the OSN (Birkett, 2015; Foley, 2016; Harris, 2016; Harris, 2014; Leslie, 2016; McCarthy, 2017a, 2017b; Social Networking, 2017).

FBM techniques are often employed in how a user is directed to fill in an online form or application and are designed to nudge the user to decide which vendor or merchant prefers. Whether viewed as malicious or not, to hook the user in maximizing time spent on an OSN or game, the software design techniques employed in the choice architecture presented are likely to be exploiting the users' unconscious biases, predispositions, idiosyncrasies and mental gremlins (Kahneman and Frederick, 2007; Soror *et al.*, 2015; Sunstein, 2016). This psychological exploitation of the mind is known as ‘brain hacking’ (Bosker, 2016; Harris, 2016; Ienca and Haselager, 2016; Leslie, 2016). These techniques may be unashamedly and unscrupulously manipulative and, although at the outset may have been rudimentary, are increasingly becoming more sophisticated and less obvious to the user.

When questioned in an interview in 2019 on the ethical implications of using the Fogg behaviour model, BJ Fogg maintained that the focus in the development of the model was never on OSN addiction. Instead, he maintained that it be used to fast-track the user in achieving what they wanted to do in the first place, hinting at the potential possible misuse of the model (Fogg and Euchner, 2019).

Whatever the focus of the Fogg behaviour model was intended for, it is being used as a basis to persuade engagement with OSNs to form what would be seen as intended good habits, which, however, may unintentionally result in bad habits (Pinder *et al.*, 2018; Urban, Hewitt and Moore, 2018). The persuasive principles of the Fogg behaviour model are currently being employed as far as Asia (Yihui, 2018; Agha *et al.*, 2019).

This leads to the work done by the research psychologist Larry Rosen in the field of the Psychology of Technology (Rosen *et al.*, 2013) on coerced addictive behaviour

(Turel and Serenko, 2020a). Recently the research in the validation of the Fogg behaviour model was presented at a conference in Belgrade (Savić *et al.*, 2023).This work is foundational in exploring nudging theory and the manipulative notion of Brain Hacking (Harris, 2016).

2.6.6 ***Brain Hacking***

According to Design Ethicist, once employed by Google Tristan Harris, Silicon Valley is developing mobile applications and gearing devices within the realm of the Internet of Things (IoT), such as smartphones and other devices, to consistently entice the user to the application or device (Bosker, 2016; Cooper, 2017; Harris, 2016; Leslie, 2016; Tabaka, 2017). According to Harris, the methods used are purposely designed and embedded inside the application or device intended to force a behavioural pattern through a process of reward habitually. This is referred to as 'Brain Hacking'. To do this, Harris explains, companies such as Apple and Google use techniques such as controlling your choices through a prescribed menu, simulating the excitement of a slot machine, the fear of missing something important (FOMSI), and enticing social approval to name a few to exploit the user's psychological vulnerabilities (Harris, 2016; Harris and Swisher, 2019; Thompson, 2019).

Brain hacking is a term implying a malicious nature. Reviewing both the contemporary and academic literature, the researcher now presents a more formal definition of brain hacking as defined by Lenca and Haselager:

> *"The term brain-hacking refers to the emerging possibility of co-opting brain-computer interfaces (BCI) and other neural engineering devices with the purpose of accessing or manipulating neural information from the brain of users"* (Lenca and Haselager, 2016).

In keeping with the relevance of this research, we need to align the BCI to that of an OSN. Here, we look at the input manipulation within the context of the OSN. This happens when the hacker manipulates the BCI user's input by stimuli offered to the user. This input may be in preselected targeted stimuli to prompt responses in the user that access the user's neural thoughts and information. This has been demonstrated to be possible research in human-to-computer interaction.

Input in this context may be confused with the user providing input using the BCI through monitored brain activity instead of an interface more familiar with a screen with menu options and pre-empted commands. The researcher refers to the latter when referring to input manipulation to remain within the context of OSN interaction using mobile devices (Harris and Swisher, 2019), where brain hacking is a technique employed in the design of OSNs by software companies to maximize the time a user spends on their mobile device or web application when engaging with OSNs (Hirschprung, Toch and Schwartz-Chassidim, 2017). This is done by presenting convenient clicks and scrolls, making it easy to “swipe” or click on an option the user may, in retrospect, not have selected. For example, the ease of making credit card payments through a conveniently presented selection may lead the OSN user to make a payment without thinking it through. In addition, this process allows for gathering data on users engaging on OSNs, enabling the development of user-profiles through the process of Big Data analysis facilitating the in-depth knowledge of personality profiles enabling targeted marketing by third-party organisations (Sætra, 2019). The more time spent browsing and clicking through OSNs, the greater the usage and selection count of OSN users' preferences which incentivises potential third-party organisations to purchase marketing and commercial space through the OSN (Harris, 2014).

2.6.6.1 Brain Hacking, a Case for Manipulative Nudging and Framing using OSNs

Manipulation: as defined by dictionary.com (Dictionary.com, 2017) is to manage or influence skilfully, especially in an unfair manner: to manipulate people's feelings and to adapt or change (accounts, figures, etc.) to suit one's purpose or advantage.

Or in the words of the nudging theorist Cass Sunstein (2014):

> *“A statement or action can be said to be manipulative if it does not sufficiently engage or appeal to people’s capacity for reflective and deliberative choice.”* (Sunstein, 2016).
>
> *“It is important to emphasise that countless choices are at least partly a product of variables that do not involve reflective*

> *deliberation – and choosers tend to be unaware of that fact”* (Sunstein, 2016).

More strongly, Joseph Raz (1986), in defining manipulations, goes as far as to disregard coercion, proposing that:

> *“Manipulation, unlike coercion, does not interfere with a person’s options. Instead, it perverts the way that person reaches decisions, forms preferences or adopts goals”* (Raz, 1986).

Further reference is made to the widely accepted two cognitive systems of the mind to explore manipulation. Nudging is actively pursued in OSN apps such as Facebook and online purchasing apps (Balebako *et al.*, 2011; Choe *et al.*, 2013; Wang *et al.*, 2013; Beldad and Hegner, 2016; Bavel and Esposito, 2017; European Commission and [JRC], 2017). In his essay entitled “How Technology Hijacks People’s Minds – from a Magician and Google’s Design Ethicist”, Harris (2016) lays out ten programming techniques technology companies deploy to hijack the user’s brain. Harris uses technology to exploit human instinct in “the race to the bottom of the brain stem” (Harris and Swisher, 2019; Thompson, 2019). He likens the methodology in these techniques to that of a magician who uses the limits of people’s perception, such as blind spots, to influence people to select and engage in online activities without realizing it, as if to nudge them. These techniques are explored by the researcher in the context of nudging and whether the intention of nudging and/or framing translates to manipulation or even out of the realm of soft libertarian paternalism to cohesive hard paternalism.

2.6.6.2 Hijack 1: Menu Control and Directive

The use of menu options controls the usability design of an OSN. The user’s choices are directed by the options provided, and though the user is free to choose from the options available, they are limited to those options. For example, when faced with a restaurant food menu of options, the prospective diner is not expected to ask, “What is available that is not on the menu?” However, in the diner's case, it is known that should he request a non-menu item, provided it is reasonable, many restaurants will try to accommodate the diner. However, the OSN user is often trapped into believing they can only select what is available to them on the OSN application. Let us consider a nudge defined in the paper, PINC: Persuasion, Influence. Nudge and Coercion Through Mobile Devices, …*as a piece of the choice architecture (how choices are presented) that directs people's behaviour towards a determined goal without obscuring any options or introducing significant economic incentives* (Eslambolchilar *et al.*, 2011). We can argue that the position of controlling the menu through programming the options presented in an OSN the software developer nudges the user to one of the limited options available.

Nys and Engelen (2017) argue that nudging uses and exploits factors such as cognitive biases and heuristics and cannot merely be seen as rational advice and that nudging persuades people actually to make decisions outside the realms of their own interests.

Here, we can further explore the term coined by Thaler and Sunstein (2008), "choice architecture". Choice architecture revolves around how choices are articulated to the user in the case of OSNs. The way that the choice is made reflects how the options are presented. The approach of the choice architect can be likened to that of a building architect who will place passages, hallways and access to doors etc., to direct a smooth and easily accessible human traffic flow through a building. It can be argued that the approach of choice architecture may be manipulated in that the human traffic flow in a building may be designed to direct people to a specific building area whilst purposely directing them away from other parts of the building. The choice architect thus influences how choices are decided upon (Johnson *et al.*, 2012).

The financial incentive for a successful OSN is increased time spent by the user in engagement with the OSN, where a product or service can be promoted. For example, a person seeking companionship may engage with an OSN such as Tinder on entering a cocktail bar. Tinder is an online 'easy to use' dating application that uses the user's geographic location to connect interested persons seeking companionship mutually and then matching them by linking and using their user profiles from Facebook, Spotify and Instagram, enticing them to chat. Tinder will present photographs of persons matching your set preferences. You have the simple option of swiping right to show interest or swiping left if you have no interest. If someone swipes right on your photograph, the app instantaneously notifies you, "It's a Match!" as a directive to start chatting. Engaging in this type of behaviour using Tinder is addictive (Borrello, 2016;

Carpenter and McEwan, 2016). Once engaged, Tinder is designed to keep you entertained by introducing gaming. When two user swipes result in a match, the app will prompt the user to message their match, or it will prompt the user to "keep playing." The "Keep playing!" is intended as a gaming technique that clocked up a record three billion swipes in one day in May 2020 (Iqbal, 2021). Tinder's design aims to keep the user engaged in the application. This effectively nudges the user away from other potential persons in the cocktail bar who may be a far better match for companionship not on Tinder but are also seeking companionship.

The frequently cited Harvard Business Review article, “Nudge Your Customers Toward Better Choices” (Goldstein *et al.*, 2008), discusses how organisations can use choice architectures to best select and present a default option to nudge the customer to a choice ensuring not only customer satisfaction but added profitability to the organisation.

A study that looked at the use of choice architectures used default options to optimize privacy and access control on Facebook (Hirschprung, Toch and Schwartz-Chassidim, 2017). The study found that the default options nudge the customer to a more exposed open level of privacy and access control resulting in Facebook’s current choice architecture leaning to benefit the software company rather than its customers.

2.6.6.3 Hijack 2: Variable Schedule of Rewards – The Slot Machine Hook

Extensive experimental research by the prominent 20th-century psychologist B.F Skinner resulted in the variable schedule of rewards theory, known as the Hook Model, which explains the addictive nature of gambling slot machines. The addictive hook comes when the nature or size of a reward for behaviour varies. The variation of the reward for behaviour each time the slot machine lever is pulled creates a more compelling need to continue the behaviour than if the reward is a timely fixed, known entity every time the behaviour is enacted (Skinner, 1957; Schull, 2012; Weinschenk, 2013).

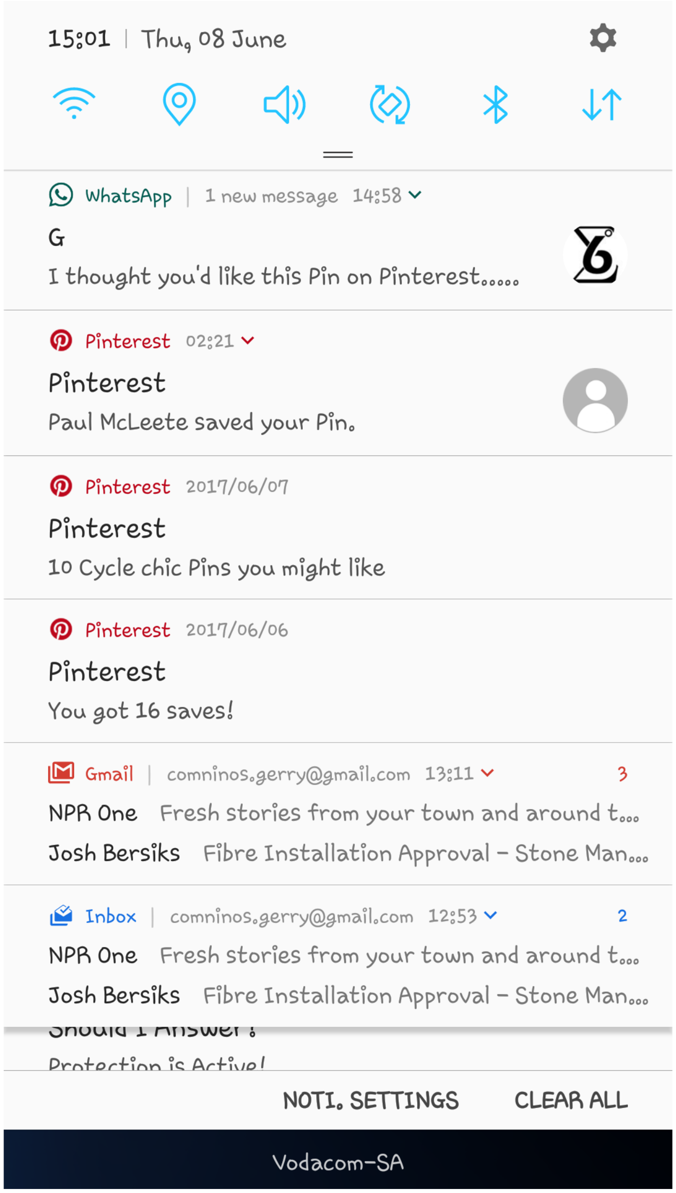
When a user regularly engages with their mobile device to check on an OSN for notifications without being prompted, their behaviour is likely that of succumbing to the addictive nature of the variable schedule of rewards as if to be pulling a slot machine lever to see what they may have been rewarded with (Eyal, 2014). This is manifested when we continually refresh our email Inbox with the hope of new emails or when we instinctively browse a suggested Pinterest board in the hope of finding new pictures or, when we down-swipe on our mobile device screen, see Figure 2.9 to check the notifications to see if there are any new WhatsApp or Facebook notifications. This is aptly described by Simon McCarthy-Jones, a researcher in clinical psychology and neuropsychology, as follows:

> *"It could be argued that Skinner's pigeon lab was resurrected at Harvard in 2004, with two modifications. It was called Facebook. And it didn't use pigeons (Mccarthy-Jones, 2018)."*

The user's habitual need to check and engage an OSN app eventually becomes so ingrained that the stress resulting from the anxiety of not engaging with the mobile device leads to an unhealthy increase in cortisol (Afifi et al., 2018). Thus, it can be argued (Haynes, 2018) that OSNs are designed to leverage the same neural circuitry that induces compulsive use of slot machines or excessive cocaine to addict the user trapping them into consistent engagement physically.

2.6.6.4 Hijack 3: Fear of Missing Out (FOMO) or Something Important (FOMSI)

Fear of missing out or missing something important FOMO / FOMSI is the anxiety when a person feels that they are missing an experience by either not being able to explore a rewarding opportunity or not having immediate access to knowledge or information they may find of interest (Rosen and Samuel, 2015). A recent study of Chinese adolescents revealed FOMO / FOMSI regarding OSN engagement as a global psychological condition linked relationship to OSN addiction, the 'need to know' and envy with adolescent FOMO (Yin *et al.*, 2019). Using techniques to play on this anxiety or the fear of there being an important message or notice on a mobile device you may miss is a powerful way of keeping a person constantly attentive to any sign of notification, whether it be a message or news alert on their mobile device (Blackwell *et al.*, 2017; Wegmann *et al.*, 2017).



15:01 | Thu, 08 June

WhatsApp | 1 new message 14:58

G

I thought you'd like this Pin on Pinterest.....

Pinterest 02:21

Pinterest

Paul McLeete saved your Pin.

Pinterest 2017/06/07

Pinterest

10 Cycle chic Pins you might like

Pinterest 2017/06/06

Pinterest

You got 16 saves!

Gmail | comninos.gerry@gmail.com 13:11 3

NPR One Fresh stories from your town and around t...

Josh Bersiks Fibre Installation Approval - Stone Man...

Inbox | comninos.gerry@gmail.com 12:53 2

NPR One Fresh stories from your town and around t...

Josh Bersiks Fibre Installation Approval - Stone Man...

Should I Answer?

Protection is Active!

Figure 2.9.Typical Screen down Swipe to check notifications

This anxiety entices people to become and remain friends within a social network. FOMO or FOMSI drives mobile device users to subscribe to news feed updates and follow friends or influential people who tweet or post regularly on OSNs. This anxiety keeps users checking the latest posts from their friends on Facebook in case they miss out on a topic, gossip on a group chat, being tagged in a photo with others, a notice of an up-and-coming social event or gathering they could partake in (Elhai *et al.*, 2016). Before the prolific use of OSNs, people were more inclined to pre-arrange and schedule social gatherings ahead of time. Because of the FOMO syndrome of knowing “where it’s happening” regarding social gatherings, people now leave their social plans to the last minute opting to choose an event or venue that is currently seen to be the flavour of the evening through the use of friend notifications or messages on OSNs (Taylor, 2019).

2.6.6.5 Hijack 4: Social Proof / Approval

When reading a Facebook news feed, watching a YouTube video, or purchasing a product or service, we are immediately led to the “Likes”, “Shares”, comments, and reviews. The amount of “Likes” or “Shares” or content of the reviews and comments are regarded as social proof that is used by at least 70% of online consumers in deciding to purchase a product (Hallen, 2014). Furthermore, the findings of a quantitative research study demonstrate the use of social proof as a method of “hijack” to influence the response bias whilst engaging in an OSN (Vashistha *et al.*, 2018).

Social proof is when people feel justified in engaging with a service or product because, in doing so, they conform to the actions of others. OSNs will display “Likes”, comments and reviews about a news feed, service or product more prominently than the service or product description itself. Using a social proof “hijack” effectively increases and gains customer trust during online purchasing (Abdul Talib and Mat Saat, 2017). Empirical research has shown that, when a “Like” is actioned, it can have a herding nudging effect by spurring others to also action a “Like”, thus, accelerating a conforming pattern of social proof (Bhattacharyya and Bose, 2020).

In his book “Social: Why our brains are wired to connect”, Matthew Lieberman (2013), a Professor of Social Cognitive Neuroscience at the UCLA Department of Psychology, Psychiatry and Bio-behavioural Sciences, contends that our happiness and general well-being are determined by the strength of our immediate social network. The strength of our social environment dramatically influences who we are, and researched data has indicated that even the thought of severing these ties can have a traumatic effect (Cook, 2013; Lieberman, 2013).

Lieberman argues that our need for social approval to belong and to be valued within our social networks is higher than the base physiological need of Maslow’s hierarchy of needs. This would make us vulnerable within our social networks for social approval.

This vulnerability is used by companies running OSNs to exploit our need to grow our social capital.

OSNs have various mechanisms to illicit social approval between uses within their social networks. These come in the form of the infamous “Like” and the “Share” or “Retweet” or tagging people in uploaded posts.

Whenever a user changes a part of their profile, be it their profile photo, work status, or relationship status, OSNs such as Facebook will send out notifications within their social network of such a change prompting friends or connections to “Like” or comment on the change. So, for example, the connections (friends) of a registered user of LinkedIn will be informed via the LinkedIn OSN when that user has a work anniversary, has been promoted or is employed by a new firm, thus alluring that user’s connections to a flurry of OSN activity in social approval.

Being tagged in a picture uploaded as a post on an OSN such as Facebook, Snapchat or Instagram is not necessarily an entirely conscious decision of the person tagging you but rather a decision orchestrated by prompting the tagger toward such a decision by the OSN. This type of gentle nudging promotes the experience of social approval and, in turn, getting more and more people to tag each other in photos helps a surge of increased activity on the OSN every time a photo is uploaded, generating a multitude of social externalities (Anaraky, Knijnenburg and Risius, 2020).

The effect of Social Approval within Organisational OSNs

If we argue that the internal networks are a central force in propagating the ethical climate within an organisation and we assimilate these networks with the OSNs engaged with by employees of the organisation whether they be primary or secondary stakeholders, the desire for social approval within these OSNs may become an influential factor in determining the ethical climate. This is alluded to in an editorial essay that explores using OSNs to educate students and an organisation’s stakeholders on business ethics, corporate social responsibility and sustainability (Montiel *et al.*, 2020).

> *“The importance of credible information sharing through OSNs is explored in a recent survey study of the role OSNs can play in the credibility of shared information based using review*

> *ratings and recommendations in an ethical environment* (Hajli, 2018)*."*

The social networks within an organisation formed on an OSN will attract people with similar interests and motivations. The larger the organisation, the greater the possibility of the social networks fragmenting into OSN cliques, threatening the homogeneity of the ethical climate within the organisation (Brass, Butterfifld, and Skaggs, 1988). The power of social approval within the formation of these cliques may act as a catalyst in determining ethical or unethical, negating the fear of retribution (Jackson, Wood, and Zboja, 2013).

From a marketing perspective, social proof can be used as an emotional trigger influencing a reactive response from OSN engagement, whether you are promoting yourself, your company or specific products (Shah, 2019).

2.6.6.6 Hijack 5: Social Reciprocity

The foundations of OSNs, particularly Facebook, are built on reciprocal friendship. On the other hand, the emphasis on reciprocity on LinkedIn is more on business connections. Using the technological platforms of OSNs, the ease at which friends or connections are attained leaves many users seeking the status associated with a large number of Facebook friends or entices them to race to display the "500+" connections indicator on their LinkedIn profile. This leaves many OSN users managing relationships far exceeding the Dunbar (Makovsky, 2014) number of 150 to 250 such relationships.

Social reciprocating to a gesture from another is part of a social norm that an act of kindness should be returned by a similar act of kindness (Brown *et al.*, 2013), even as simple, friendly facial expressions on OSNs (Florea and Roman, 2019). Therefore, the ability to programme control to nudge the user to feel obliged to comply through reciprocal behaviour can be seen as a powerful tool of OSN manipulation (Harris, 2016).

The LinkedIn methodology of accepting, endorsing or responding to a message maximises user time on LinkedIn. Both Facebook and LinkedIn persistently suggest connections, making it as easy as a one-click acceptance to fire off an invite to connect. In many cases, this type of suggested nudge is not a deliberate decision with cognitive intention but rather an emotional reaction to LinkedIn's suggested list of contacts triggered by system one thought intuition. However, this invite appears to be a deliberate intention to connect to the recipient.

Likewise accepting endorsements, LinkedIn will nudge the endorsed user by exploiting their intuitive bias by selecting and presenting them with the opportunity to reciprocate an endorsement.

This exploitive approach of social obligation through nudging can lead to inappropriate meaningless endorsements of connections that may compromise the validity of endorsements and privacy.

2.6.6.7 Hijack 6: Endless Feeds using Autoplay

Endless feeds and autoplay are commonly found in OSNs such as Facebook, YouTube and Netflix. After a user has knowingly selected to play a video or movie on an OSN such as YouTube and Netflix, the OSN will start loading a new video or film as soon as the selected video ends. The selection of the following video is most likely to be preselected based on the user's browsing history, thus enticing the user to continue engaging on the OSN by predicting what the user would like to see. Initially deciding what movie or video may have used the cognitive system two thinking; however, a default nudge of preselecting the following video or movie that appeals to the user shifts them into system one impulse thinking. This accounts for enormous traffic and clicks or swipes on these OSNs (Green, 2015; Harris, 2016; Morrison, 2014; Mott, 2014; Williams, 2016).

This is similar to moving to OSNs that provide news feeds. Once the user has read a knowingly selected news feed on an OSN such as Twitter, the OSN will, by default, nudge that user to the next news feed with similar content and subject matter. Once the user is presented with the following news feed, the user is in autopilot mode, where their intuition almost makes them the intelligence behind the selection of the following news feed based on more than just their browsing history, inducing the FOMO effect.

It can be argued that the techniques employed in endless feeds using autoplay are akin to a gentle default nudge as a combination of FOMO and Skinner's variable schedule of rewards box effect. Nudging the user to continue further news feeds or loading the next video on YouTube or Netflix subtly appeals to the system one thinking, automatically enticing the OSN user to explore the possible reward of what is next. Once initiated, the user would have to consciously terminate the process if they feel enticed to engage further on the OSN. This would force the user to fall back on system two thinking to overcome the feeling of missing out on the possible reward of seeing something exciting or important.

2.6.6.8 Hijack 7: Instant Interruption vs “Respectful” Delivery

As discussed later in ‘Text Messaging versus Calling’, the preference of texting messaging to a direct voice or video call is to protect the recipient's privacy by avoiding the disruption and intrusion of a direct phone call. In addition, text messaging allows the recipient to reply asynchronously at the least interruptive time. However, it would appear that this may not be in some OSN companies' interest. Both Facebook and WhatsApp will tell the sender when the recipient has read their message in an attempt to place an obligation on the recipient to respond timeously (Khedekar, 2014). This system one thinking nudge will typically trigger a rushed response that may lead to a flurry of back-and-forth messaging where one well-drafted system 2 thinking response may have sufficed with the least disruption. An online survey investigating the message seen function found that obligation to respond as soon as possible correlates to those character traits associated with the anxiety of being ostracized and the need for social acceptance and belonging (Mai *et al.*, 2015). A court in Delhi, India, has recently accepted the double blue click feature on WhatsApp, indicating that a message has been read as a receipt of the legal acknowledgment of the notice (tech2 News Staff, 2017).

2.6.6.9 Hijack 8: Looking for your messages? First, let us look at the latest News Feeds.

To navigate traditional software systems and applications, a menu was presented upfront. However, when opening an OSN such as Facebook or LinkedIn, the user is immediately presented with a news feed where menu options appear secondary located usually in the upper right-hand corner of the user interface surrounding the news feed. If users want to check their messages or notifications, they should immediately be nudged to first look at the latest news feed. Both messages and notifications on both Facebook and LinkedIn can be found as small icons on the top left-hand side of the screen. This technique is similar to how a supermarket strategically places essential and popular items at the back of a retail outlet, enticing the customer to less essential but desirable items by forcing them to walk past and notice the less essential but desirable items enticing them to purchase these items (Notre Dame College, 2013).

2.6.6.10 Hijack 9: Inconvenient Choices

Unsubscribing to an OSN or website feed may seem to be made purposely cumbersome and time-consuming. This inconvenience may convince the user to indefinably prolong unsubscribing, thus remaining a subscriber not through choice but by avoiding an inconvenient nudge. In addition, certain OSNs, such as Facebook, may influence users' online privacy ignorance (Van Heerden and Jordaan, 2017). The default privacy settings of Facebook monitor the user’s browsing history, data which Facebook then use to target advertisements to the user. When purchasing from a Facebook advertisement link, Facebook will send the relevant information to the advertiser. If a user consciously opts out of the initial default settings, Facebook will keep monitoring their browsing and purchase history, ultimately sharing their personal data with other third parties (Facebook, 2017d, 2017b; Van Heerden and Jordaan, 2017).

2.6.6.11 Hijack 10: “Foot in the Door” strategies

A “foot in the door” is a technique to entice an OSN user to click or swipe in what would appear as a brief engagement but may end up entrapping the user for a much longer engagement using an intuitive system one compulsive thinking of “what comes next?”

A recent experiment related to OSN engagement revealed the persuasive power of the “Foot in the Door” strategy through the automated dialogue conversation system (Wang *et al.*, 2019).

Pinterest will consistently email or message your mobile device with suggested pins for your boards. All it takes is a little “Foot in the Door” nudge to click on the suggested pins for your board, and Pinterest knows that they have you trapped for much longer than you anticipate. Pinterest will suggest one board after the other. Facebook follows the same technique of a little nudge to quickly click on a photo, not knowing the OSN will keep you longer than anticipated, with the slight nudge leading to more and more nudges. This “Foot in the Door” strategy could be attributed to the 30% growth of the Pinterest user base between 2018 and 2019 (Richter, 2019). As of January 2019, Pinterest is one of the fastest-growing online content-sharing OSNs (Meng, 2019).

2.6.6.12 Snapchat’s Snapstreak: a combination of Brain Hijacks

This habit-forming phenomenon is illustrated with the introduction of Snapchat’s Snapstreak challenge. Snapstreak is a game or challenge set up by Snapchat that measures the number of days two Snapchat users send reciprocating snaps. A reciprocating message must happen at least once to continue a streak. It is likened to the length (streak) of a volleyball or tennis rally, where the ball is returned to the opposing player without a break (Foley, 2016). The lure of this challenge is an example of self-compromise on the one hand, where users share their passwords with others to help them keep the streak going (Tabaka, 2017), leaving the users with the anxiety of breaking the streak (Thompson, 2017). The current Snapstreak record is set at 2 146 days as of March 2021.

Engaging in the Snapstreak challenge involves being caught between the release of endorphins through the “slot machine” (Greenfield, 1999, 2016a; Harris, 2016) effect and the oxytocin release of “social approval” effect (Ditzen *et al.*, 2009; Sumioka *et al.*, 2013) and the anxiety-driven by the FOMSI (Greenfield, 2016b; Harris, 2016; Tabaka, 2017).

2.6.7 *Psychological Impact and Effects of OSNs*

The OSN has transformed society from the ‘information age’ to “an age of networked intelligence” (Tapscott and Williams, 2013: Loc 389) of a live network topography of edges instantly connecting nodes in the form of people and sources of information. Online social networking enables the sharing and discussing events and ideas, facilitating immediate responses and feedback between nodes. This has fuelled today’s mindset and is sometimes known as a narcissistic “Need to Know, Want it Now” (Bolton et al., 2013) culture, particularly evident in the Y and Z Generations.

This immediate social connectivity and instant gratification behaviour (Naumovska and Novkovska, 2018) have recently been linked to an addictive nature by releasing dopamine and Oxytocin when engaging in social activity on OSNs (Edwards, 2016;

King and Dong, 2017). In addition, a study of Spanish adults and seniors exploring the relationship between positive and negative experiences in quality of life found that both positive and negative stress was experienced through OSNs (Díaz-prieto and Canedo-garcía, 2019). Conversely, the implication is that individuals may become addicted to engaging in OSNs, which could negatively impact their ability to control their urges to connect with others. Furthermore, engaging with OSNs involves an active investment in time that may be driven by addiction that, in a recent study on adolescents, has been correlated with anxiety, distress and depression (Keles, Mccrae and Grealish, 2020).

With this introduction of the psychosocial impact and its effect on the profitability, reputational risk and day-to-day functioning of the organisation, other adverse health and psychological effects of OSNs in the literature reported to exhibit are explored.

Day-to-day observation has indicated that over-usage of OSNs may be, as discussed earlier, by using the Hook Model and the Fogg behaviour model as design elements using brain hacking techniques by OSN developers, prolonging application usage (Montag *et al.*, 2019). Furthermore, the psychological impact of this prolonged usage and compulsive use of OSNs has been reported to manifest itself in social media fatigue, leading to distress, depression, and anxiety (Dhir *et al.*, 2018). The effect of these and further psychological factors such as sleeping disorders, digital dementia, nomophobia and others are discussed.

2.6.7.1 Mobile device separation anxiety

The concept of a cyborg as a person whose physiological functioning is supported and managed by an electronic device helps explain the current habit-forming behaviour and anxiety experienced, in particular by millennials with their relationship to their mobile device. In 2008 YouGov, a research company, was commissioned by the UK Post Office to investigate anxieties associated with mobile phone use (Merz, 2013; Vincent, 2013; Elmore, 2014). The survey showed alarming levels of anxiety associated with what YouGov devised as the term “Nomophobia”, an abbreviation for “no-mobile-phone phobia,” meaning the distress of being either separated from your mobile device or rendered inoperable from either a rundown battery or being out of cellular coverage.

A literature review analysing the psychological and behavioural effects of nomophobia during the decade from 2009 to 2019 reports that symptoms of anxiety, panic, fear and depression by people suffering from panic disorder associated with agoraphobia are significantly more severe relative to those associated with Nomophobia. Furthermore, excessive smartphone use can partially ease the emptiness of depression (Goncalves *et al.*, 2021). A study of 274 adolescent smartphone users revealed an increase in loneliness and anxiety in adolescents contributes to more time spent engaging with their smartphone, indicating nomophobia behaviours (Kara *et al.*, 2019).

A recent Australian study attributes FOMO as one of the brain hacking techniques (Hijack 3) as part of users' unhealthy dependence on their mobile phones (Oviedo-Trespalacios *et al.*, 2019).

2.6.7.2 Blurred vision and Headaches

Computer vision syndrome (CVS) is a condition that results from continuous staring at computing-related devices such as computer notebooks, tablets and smartphones. Symptoms of CVS include blurred vision, headaches, eye strain and dry eyes.

Research on the detrimental effects of CVS in the workplace has been ongoing for the last couple of decades. For example, a 2011 study revealed that approximately 90% of people who stare at digital screens for at least 2 hours a day experience some form of CVS (Chu et al., 2011; Chawla *et al.*, 2019).

2.6.7.3 Extended work hours

From a work perspective, being constantly on call and available through our mobile devices may be seen as positive concerning employee performance. The gain in extended work performance may, however, be destroying employee work-life balance and, in turn, opening the organisation to a host of labour-related legal ramifications, especially when the line between work and personal time becomes blurred (Marcum, Cameron and Versweyveld, 2018; Mullan and Wajcman, 2019).

2.6.7.4 Sleeping Disorders and Deprivation

An experiment conducted at Brigham and Women's Hospital in Boston revealed that, when reading on an iPad instead of a printed book, those using iPads showed a reduction in melatonin associated with inducing sleep (Dennis, 2014). Furthermore, sleeping disorders were associated with problematic mobile phone use (Zhu *et al.*, 2019).

2.6.7.5 Phantom Vibration Syndrome

Phantom vibration syndrome is the illusion that a person may feel their phone vibrate, thus believing they are receiving a call, message, or notification (Rosenberger, 2015). A survey of approximately 400 participants in the US found phantom phone vibrations widespread (Tanis et al., 2015). In addition, a recent study found that from a sample of 258 mobile phone users, 34% experienced phantom vibration syndrome due to mobile device overuse, potentially causing damage to intellectual and cognitive skills (Desai, Patel and Mohit, 2019).

2.6.7.6 The stress of OSNs in the workplace

In a recent study, using OSNs in the workplace affected the employee physically and emotionally. Excessive OSN engagement may lead to a physical path of addictive behaviours that may impede the employee’s work-family balance. In addition, OSN reactions may lead to emotional burnout (Zivnuska *et al.*, 2019b).

In contrast, a further recent study showed that younger employees entering the workplace have already aligned their mindset to the practical and professional use of OSNs within the professional environment rather than falling prey to less professional social etiquette that they may have become accustomed to as students (Towner, Everett and Klemz, 2019).

2.6.8 *OSN Addiction*

Excessive use of OSNs has yet to be recognised as an addiction disorder by the World Health Organisation however the evidence that overindulgent and unrestrained use can disrupt functional workplace environments (Turel and Serenko, 2020b). Eventually, this habitual behaviour is translated into a ‘bad habit’ exhibiting a pathological and maladaptive psychological craving and addiction.

2.6.8.1 Compulsive Texting Habits

We will define a bad habit as a well-practised disagreeable behavioural pattern requiring marginal energy that renders little value. This typically happens when the now-formed bad habit previously rendered a valued result but presently no longer does. This habit is often associated with instant gratification that may conflict with long-term objectives (Wood, 2017). For example, a recent study conducted in Australia revealed that habitual text messaging is correlated to a high incidence of texting while driving (Moore and Brown, 2019).

2.6.8.2 Measuring OSN Addiction

As discussed earlier, brain hacking will use OSNs to facilitate technology addiction. The subject of OSN in addiction has been extensively researched over the past decade (Andreassen *et al.*, 2013; Griffiths, 2013; Davenport *et al.*, 2014; Sultan, 2014; Andreassen, 2015; Choi, 2018; Kircaburun and Griffiths, 2018; Zivnuska *et al.*, 2019a). This has led to the development and use of the well-known Bergen social media addiction scale (BSMAS) (Andreassen, Pallesen and Griffiths, 2017; Monacis *et al.*, 2017). However, the effect of OSN addiction in both the workplace and private life remains contentious and subject to further research (Choi, 2018). A study sample of 326 employees was conducted to explore the possible relationship between OSN addiction and the workplace and found a negative correlation between OSN addiction and work performance and the balance between work and family (Zivnuska *et al.*, 2019c).

This has led to further studies to identify the addictive habits of personality types to associated OSN platforms (Hughes *et al.*, 2012; Andreassen *et al.*, 2013; Kircaburun and Griffiths, 2018). In addition, identifying personality types and traits of OSN usage has led to exploring the possible connection between self-esteem and OSN addiction (Hawi and Samaha, 2017a).

2.6.8.3 OSN Addiction and the Organisation

Addiction of any kind can have a detrimental effect on the functioning of an organisation. For example, addictive behaviour associated with OSN engagement by the employees of an organisation may expose the organisation to reputational risk, work inefficiency and lacklustre productivity.

OSN addiction is exacerbated by the financial incentive of OSN companies, such as the Facebook group of companies, to program addictive features in the software of their OSNs (Andersson, 2018). This should be of grave concern to the organisation regarding OSN engagement and business transparency. The ubiquitous nature of OSNs, both as web and mobile device applications, has become an imperative tool in business communication (Pourkhani *et al.*, 2019). The prescribed guidelines in usage as a necessary business communication platform often cannot be divorced from direct social use. Personal and private engagement with OSNs can challenge an organisation’s governance framework. Responsible OSN engagement may be reflected in the organisation’s work culture, which in turn is reflected in the organisation’s ethical climate. Evaluating OSN addiction and its effect on the organisation becomes a vital element in this study. This incidence of habitual behaviour and the specific difficulty individuals may have in overcoming their compulsions of text messaging. This aspect should concern the organisation since the vulnerable employee is far more likely to compromise the organisation's integrity.

2.7 A CASE FOR ONLINE SELF-AWARENESS AS AN INFLUENCING FACTOR

From the literature review, when considering responsible OSN engagement, we note the exposure to behavioural science techniques purposely programmed into OSNs to drive compulsive texting habits and OSN addiction. To gather insight into the psychological predisposition of the user to the susceptibility of compulsive addictive OSN engagement, we turn to findings in research studies.

Some of the leading researchers' Mark Griffiths, Daria Kuss, and Cecilie Andreassen, have been linking low self-esteem and low self-efficacy levels to OSN addiction (Andreassen, Pallesen and Grif, 2017; Griffith and Kuss, 2017; Kuss and Griffiths, 2017; D’Arienzo, Boursier and Griffiths, 2019).

> *“In relation to SNS addiction, self-esteem is reported to be one of the important factors, and it is negatively associated with SNS use and social media addiction* (Kircaburun and Griffiths, 2018)*.”*

Further recent findings from quantitative studies have confirmed the link of OSN addiction to self-esteem and self-efficacy across cultures (Hawi and Samaha, 2017b; Atroszko *et al.*, 2018; Osatuyi and Turel, 2018b; Wang *et al.*, 2018; Hou *et al.*, 2019).

> *"Facebook addiction would be a result of ineffective mood regulation by individuals who have a problematic social life, specifically those who have high social anxiety and loneliness, and general emotional instability, low self-esteem, and low general self-efficacy combined with low openness to new experiences…This is one of the most important findings, as self-efficacy has been more or less neglected in the context of Facebook addiction, despite the fact that there is a well-established link between this trait and addiction in general."* (Atroszko *et al.*, 2018)*.*

2.7.1 *Measuring Self-Esteem*

Measuring self-esteem has prompted research into the association between OSN addiction, self-esteem and cyberbullying. The most popular measurement of self-esteem is the ten items Likert scale, developed by Morris Rosenberg as far back as 1965 (Rosenberg, 1965). As a scale, the Rosenberg Self-esteem Scale (RSES) has been validated for its internal consistency and repeated test dependability (Kille and Wood, 2012). The RSES has been shown to have sound convergent and discriminant validity (Blascovich and Tomaka, 1991). The RSES is consistently being used and validated (Donnellan, Ackerman and Brecheen, 2015; García, Olmos and Matheu, 2019).

Recent studies using RSES found that a lack of self-esteem may be a significant protagonist in the recent phenomena of both OSN addiction and cyberbullying. The RSES is commonly selected to assess self-esteem in quantitative studies revealed that texting habits, susceptibility to OSN addiction and cyberbullying are linked to self-esteem and fatigue due to the overuse of OSNs (Dhir et al., 2018; Kowalski, Toth, and Morgan, 2017; Saridakis, Benson, Ezingeard, and Tennakoon, 2016; Yin et al., 2019; Błachnio, Przepiorka and Pantic, 2016; Bányai *et al.*, 2017; Burrow and Rainone, 2017; Hawi and Samaha, 2017a; Brewer and Kerslake, 2015; Bányai *et al.*, 2017; Kircaburun and Griffiths, 2018; Hou *et al.*, 2019). In addition, a web-based Norwegian study using the Bergen social media addiction scale (BSMAS), the RSES and the Narcissistic Personality Inventory identified narcissism and a lack of self-esteem associated with addictive OSN engagement (Andreassen, Pallesen and Grif, 2017).

2.7.2 *Measuring Self-Efficacy*

The psychologist Albert Bandura (Bandura, 1998) is known to have originated the concept of self-efficacy as the level of a person's self-belief in their capabilities through exercising a functional ability to accomplish events that may affect their lives. Research findings show that self-esteem and self-efficacy are positively correlated as a mediating role in retaining self-control over behaviour abuse such as compulsive bad habits and addiction (Yang *et al.*, 2019). Furthermore, the same research findings revealed that subjects who exercise a high self-control level were positively associated with high levels of self-esteem and self-efficacy.

The General Self-Efficacy Scale (GSE) (Schwarzer and Jerusalem, 1995) has been consistently used to evaluate and measure self-efficacy levels (Luszczynska, Scholz and Schwarzer, 2005; Schwarzer and Warner, 2013; Atroszko *et al.*, 2018; Lazi and Jovanovi, 2018). For example, in evaluating the disparities in gender in technology employment, a recent study developed and adapted the Cybersecurity Engagement and a Self-Efficacy Scale (CESES) that was reviewed regarding OSNs (Amo, 2016). This scale included self-efficacy constructs regarding general computer use, cybersecurity, systems administration, networking, web management, and cyber threat identification (Amo, L., Zhuo, Wilde, Murray, Cleary, Upadhyaya, 2016).

This opens the opportunity to tailor the GSE using the CESES to a 10-item Online Self-Efficacy Scale geared to measuring efficacy levels that promote responsible OSN engagement.

2.7.3 *Online Self-Awareness*

Also noted is the reliance on a personal moral code of ethical considerations such as the earlier defined 'Techno Moral Lag', radical transparency and messaging privacy which determine the online behaviour of the organisation's employees. OSN engagement behaviour is guided by what the researcher defines as the employee's online self-awareness.

Online self-awareness within the organisation is about the employee’s own online code of conduct and online behaviour concerning organisational and personal confidentiality and privacy whilst engaging with OSNs. In addition, the employee’s personal assessment of their vulnerability to malicious elements within the virtual world is also assessed when engaging with OSNs.

Awareness of online security and privacy protection has been linked to online security behavioural intentions (Barth and de Jong, 2017) and online self-efficacy (Hocevar, Flanagin and Metzger, 2014; Bada, Sasse and Nurse, 2019).

Self-concept may be defined as the formation of a cognitive view of attitudes, beliefs and value judgements a person understands about themselves that is manifested in their thought processes, abilities, emotions and habits (Rodriguez and Loos-Sant’Ana, 2015). Simply stated, self-concept is how a person perceives their negative and positive aspects (Showers and Zeigler-hill, 2015). Furthermore, self-concept is related to self-esteem and self-efficacy (Wehrle and Fasbender, 2018). A review of comparisons between self-concept and self-efficacy conveys that, although the measurement constructs of self-concept and self-efficacy are alike, self-efficacy is a more predictive measure than self-concept (Bong and Clark, 1999). This is validated by previous and current research studies on the interrelations between math self-concept and self-efficacy (Pajares and Miller, 1994; Arens, Frenzel and Goetz, 2020). Therefore, self-awareness or self-referenced beliefs can be stated to be a culmination of self-concept, self-efficacy and self-esteem (Loos-Sant’Ana and Ferreira De Brito, 2017). This leads to the construct of online self-awareness that can be observed within the context of the Cybersecurity Engagement Self-Efficacy Scale and the Self-Esteem Scale and can consequently be used as an exogenous variable to assess the relationship between online self-awareness and responsible behaviour of OSN engagement.

2.8 COMMUNICATION PRIVACY AND TRUST

The nature of messaging, whether it be the now more traditional email, Short Message Service (SMS) used through a mobile phone, or instant messaging through an OSN, not only records all aspects of the communication but can facilitate the mass broadcast of the message (Flanagin, 2017). The introduction of this technology has given rise to the earlier discussed notion of radical transparency, which may expose OSN communication, whether intentional or not, to the possibility of public broadcast and scrutiny. An integral function of an OSN is to connect to a social network of friends, work colleagues, business connections, or people with similar interests through a web-based media communication network. Messaging between users is the heart of an OSN. Messaging by a mobile device using text peer-to-peer messaging reached over 12 million, while over-the-top messaging applications reached over 40 million per minute (Clement, 2019a). As of September 2021, approximately 3.1 billion mobile phone users were accessing over-the-top messaging OSNs. It is thus pertinent to review the literature on the phenomena of text messaging. All mobile devices have a simple, direct peer-to-peer messaging service, commonly known as Short Messaging Service (SMS) or Text messaging (texting) for short.

It is crucial to distinguish peer-to-peer messaging (mobile device directly to a mobile device) and messaging through the engagement of an OSN, which uses the OSNs network topology of connections and friends between users. On the other hand, SMS text messaging uses the same cellular network infrastructure to send a message as a voice call.

This enables the user to send an SMS to any device that is enabled to receive a cellular call, regardless of its operating software. Once the SMS has been generated, it will remain on the sender’s sim card until the recipient’s phone confirms receipt. The identifying source of an SMS is the sender's mobile phone number, and the transmission cost will generally be charged to the account holder of the sim card number registered by the sender (Hord, 2005). This contrasts with the mobile Instant Messaging (mIM) OSN app, also known as Over-the-Top (OTT) services such as WhatsApp, Telegram and Facebook Messenger, discussed earlier in section 2.2.1. IM requires the message participants to access the mIM app on their mobile device or web application. Furthermore, the transmission of the data are done through an Internet Service Provider as opposed to a cellular network provider that may be accessed through a Wi-Fi connection but, if not available, may use part of the cellular network provider’s conduit. In such a case, the user will only be charged for the Internet data fee, which in most cases is nominal compared to an SMS charge.

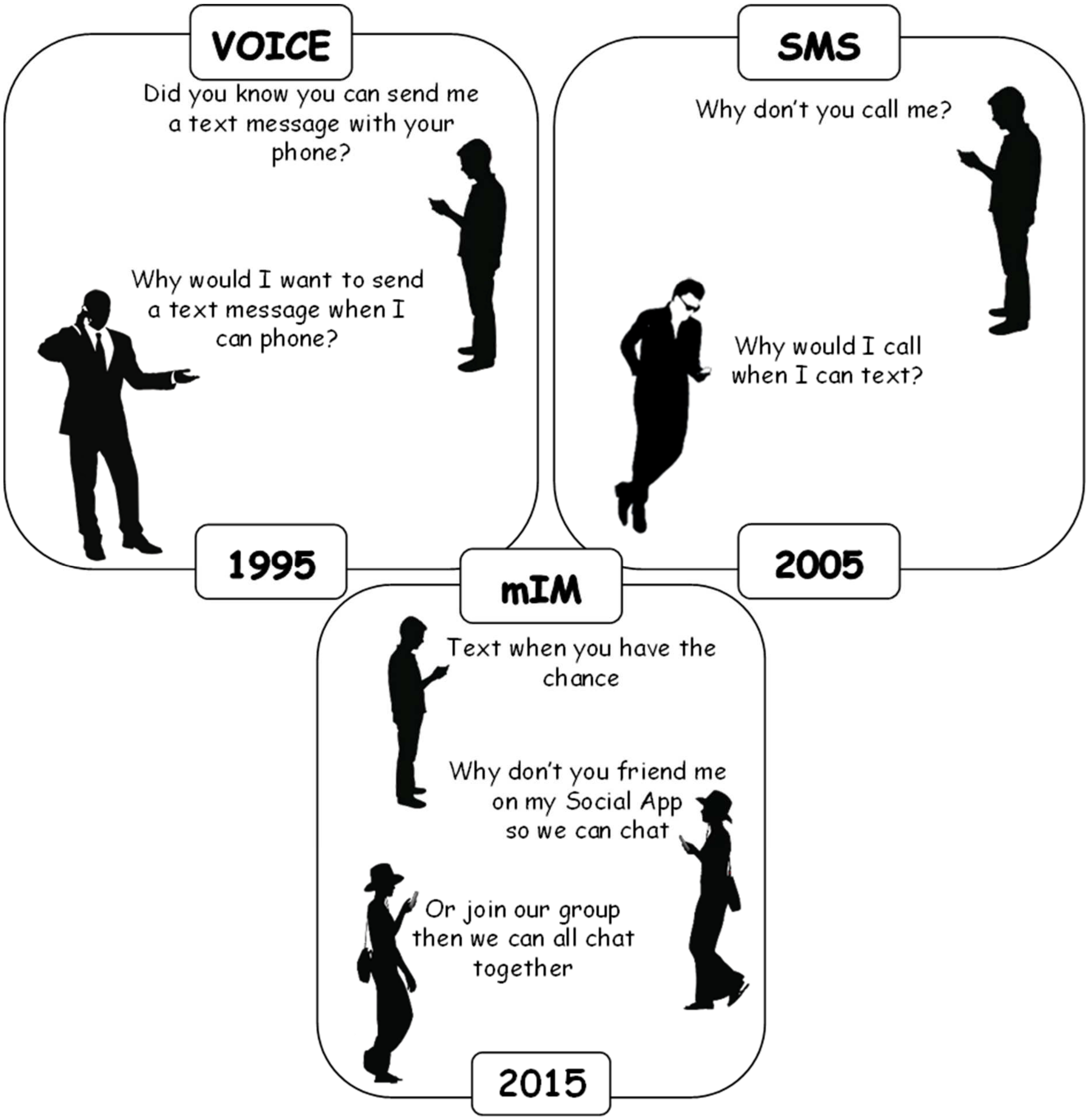

VOICE
Did you know you can send me a text message with your phone?
Why would I want to send a text message when I can phone?
1995
SMS
Why don't you call me?
Why would I call when I can text?
2005
mIM
Text when you have the chance
Why don't you friend me on my Social App so we can chat
Or join our group then we can all chat together
2015

Figure 2.10 The evolution of mobile device communications

Figure 2.10 illustrates the evolution of mobile device communication since the mobile phone was accepted as a communications device by the mainstream public.

The identifying source of an OSN message is the personal OSN profile of the user registered on the mIM OSN. An mIM can be sent from any mobile device whose operating system software is compatible with the app. In 2014 Facebook acquired WhatsApp messaging for $55 (US) per user, with approximately 400 million users (Deutsch, 2018). As of July 2021[CW1], WhatsApp is globally the most popular mobile messaging app, with 2 billion active accounts. This was followed by Facebook Messenger at 1.8 billion (Statista, 2021b).

It should be noted that the dominance of messaging platforms is regional. Asian messaging applications are dominated by local apps such as WeChat, LINE, and KakaoTalk. As of July 2019, Tencent's WeChat and QQ messaging applications had 1.132 billion and 807.9 million monthly active users, respectively, of which 902 million daily WeChat users send an average of 38 billion messages daily. The Russian messaging apps VK and OK share just over 100 million daily users (Clement, 2019a; Smith, 2019).

The behavioural traits inherent in the paradigm shift in communication from voice to messaging are relevant to this research. Understanding why texting is a preferred medium to voice or the written form is a key element to understanding need for competent online security and privacy. Messaging takes on an entirely new dimension in communication. Subtle nuances in OSN messaging platforms may influence the selection of the OSN to convey a message. Two recent qualitative studies have explored the influence of such a selection. From the studies, selection depends on user relationship stages, such as family, romance, or lifelong friends (Rost *et al.*, 2016; Schneider, 2017). From a commercial and organisational perspective, the actual text in the message concerns the user irrespective of the messaging platform. This research emphasises the human aspect and responsible engagement when sending a text message through an OSN, regardless of the continuously evolving technology it is based on. As used in other literature, text messaging and instant messaging are interchangeable and will refer to all types of electronic messages, whether typed or visual, such as emojis (McSweeney, 2018). Most OSN communication platforms can broadcast a message to multiple users. The term texting may thus also refer to texting messages posted on broadcast OSNs such as Twitter and Facebook. This type of communication medium is established as ubiquitous and is most likely becoming the most prolific means of personal communication in the world today.

2.8.1 *Mobile Devices and Face to Face relations*

In 2007 more Americans switched to communicating with each other by texting rather than calling. The prominence of texting as a preferred way of communication driven by Millennials has resulted in tension in the workplace between this younger generation and the older Baby Boomers. They feel that voice and face-to-face communication are still far more effective in maintaining business relationships and communication (Crosby, 2015). As discussed earlier, the need for constant immediate access to our mobile devices warrants the device's presence in all aspects of our lives.

A research paper on the effect of WhatsApp on the social life of adolescents warns that a lack of physical interaction may lead to a false perception of kinship and belongingness and a fake sense of intimacy with OSN connections, whether they be online acquaintances, actual friends or relatives (Kiran and Srivastava, 2018).

A study by the Meyers-Briggs organisation in 2018 and 2019 examined views on the always-on culture concerning work satisfaction and the work/home struggle (Hackston, 2020). About 30% felt compelled never to switch off, over 25% felt that being constantly on compromised their personal and family lives, and 20% indicated that it could lead to mental fatigue and burnout. On the other hand, over 10% felt that being connected and always-on was beneficial workwise.

Professional environments may vary, which may determine nuances in mobile etiquette. This is discussed in a research paper concerning a clinical environment where a balance is between maintaining privacy/confidentiality during patient-physician consultation and taking another patient's call. Other concerns may be Microbial clinical transmission from a mobile device surface and maintaining a personal/professional boundary during the consultation (DeWane, Waldman and Waldman, 2019).

2.8.2 *Central Themes of Why We Prefer Text Messaging*

The analysis of the themes derived from the literature further categorises into two or a combination of the two, as seen in Figure 2.11, namely Privacy and Efficiency. Unforeseen at the inception, the intrusive nature of not only being contactable 24/7 but having to engage in unplanned, formal conversation on the mobile phone gave rise to the less intrusive and efficient use of the mobile phone.

Communication through texting or instant messaging through OSNs is so prolific that one cannot be blamed for seeing the irony in using this form of communication to retain privacy. If anything, the mobile phone has been the key culprit in invading our privacy.

When introduced as a technology, having a mobile phone on your person meant that you were contactable at all times, whether during business meetings or driving through to being on the toilet. This was a tremendous shift in intrusion and a disturbance in going about one's daily business. Text messaging seemed to be the answer to overcoming the intrusive nature of the phone.

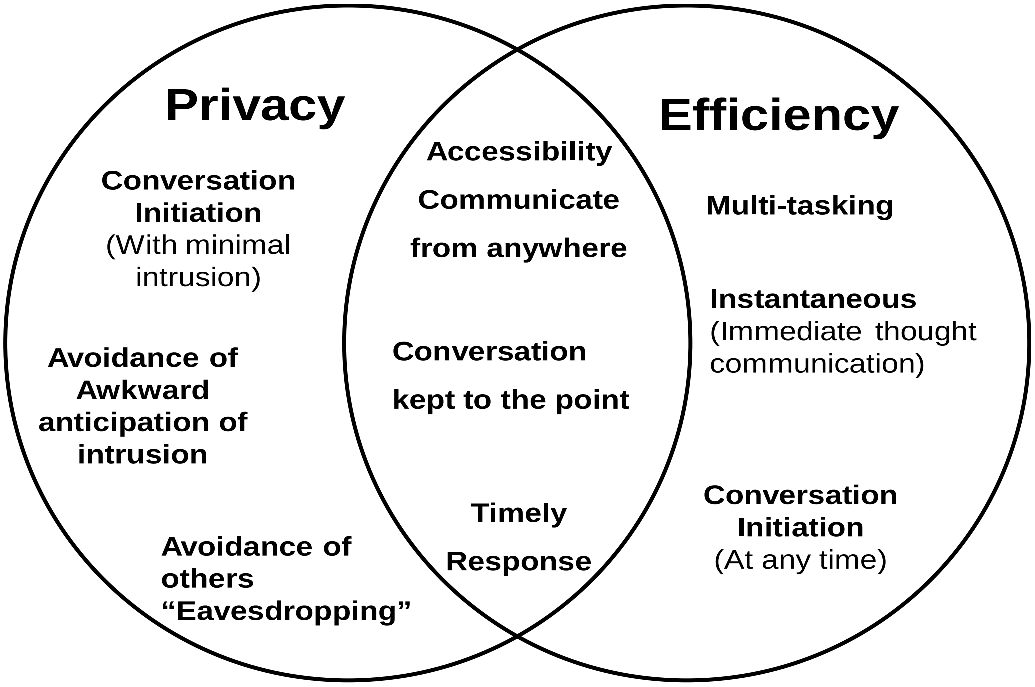

Privacy
Efficiency
Conversation Initiation (With minimal intrusion)
Avoidance of Awkward anticipation of intrusion
Avoidance of others "Eavesdropping"
Accessibility
Communicate from anywhere
Conversation kept to the point
Timely Response
Multi-tasking
Instantaneous (Immediate thought communication)
Conversation Initiation (At any time)

Figure 2.11. Central Themes of Why We Prefer Text Messaging

2.8.2.1 Millennials and Text Messaging in today's Work Environment

Little formal academic literature was found concerning the reasons for the paradigm shift from a voice call to text in today's (2015 - 2019) work environment. Therefore, as with the previous section, 'Millennials prefer text messaging to voice calls', reliance was made on less formal commentary based on interviews from recognised blogs, business newspapers and magazines from well industry experts.

In the work environment, the benefits of texting, driven by the younger workforce, are rooted in privacy and efficiency (Matthews, 2019). From a privacy standpoint, millennials seem to have developed a culture where phoning a work colleague without emailing them first could be seen as invasive (Hofschneider, 2013). Driven by efficiency, millennials want to understand and be instructed on what needs to be done, skipping the small talk or having to wade through a clutter of emotions associated with direct face-to-face or telephonic conversation (Crosby, 2015; Howe, 2015).

Moving toward the future, as Millennials dominate the workplace, organisations will adapt their communication practices and etiquette to both their employees and customers (Matthews, 2019).

2.8.2.2 The Perils of Broadcast Texting and Reputational Risk

A text or post-broadcast by an employee can present an idea or an image about an organisation that differs vastly from the organisation's values, in other words, the public image of what and how the organisation wishes to be portrayed.

In intending to mock her own privileged life through a poorly phrased tweet, Justine Saco’s tweet was interpreted as a racist comment, resulting in her becoming the number one trending topic on Twitter overnight in December 2013. This resulted in reputational damage to both her and her organisation. As a result, Justine lost her job and withdrew from public interaction (Ronson, 2015).

In January 2016, the Standard Bank economist Chris Hart resigned after being accused of an alleged ‘racist’ tweet which became a major trending social media topic (BusinessTech, 2016).

If not all, most organisations have governance and social media policies in place. However, whether intentional or not, as shown in the above examples, stakeholder engagement on OSNs still poses reputational risks and confidentiality breaches. This emphasises the need to evaluate the ethical climate concerning OSN engagement and the organisations' stakeholders' online privacy literacy level.

2.8.3 *Privacy and Closed Versus Open Social Networks*

OSNs fall into two categories, open (asymmetric) and closed (symmetric) networks (Bouadjenek, Hacid and Bouzeghoub, 2016). An asymmetric or open network where the user follows (connects) without a reciprocal connection or being followed back. This type of network connection can almost be likened to a subscription service where a user will subscribe to a connection within a social network and then be privy to all correspondence associated with this connection as a silent bystander within the social network. On the other hand, the prospect of reciprocating to a host of voluntary followers offers a followed user the platform to exercise influence at a marginal cost.

A symmetric or closed network is governed by reciprocal privacy rules where the act of connecting to another user needs an invitation and reciprocated acceptance. The privacy settings of the OSN govern all interaction between connected nodes within social nodes of a closed network.

A prominent example of an OSN typically used for asymmetric open broadcast is Twitter, where your posts are shared with whoever decides to follow your tweets (Bouadjenek, Hacid and Bouzeghoub, 2016). This type of OSN is very advantageous in the fast distribution of news feeds and related commentary. Although the asymmetric nature is key to Twitter's popularity as a broadcast OSN, Twitter facilitates private messaging enabling a user to directly send a private message to recipients (Twitter, 2020a). It must be noted that a private tweet cannot be retweeted by one of the recipients unless the contents are copied into the clipboard and then tweeted (Twitter, 2020b). Twitter has recently added an additional privacy functionality to combat abuse and spam, whereby recipients must accept a private message from a user they do not follow (Wagner, 2017). On 17 January 2019, Twitter tweeted, "*We've become aware of and fixed an issue where the 'Protect your Tweets' setting was disabled on Twitter for Android*", meaning that on an Android platform, tweets that were deemed private could be publicly accessed (Foltýn, 2019).

Facebook and LinkedIn use the closed model, where friends are connected through a reciprocal agreement. Messages and sharing are only seen by connected friends you are directly messaging. Each conversation is separate and not combined into a thread, even if more than one person may be in the conversation.

Forwarding messages using traditional SMS texting or an mIM such as WhatsApp can only be done by message content protecting the sender's identity as seen in the original message. In July 2018, WhatsApp implemented a limit of forwarding messages to a maximum of five recipients at a time. This was in response to mob killings linked to the spread of false information through its platform (BBC, 2018; WhatsApp, 2020).

When creating groups on Facebook, there is an option for three privacy settings: Public, Closed, and Secret. A user can request to join a closed group, but a user needs to be asked to join a secret group. The same confidentiality and privacy settings between two connections apply to both closed and secret group conversations

(Facebook, 2017e). Members of a group that are not directly connected can chat or message each other within the group chat but cannot directly message each other on a one-to-one basis until they connect as friends (Facebook, 2017a). If a new friend is included in an existing group, they will now have access to the history of messages that have taken place since the inception of the group message or chat (Facebook, 2017c). As with private electronic conversations, whether email or direct texting, maintaining the privacy of the message requires an implicit level of trust between the messaging parties.

Although Facebook is considered symmetric, operating on the default privacy settings renders the user open to asymmetric properties. In addition, users are often loathed to go through the time-consuming, somewhat complicated privacy settings on Facebook (Facebook, 2020), thus leaving much of the user’s posts, shares and other activities often linked to other third-party apps, such as their activity on Tinder open for public scrutiny.

OSNs such as Instagram and Snapchat are far more symmetric by nature. Instagram offers little interaction other than posting images, sporting “look at”, “like”, and “comment on” buttons, whereas Snapchat has no “like” or “comments” buttons. Most interaction on Snapchat is direct user-to-user communication.

The intention or purpose of a user when engaging with OSNs should determine whether an open, closed or variation thereof OSN is selected. For example, when tweeting whilst engaging on Twitter, users put their message out there for all who wish to see it. On the other hand, when posting on Facebook, the message or post is intended only and limited to the user’s social network of friends. The key for a user to maintain their privacy on a symmetric network such as Facebook or an asymmetric network such as Twitter is understanding the privacy settings of the OSNs.

2.8.4 *Messaging versus Social Media*

In line with the move from voice to messaging, the move to communication with family, friends, and work colleagues using mobile Instant Messaging (mIM), OSNs, instead of OSN Media platforms, has to do with regaining and maintaining privacy when using OSNs. Up-to-date usage and user visit statistics change quarterly and annually. Sources such as Statista (Clement, 2019b; Jessica Clement, 2020a) and Business Insider (Business Insider, 2016; Browse Media, 2017; Dogra, 2017; Opzeeland, 2017) put the usage of the top four OSN Social Messaging platforms combined as now higher than that of the combined top four OSN Social Media apps (Schaefer, 2016) by 2017.

As of 2020, it is reported that just over one-third of users with messaging apps have at least two messaging apps; global usage of messaging apps exceeds user interaction of generated content of social media platforms by 20%. WhatsApp, followed by Facebook Messenger, remain the most downloaded messenger app globally (Spectrm, 2020; Tankovska, 2021). It must be noted that during January 2021, Telegram app downloads exceeded downloads of the WhatsApp app in South Africa. However, as of August 2021, there are still only 550 million Telegram users to the 2 billion WhatsApp users and 1.3 billion Facebook Messenger users (Business Insider SA, 2021; Statista, 2021b).

As discussed earlier in the section 2.2.3, OSNs as a media of information, when defining OSNs, the distinction between social networking sites, OSN social media and OSN messaging platforms is increasingly becoming blurred. For example, Facebook Messenger can be accessed from the Messenger.com website and the user's Facebook account on the mobile or web application. Third-party apps have been developed, enabling add-ons for faster access in many browsers (Moreau, 2020). Facebook is in the process of connecting Facebook Messenger, Instagram and WhatsApp to enable a cross-over messaging experience while maintaining each app as its own entity (Mosseri and Chudnovsky, 2020). This goes hand in hand with the term OSNs for this study as a Web 2.0 online application that encompasses all social networking generated using interactive user-rich-generated content through a cloud platform.

2.9 A CASE FOR ONLINE PRIVACY LITERACY AS AN INFLUENCING FACTOR

The privacy paradox often characterises research on OSN engagement (Barth and de Jong, 2017). Concern about online privacy when engaging with OSNs is invariably negated through a lack of awareness and knowledge of the exposure and vulnerability of online privacy disclosure or simply through careless online behaviours. However, a quantitative study revealed that 66 university students from the Netherlands with a technical background, downloaded five prescribed apps that had varying degrees of privacy threats. The study revealed that the students did not rank privacy and security related aspects as a high priority and were prepared to risk privacy intrusions while being fully aware of any potential risks (Barth *et al.*, 2019).

When a typical user first starts interacting using an OSN, they may be struck by the simplicity of sending or posting a message, whether plain text, an emoji, an image or video. The ease of communicating with text messages explored earlier may render the user oblivious to the privacy risks of using OSNs, especially when communicating with other trusted parties. However, as explored in this section, communicating by engaging with OSNs, as simple as the experience may be, is fraught with underlying invasive exposure to unintended and possible malicious disclosure of personal or organisational private and confidential information. Whether it be the lack of awareness, knowledge or a careless attitude, the onus and accountability to engage responsibly with OSNs fall on the user.

For responsible engagement on OSNs, a user not only needs to choose what personal or organisational information to disclose but needs to know and understand how to protect against any unwanted disclosure of personal and organisational information through the privacy settings on the OSN and its communication infrastructure. It is this *'I know why'* and *'I know that'* factual knowledge and the *'I comply with'* policies, regulations and procedures and then the *'I know how to'* skills for data protection that involve and define online privacy literacy (Trepte *et al.*, 2015; Masur, 2020).

In the last decade, empirical studies have revealed a disconcerting gap between the intent of addressing OSN privacy concerns and actual online privacy awareness and knowledge which suggests that online privacy literacy is one of the key culprits of this gap (Lewis, Kaufman and Christakis, 2008; Park, 2013; Park and Mo Jang, 2014; Dienlin and Trepte, 2015; Trepte *et al.*, 2015; Bartsch and Dienlin, 2016; Barth *et al.*, 2019; Masur, 2020). This has led to the development of the standardised online privacy literacy scale (OPLIS) (Philipp K. Masur, Teutsch and Trepte, 2017). OPLIS has regularly been used as a foundational standard in measuring online privacy literacy (Hagendorff, 2018; Oeldorf-Hirsch and Obar, 2019; Rosenthal *et al.*, 2019). In addition, understanding the need for online privacy settings has been recently highlighted in the media (Suciu, 2020) and has been formally addressed as a privacy model for OSNs (Masur, 2020; Trepte, 2020).

Online privacy literacy is often countered with the propensity to conveniently shrug off responsibility for the default settings of the OSN. It is as if it is in the hands of the developers of the OSN, who render the complexities and privacy settings hard to understand and beyond the scope of the average individual. The intimidated user's approach can be further exacerbated by an OSN provider purposely constraining the ease of configuring their OSN privacy settings (Debatin, 2011; Ramokapane, Mazeli and Rashid, 2019). When engaging with OSNs, employees need to cultivate a knowledgeable appreciation of OSN privacy rather than adopt a conveniently ignorant, naive indifference towards the apparent intimidation of technology (Debatin *et al.*, 2009; Debatin, 2011; Alkire, Pohlmann and Barnett, 2019). A recent study revealed that students aware of the privacy risks and intrusions were still prepared to forego the inconvenience of setting privacy settings for expediency (Barth *et al.*, 2019).

The evaluation of this gap or disparity between addressing online privacy intent and online privacy conduct is a key element in evaluating the intended behaviour of the employee of an organisation in contrast to the actual behaviour exercised whilst engaging on OSNs regarding business transparency (Masur, 2020). This leads to the need to address online privacy literacy with online privacy behavioural intent.

The challenge of a measuring standard to evaluate end-user security and privacy behaviours has been addressed by developing the security behaviour intentions scale(SeBIS) (Egelman and Peer, 2015). The initial development of this 16-item scale of the user's behavioural intention measures the proactive awareness of web security settings and links, device securement, password generation, and software updates' vigilance. SeBIS was further validated as a reliable tool for predicting computer security behaviours (Egelman, Harbach and Peer, 2016). A cross-culture study using the SeBIS of over 5000 users revealed differences in security behaviour across cultures. The same study further revealed that personal self-confidence in computer security had a greater influence on positive security behaviour than actual knowledge itself (Sawaya *et al.*, 2017). Work has been done in developing the SeBIS, which has spawned subsequent further research refining this scale (Crowell and Ramakrishna, 2020). SeBIS was recently adapted for smartphone use and was validated as a 14-item Smartphone Security Behavioural Scale (SSBS) (Huang *et al.*, 2020).

Furthermore, within the ethical climate of an organisation, we distinguish between horizontal and vertical privacy. Horizontal privacy is more concerned with norms and rules regarding privacy influenced by the individual employee's interaction within the social and business environment, whereas vertical privacy within the organisation is concerned with stakeholder privacy within the organisation's information repositories (Masur, Teutsch and Dienlin, 2018).

When considering specific industries such as healthcare services, one must consider online privacy intentions and online privacy literacy concerning OSN engagement specific to organisational governance and the professional and industry standards geared to information technology specifications defined in eHealth. eHealth addresses the effect of the digital platform in facilitating healthcare. This would incorporate online digital skills to communicate and search for relevant healthcare material whilst maintaining patient privacy and confidentiality. Recent research revealed that online privacy competency directly influences eHealth (Li, 2018). This was brought to light in an audit showing the ease of public accessibility to medical staff and student Facebook profiles by patients and external professionals (Shah *et al.*, 2019).

Online privacy literacy on OSNs and the communication infrastructure they operate on can be mediated by the intention to exercise and comply with the protection of private and organisational information disclosure is an observed gauge of responsible OSN engagement. This leads to the construct of online privacy literacy that can be observed using the OPLIS mediated by the SeBIS [R2]and can consequently be used as an exogenous[R3] variable to assess the relationship between online privacy literacy and responsible behaviour of OSN engagement.

2.10 ETHICAL CLIMATE AND ONLINE ORGANISATIONAL AWARENESS

Following the discussion in the introduction, ethical climate reflects the organisation's core values that define the work culture in the workplace environment and influence either ethical or unethical employee behaviour (Teresi *et al.*, 2019). Thus, the ethical climate is fundamental to the core values of the organisation and critical in managing deviant behaviour. In addition, the ethical climate impacts the employee's commitment to the organisation through the perceptions and emotions in the workplace (Pagliaro *et al.*, 2018; Tang, Holmes and Foley, 2020).

2.10.1 *Online Behaviour, Ethical Climate and the South African Labour Act 1995*

The need to evaluate the ethical climate within the organisation is critical in establishing the attitude and approach of stakeholders within an organisation regarding online behaviour concerning their engagement on OSNs. The differences in approach between the Baby Boomers, the Millennials, the Net-Generation and the Z Generation as to what is good, what is acceptable or non-acceptable behaviour and conduct when engaging on OSNs is often open to interpretation (Watson and Lopiano, 2016; Dolan *et al.*, 2019).

2.10.1.1 Labour Related Studies from the South Africa

In South Africa grounds for employee discipline or dismissal is based on the conduct outside the workplace can constitute a breakdown on the working relationship. This is evident in the disrepute of the employer and an employee’s actions, causing a breakdown in the inherent trust relationship between employer and employee (Davies and Badal, 2016).

This means that, if an employee engages in an OSN with content that adversely affects the trust relationship, the employer can motion a disciplinary hearing, resulting in disciplinary action or dismissal of the employee. This means that the said charge does not need to bring against the employee being a breach of the company's stated policy or governance as long as it can be shown that the employee’s action has consequently resulted in a break of working trust between the two parties.

This trust relationship can be compromised either directly by a social media post that directly references work colleagues of the employer, eroding a working trust relationship or indirectly by associating the employer and work colleagues in a social media post that offends or is inappropriate to a third party which leaves the employer vulnerable to disrepute.

2.10.2 *Survey of Ethical Climate (ECQ)*

In 1987 Bart Victor and John Cullen published the results of an instrument they developed around Kohlberg’s three levels of moral development (Kohlberg, 1968) to survey the ethical climate within an organisation (Victor and Cullen, 1987). Today the Victor and Cullen ECQ is a widely respected cross-cultural survey of ethical climate

(Grobler, 2016; Malisetty, Rao and Kumari, 2018; Mitonga-Monga, 2018; Vryonides *et al.*, 2018; Abadiga *et al.*, 2019; Viđak *et al.*, 2020).

This theoretical typology of ethical climate is divided into two survey measurements. The first is the ethical criteria used to decide on particular actions or behaviours, and the second relates to the locus of analysis as a frame of reference in ethical decision-making. The first survey of the ECQ is based upon Kohlberg's moral reasoning development, divided into three levels: pre-conventional, conventional, and post-conventional (see Figure 2.12). Exploring the moral condition through these three levels, we note that Kohlberg categorises each level into two stages where different ethical norms and standards in human development gauge and determine moral decision-making and reasoning.

The literature classifies three key aspects of ethical behaviour within an ethical climate. Firstly, broadly referred to as 'Egoism", it is the effect of actions and behaviour of a person on their personal well-being. Secondly, 'Benevolence' is the actions and behaviour that promote the best possible outcome for all. The third aspect of ethical behaviour, called 'Principles', is the actions performed out of a sense of duty and obligation. There has been recent criticism of Kohlberg's conception of various stages, levels, and reasoning processes as incompatible with reality (Carpendale, 2000) or that Kohlberg's theory lacks in fully comprehending the moral judgement-action gap (DeTienne *et al.*, 2019). However, for this research, Kohlberg's stages of moral development are used as a basis for the Victor and Cullen ECQ.

Sociology Referent Theory is used to quantify the second measurement. The locus of analysis is then broken down into three aspects: the individual, local (related to those within the organisation), and cosmopolitan, which relates to the affected society around the organisation. Finally, when merging these two distinct measurements with the three above aspects leads to Victor and Cullen's nine theoretical ethical climate typology types, as depicted in Table 2.2.

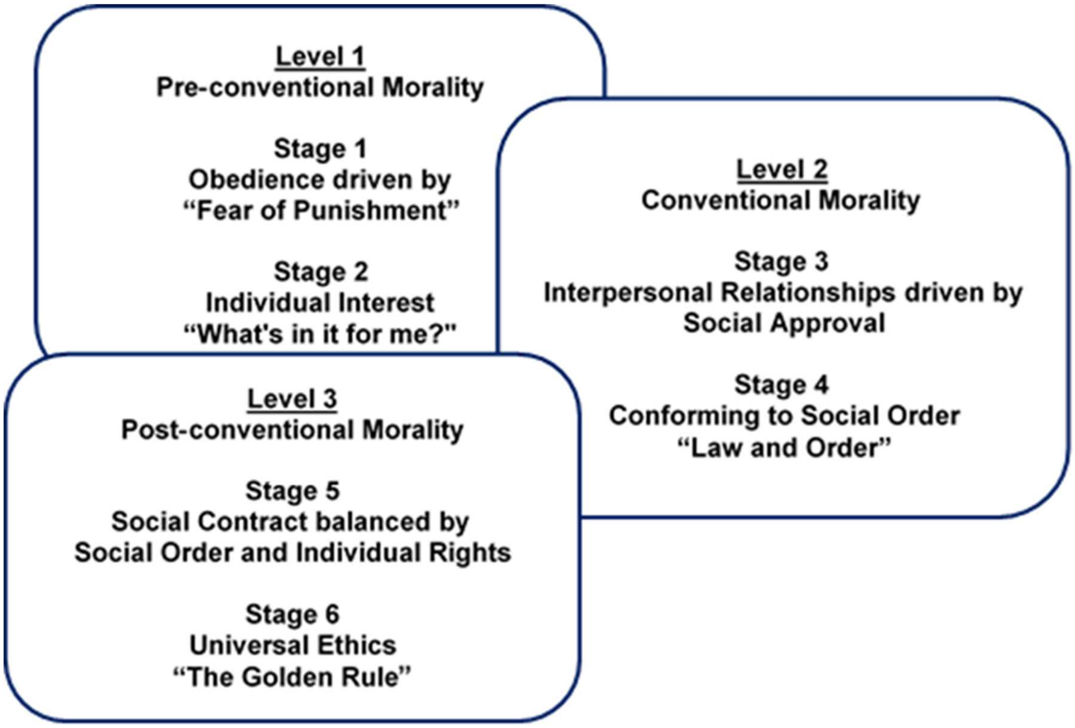
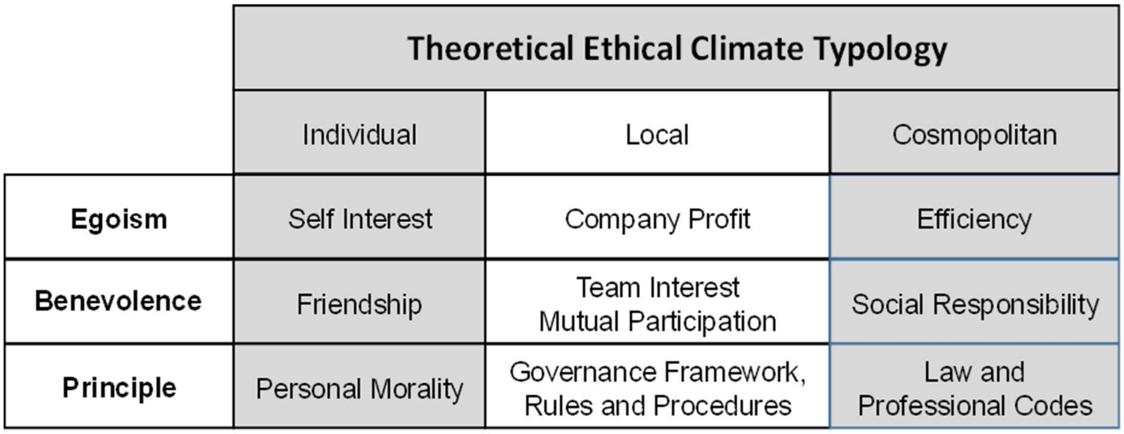


Figure 2.12 Kohlberg's Stages of Moral Development

Table 2.2. Theoretical Ethical Climate Typology



	Theoretical Ethical Climate Typology		
	Individual	Local	Cosmopolitan
Egoism	Self Interest	Company Profit	Efficiency
Benevolence	Friendship	Team Interest Mutual Participation	Social Responsibility
Principle	Personal Morality	Governance Framework, Rules and Procedures	Law and Professional Codes

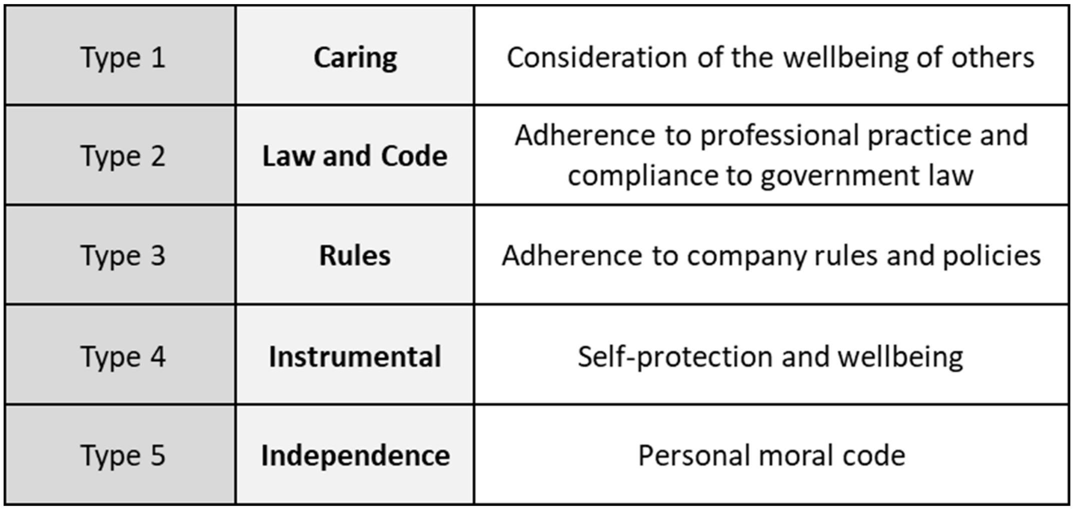
Source: (Victor and Cullen, 1987, 1988)

For this research, Cullen and Victor's definition of ethical climate is used as the broad definition of 'ethical climate'. The locus of analysis refers to the leading referent group that identifies "the source of moral reasoning used for applying ethical criteria to organisational decisions and/or the limits on what would be considered in ethical analysis of organisational decisions" (Victor and Cullen, 1988:105).

A new sample used on the ECQ by Victor and Cullen (1988) resulted in the classification of five ethical climate types summarised in Table 2.3.

Research on the ECQ has recently been conducted in countries with specific reference to China, Japan, Singapore (Shafer, 2013), Ethiopia (Abadiga *et al.*, 2019), the Democratic Republic of Congo (Mitonga-Monga, 2018), the USA (Curtis, 2014; Taylor and Curtis, 2018) and Australia (Shacklock, Manning and Hort, 2011; Tang, Holmes and Foley, 2020). Research in South African of ethical climate in organisations (Grobler, 2016) has resulted in the validation and standardization of the ECQ.

Table 2.3. The five types of Ethical Climate



Type 1	**Caring**	Consideration of the wellbeing of others
Type 2	**Law and Code**	Adherence to professional practice and compliance to government law
Type 3	**Rules**	Adherence to company rules and policies
Type 4	**Instrumental**	Self-protection and wellbeing
Type 5	**Independence**	Personal moral code

Source: (Victor and Cullen, 1988).

Grobler's research has now resulted in the classification of three ethical climate typology represented in the five-type typology (Victor and Cullen, 1988) illustrated by Grobler in

The three resultant ethical climate types, namely, Institutionalised ethics (ethical work environment), Instrumental and Personal morality, are classified by the researcher by their characteristics and resultant outcome in Table 2.5. stakeholders when engaging in OSNs. 'Cosmopolitan' refers to the ethical implications when engaging in OSNs affecting society beyond the organisation.

2.10.3 *Ethical Climate within the context of OSN engagement*

The typology's ‘individual’ and ‘local’ aspects will refer to the ethical and moral reasoning of the individual employee, fellow employees, and other organisation

Table 2.4. Classification of the three types of Ethical Climate

ETHICAL THEORY	**LOCUS OF ANALYSIS**		
	Individual	***Local***	***Cosmopolitan***
Egoism	INSTRUMENTAL Self-interest (16;17;18) Company profit (19;20;21; **22 [EC])**		Efficiency (6;7)
Benevolence	Friendship (3;4) Team interest (1;2)		Social responsibility (5)
Principle	Personal morality (23;24;25;26)	Company rules (12;13;14;15)	Laws and professional codes (9;10;11)

Source: (Grobler, 2016)

Table 2.5. Three ethical climate type typology

Ethical Type	**Characteristics**	**Outcome**
Institutional Ethics	Ethics defined and entrenched in the organisation. Consideration of the well-being of others.	Efficiency well-being of all Stakeholders
Instrumental	Ethical criteria is egoism. Loci of analysis are both individual and local. Interest for public sector	Maximise self-interest (Individual) Profitability
Personal Morality	Decisions driven by personal moral code. Limited to principles and deontology. Discrete ethical reasoning with in organisation.	Stakeholders Principles Affirm Company Ethics

Source: (Grobler, 2016)

A recent study of 376 workers from selected Italian SMEs found that attention to an ethical climate identifying and directed at individual self-interest and competitiveness is paramount to the organisation’s ethical climate, which may influence individual behaviour on the level of self-categorization within work or social groups (Pagliaro *et al.*, 2018). A key feature of OSNs is group communication, where OSNs such as

WhatsApp's individual ethics and behaviour may benefit from the social conduct appropriate to the group (Regina *et al.*, 2017).This is where organisations in the financial or healthcare sectors can use ethical climate-promoting guidelines in targeting the individual’s self-categorization concerning the correct behaviour of a member belonging to WhatsApp group chat where inappropriate sensitive content is vulnerable to be seen or shared within seconds (Bouter, Venter and Etheredge, 2020).

In promoting organisational governance and policies when engaging in OSNs, the importance of an ethical climate driving a high level of trust in relationships between employees, customers, partners, and other stakeholders should not be underestimated when communicating online (Teresi *et al.*, 2019).

In addition, it is here where the evaluation of the ethical climate in the organisation is reflected in a culture conducive to encouraging the employee to regain agency by seeking an enlightened approach to online privacy settings available through the OSN.

The organisation’s ethical climate should echo a culture that encourages them to understand the consequences of a breach of their privacy, empowering them to make proactive choices protecting themselves from the possible negative impacts of OSN engagement (Alkire, Pohlmann and Barnett, 2019).

2.10.4 *Deviant Workplace Behaviour and Ethical Climate*

A recent study on Nigerian employees shows ethical climate to be a significant factor in deviant workplace behaviour (Obalade and Arogundade, 2019). In Portugal, a quantitative study of 223 employees supports the role of an ethical climate driven by leadership to temper bullying in the workplace (Freire and Pinto, 2021). deviant workplace behaviour and traits susceptible to OSN engagement, assert that the more minor deviant behaviours, including gossiping and more serious sexual harassment, verbal profanities, and abuse, associated with interpersonal deviance often leads larger deviances (Bressler and Bergen, 2023). They also relate to the unethical sharing of confidential company information associated with organisational deviances (Troshani and Wickramasinghe, 2018). Organisational deviance is defined as deviant behaviours directed at an organisation, company vandalism, theft from the company, fraud, purposely not working to one’s full potential and violating a company’s confidential information (Christian and Ellis, 2014; Pagliaro *et al.*, 2018; Obalade and Arogundade, 2019).

2.11 A CASE FOR ONLINE ORGANISATIONAL AWARENESS AS AN INFLUENCING FACTOR

Ethical behaviour in an organisation may be defined as conforming to the values, principles and norms of what is agreed upon in the professional business community as responsible and moral. Guidelines to type this behaviour are mostly through the organisation’s governance, policies and procedures and industry-specific codes of conduct and what has been legislated by law (Remišová, Lašáková and Kirchmayer, 2019). However, there are times when judgements about what is responsible and moral behaviour fall in a grey area. Moral judgement is the process of assessing the moral responsibility of an action (Cullity, 2018). As Trevino and Nelson (2017) explored, a moral judgement leading to ethical behaviour within the organisation is influenced by the characteristics of the individual employee and the organisation as a whole. Described as the ethical decision-making process, ethical behaviour is influenced by an ethical judgement that originates from ethical awareness (Small and Lew, 2021).

Moral or ethical awareness is critical to identify the ethical implications of a possible pending situation within the organisation (Trevino and Nelson, 2017). However, a lack of a culture of awareness of the ethical nature of pending choices in decision-making leaves the employee without the building blocks of moral reasoning (Filabi and Bulgarella, 2018). This would likely result in a lack of guidance concerning ethical and responsible behaviour when engaging in OSNs.

Organisational awareness is the understanding of the components such as the ethical and moral demeanour, the leadership style of the hierarchical relationships and influencers of an organisation, both through the perception of formal and informal dynamics within the organisation (Goleman *et al.*, 2017; My HR, 2017; Office of Human Resources, 2019; Caredda, 2020).

Online organisational awareness is understanding the nuances of the organisation transformed from the physical to the global online platform. When interacting on this global online infrastructure through the engagement on OSNs, the ethical climate survey refers to shared perceptions of the employees of an organisation regarding “what constitutes moral and responsible online behaviour.” More specifically, this occurs as soon as an employee or group of employees feel compelled to exercise ethical reasoning for responsible behaviour when engaging in OSNs and are aware of adhering to the online culture, standards, or rules for decision-making within the organisation. This leads to the construct of online organisational awareness within the context of the ethical climate questionnaire that can consequently be used as an exogenous[R4] variable to assess the relationship between online organisational awareness and responsible behaviour of OSN engagement.

2.12 A CASE FOR A SURVEY OF RESPONSIBLE OSN ENGAGEMENT

The concern of responsible engagement of OSNs in industries such as healthcare can be found more than a decade ago where it was felt that the medical practitioner was left to personally negotiate online forums in the absence of any professional guidance or standards (Gusehl, Brendel and Brendel, 2009). Then again re-enforced later where if used responsibly and professionally OSN platforms could be used as a medium for interactive healthcare (Kotsilieris et al., 2017). And then from the perspective of brand development, again embracing the case for responsible OSN engagement (Yoganathan, Osburg and Bartikowski, 2021).

This holds equally for the financial services sector, where although the financial sector understands the power of OSNs to engage with and market its brand and image to all stakeholder, financial organisations are fully aware of mitigating the possible risks associated with irresponsible OSN behaviour. To this end many financial institutions employ strict compliance with their policies with regard to all online activities (Van den Berg and Struwig, 2020).

Whether it be the challenge of navigating the ethical implications of using a new communication platform or shortfalls in the judicial system as legislation regarding the implications of the new media platform as assessed and reviewed, the onus on the employee remains to engage with responsible caution on OSNs. Regarding the organisation’s governance framework regarding promoting responsible OSN engagement, the primary aim of this study is to understand the factors that influence and impact the behavioural traits of responsible usage of OSNs.

2.12.1 *The Levels of Responsible OSN Engagement within the organisation*

The first objective of this research is to identify factors that promote responsible engagement of OSN usage. This asks what constitutes and how does one gauge the levels of responsible engagement within the organisation?

Recent findings indicate that factors like the fear of missing out (FOMO) are positively correlated to OSN addiction which drives a higher frequency of engagement amongst users of more social applications, namely, Facebook, Instagram and Snapchat (Sheldon, Antony and Sykes, 2020). In another study, selfies related to loneliness and depression (Sheldon, Rauschnabel and Honeycutt, 2019) were dominated by the frequency of usage of the social applications Snapchat, Facebook, Twitter, and Instagram (Matthes *et al.*, 2020).

OSNs geared to direct and formal communication, such as Emails, SMS, WhatsApp, and BBM, provide seamless, instantaneous legal and business communication through mobile devices (Townley, 2019). Further studies demonstrated that the efficiency of WhatsApp usage by 455 participants in Northern Cyprus in the workplace boosted work performance due to expediency and convenience (Terkan and Celebi, 2020). Furthermore, the ever-present nature of WhatsApp allows immediate communication enabling virtual meetings to be conducted from anywhere, where users maintain the etiquette and behaviour appropriate to the group they belong to (Regina et al., 2017).

From a business perspective, higher frequency usage of business applications relative to frequency usage of social apps is associated with higher levels of responsible OSN engagement in the organisation.

OSN engagement within the organisation lends itself to using business applications for business communication, whether it be the exchange of business conversation, through documentation, formal, legal or through memos and setting up and monitoring organisation schedules such as meetings, organisational and project deadlines. As explored above, the popular platforms include Emails, SMS, WhatsApp and Skype. Product and service communication to clients would apply to YouTube and Twitter. Maintaining a business network of colleagues regarding organisational trends, skills availability and pedigree is suited to LinkedIn.

The use of more social based platforms such as Facebook, Facebook Messenger and Instagram, although they have business capabilities, lends itself to the addictive nature of FOMO, selfies and social conversation not associated with the organisation, which often may include gossip.

The broadcast applications Twitter and YouTube fall between business and social-orientated applications. They have been seen from the business side to increase visibility and online performance by up to 30%, whereas YouTube is primarily used for marketing and Twitter for customer communication (Ioanid and Scarlat, 2017). A further study showed that users engaging with YouTube seek a multifaceted range of services such as entertainment, information on products, services and news, thrill-seeking and social interaction (Antoniadis, Saprikis and Karteraki, 2018). Therefore, platforms such as YouTube, Twitter, and WhatsApp are often used in social and business contexts.

In gauging the levels of responsible OSN engagement, we can survey the usage frequency levels of business platforms relative to social-based platforms. The higher the self-reported levels of frequency usage engagement with business platforms to that of social platforms is observed as an indicator of higher levels of responsible usage.

2.13 THE RESEARCH GAP FROM THE LITERATURE REVIEW

From the outset of the literature review, a key factor when engaging in OSNs is promoting responsible online behaviour by employees.

In developing a conceptual framework, it is important to understand the perceptions of the organisation's current ethical climate concerning responsible online engagement. Simultaneously, it is crucial to gauge the actual frequency usage of the employees of the most popular and common OSNs to gauge the levels of responsible engagement. By surveying the self-reported engagement practices, behaviours and habits, their effect on the level of responsible online behaviour can be quantified. This can run in conjunction with surveying the effect of self-awareness and organisation awareness in driving responsible online behaviour. This opens a research gap as a need in both qualitative and quantitative knowledge for an observed effect influencing factors on responsible OSN engagement in the workplace to develop a governance framework.

2.13.1 *A Quantitative Gauge of factors influencing Responsible Behaviour*

In meeting the first objective, through critically reviewing the literature to identify factors that influence responsible and abusive OSN engagement within the organisation, the following three constructs that can be observed as exogenous[R5] variables on the effect and impact [R6]of the levels of responsible behaviour when engaging on OSNs derived in the literature review, namely:

- Online Self-Awareness.
- Online Privacy Literacy.
- Online Organisational Awareness.

The observed levels of responsible behaviour regarding the identified constructs with the actual surveyed usage of the most commonly used OSNs may offer an understanding of the effect and impact these constructs have as influencing factors on responsible behaviour. This will identify the key factors that should be included in developing a governance framework for an employee or any other stakeholder guidance for responsible OSN engagement.

Further literature review revealed several validated instruments that can be used and adapted to measure the identified constructs. This will enable meeting objective three to gauge the opinions and perceptions of a sample of employees from selected industries towards factors that influence responsible behaviour when engaging in OSNs.

Surveying online self-awareness can be gauged using the Cybersecurity Engagement Self-Efficacy Scale and the Self-Esteem Scale, meeting objective four, to gauge employees' awareness of psychological and external factors affected by manipulated impulsive behaviour, habits and OSN addiction on responsible OSN engagement.

To survey online privacy literacy using the online privacy literacy scale and mediated by the Security Behaviour Intentions Scale, meeting objective five, to gauge the perceived effect of the individual employee’s online privacy literacy and security intentions on responsible OSN engagement.

To survey the online organisational awareness using the ethical climate questionnaire, meeting objective six, to gauge the influence of the employee’s awareness of the ethical climate within the organisation on responsible OSN engagement.

2.13.2 *Observed Perceptions of Responsible OSN Engagement as Qualitative research*

As a phenomenon, in particular for those that fall in the Baby Boomer and X-Generations, the radical transformation in the change of how we now communicate using OSNs has introduced a myriad of behavioural traits in the way employees interact online with each other and with other stakeholders such as clients and suppliers within an organisation. The literature review has examined and developed various concepts associated with these interactive online behavioural traits when engaging in OSNs, from techno moral lag; nudging assisted brain hacking, mobile device attachment and separation anxiety, OSN addiction, self-esteem, self-efficacy, online privacy literacy and online security behavioural intentions, through to the organisational awareness of what the employee constitutes and perceives to be responsible and ethical conduct which the organisation subscribes to reflected in the ethical climate.

2.13.3 *The perceptions of behaviour and adherence to current governance in Responsible OSN engagement*

As discussed and presented in the literature review, these concepts have already been researched and examined more extensively than others. However, these concepts' underlying premise and effect may not be familiar to typical executive managers in the sectors selected for this research. To meet objective two, to explore through the use of interviews and a literature review the perceptions of behaviour and adherence to current government policies and guidelines of employee OSN engagement in the selected industries, the researcher thus sees the need to understand the perceptions and views through the eyes of the executive manager of the challenges of promoting and maintaining responsible OSN engagement by employees and other stakeholders. The key concepts would be to understand management’s view of the current governance and guidance regarding business transparency and responsible OSN engagement. Of key interest would be the executive manager’s perception of the frequency of use of OSNs, the level of online privacy literacy of employees and their intentions to protect the integrity of company information. Perceptions of employee behaviour would include the degree of perceived OSN addiction and cyberbullying by employees and whether, in the manager’s view and experience, this may have led to adverse effects within the organisation. Furthermore, what is the management's perception of the influence and awareness of the organisational and ethical climate on business transparency and OSN engagement?

CHAPTER 3 : RESEARCH METHODOLOGY

3.1 INTRODUCTION

This chapter explains the research methods employed for this study. The research gap is summarized and identified in the literature review as a lack of organizational control towards which executive management directs attention, motivates, and encourages employees to act responsibly when engaging on OSN platforms. This necessitates examining, gauging and analysing the influencing factors associated with responsible engagement. A deeper understanding of influencing factors associated with responsible engagement is key to the development of a governance framework.

A gauge of responsible usage and frequency engagement of OSNs within the industries of the target population is largely undefined. As discussed in the literature review, this enables meeting the following stated objectives.

Objectives two to six lead to a mixed-methods study to unravel the prevailing research question that encompasses the specified research question on page 26, namely:

> *“What are the factors in the development of a conceptual governance framework as part of the work culture reflected in the organisation’s ethical climate to promote responsible OSN engagement by employees in the financial and healthcare services industry, to mitigate the perceived loss of control through the notion of radical transparency?”*

3.1.1 *A Mixed Methodology Approach*

The research under taken was a mixed methodology. A combination of qualitative and quantitative data produces a more comprehensive analysis by complementing, corroborating or supporting findings (Creswell and Creswell, 2018). The reasoning behind the mixed methodology is that neither qualitative nor quantitative methods on their own would be able to unravel both the social adoption and technological complexities of a social phenomenon that is redefining how we as humans interact with each other.

From an organisational perspective the stakeholders / population groups considered around OSN platform engagement is at both a macro and micro scale namely; executive management and employees respectively. To understand the challenge of directing attention, motivating, and encouraging employees to act responsibly when engaging on OSN platforms cannot be easily quantified and requires a qualitative analysis. Whereas the actual online behaviour of employees when engaging with OSN platforms can be gauged using a quantitative study (Almeida, Queirós, & Faria, 2017). By identifying commonalities in both qualitative and quantitative methodologies, each of the methods adapt to different sources of data making a distinct contribution through a shared set of influencing factors in OSN platform engagement behaviour, recognising the complexity and diverse perspectives of the research undertaken (Creamer, 2022). In addition, the development of a balanced conceptual governance framework from the perspective of the challenges facing executive management as well as gauging the online behaviour necessitates both a qualitative and quantitative study.

3.1.1.1 A Qualitative Study to Gain an Insight into the Perceptions of Behaviour

The purpose of this research approach is first to perform a qualitative study to meet the second objective through the use of interviews to gain an insight into the perceptions of behaviour and adherence to current governance, policies and guidelines of employee OSN engagement in the selected industries. To gain an in-depth view of the extent of the notion of “loss of control” by management and a management perspective of a governance framework and policies in addressing the perception of radical transparency, a code of ethics towards business privacy and confidentially and customer privacy. Further is an analysis of the employee’s perceptions of their rights to freedom of speech within the context of the professional code of conduct of the organisation.

3.1.1.2 A Quantitative Study to Gauge OSN usage

Furthermore, the purpose of this research approach is secondly to conduct an online quantitative instrument to gauge the actual OSN usage against the identified factors that may influence the conduct of OSN engagement. As part of this instrument is used in gauging the competency of online privacy literacy, online security self-efficacy, general self-esteem, the behavioural patterns towards online security, the propensity of OSN addiction and texting habits of the organisation's stakeholders within the context of the perceived ethical climate by the employee of the organisation.

3.2 RESEARCH APPROACH

In approaching the research, Saunders research onion found in chapter 4 of Research Methods for Business Students was considered and investigated (Saunders, Lewis and Thornhill, 2019). Four layers were considered important for this research study: 1.) research philosophy, 2.) strategy, 3.) method and 4.) data collection and analysis, as seen in Figure 3.1 below.

The research philosophy is a combined approach of positivism and realism from the mixed methods approach (Saunders and Tosey, 2013). Returning to the prevailing research question, the research study seeks to understand the influencing factors to mitigate the perceived loss of control through the notion of radical transparency from the perspective of management. The research was exploratory sequential design. This approach was used to adjust the validated scales for gauging behaviour, where needed for OSN engagement and to adapt where required for a South African context. In addition, this approach allowed the two sets of findings to confirm or generalise the qualitative findings.

3.2.1.1 Meeting the Research Objectives

The notion of loss of control is based on the perceptions of management. Investigating the perceptions of management on responsible employee OSN engagement meets objective two by gaining insight into how management understands the influences researched in the literature review toward responsible engagement. The researcher seeks to contrast management perceptions with empirical findings of actual OSN engagement within employee demographics meeting objective three whilst gauging the employee awareness of the influences set out in objectives four, five and six. This combined philosophy is suited to an inductive qualitative study in combination with a quantitative deductive study of in-depth interviews with management with an online survey of a cross-section of stakeholders. The insight from the qualitative study with the empirical findings of OSN usage and awareness levels of employees is used in developing a governance framework as part of objective seven.

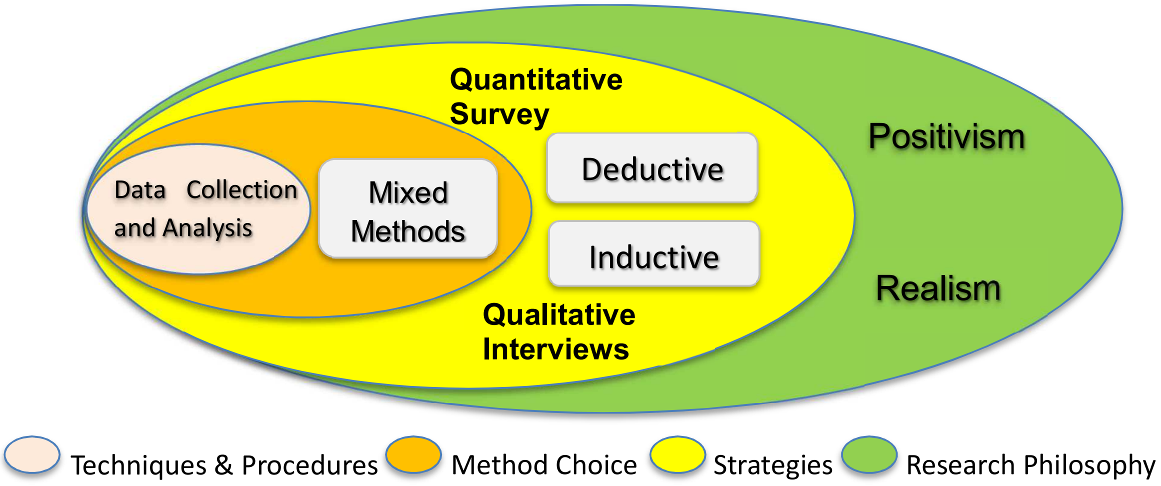


Figure 3.1 Customised Research Onion

Adapted from Research Methods for Business Students (Saunders, Lewis and Thornhill, 2019).

3.2.1.2 The Reason for the Selected Industries

The reason for the selection of organisations in the financial and healthcare sectors is that the confidentiality of client information and the susceptibility to misinformation is of paramount importance (Kumar and Devi, 2014; Chou et al., 2017; Braun and Eklund, 2019; Brashier and Schacter, 2020; Kogan, Moskowitz and Niessner, 2020).

In April 2020 McKinsey & Company conducted a survey of North American consumers regarding the protection and maintenance of confidentiality of data from hacking, breaches and not subscribing to regulations. A risk practice report revealed that consumers from this survey are most comfortable sharing data with providers in the healthcare and financial services. Both industries scored 44 out of 100 which was double or more than any other industries. This further corroborates the selected organisations within the healthcare and financial services for the research in this study (Anant et al., 2020).

The study is not concerned with the disparate business functions of the two sectors. The study is concerned, with the stringent need, by both sectors to protect and maintain the privacy and confidentiality of clients and patients as a minimum benchmark. Working in the financial and healthcare sectors in South Africa for more than three decades, the researcher is familiar with knowledge in these sectors. The researcher's relationships with executives and managers in these sectors will assist in accessing appropriate personnel with whom the researcher is not familiar, to avoid any possible bias.

3.2.1.3 Target Population

The target population of this qualitative study is the entire workforce within divisions of the management participating in the qualitative study of the five commercial organisations selected (500 employees in each on average) from the healthcare and financial sectors.

The target population will comprise of approximately 2500 employees. The researcher has been involved with and consulted concerning Information Technology in the financial services and health sector and is thus familiar with the business models, structures, compliance, governance and business ethics of these sectors. The researcher feels that this knowledge base and experience are crucial to the interpretation and analysis of the research.

3.2.2 *The Unit of Analysis*

The unit of analysis is a stakeholder employed and represents the organisation in their capacities ranging from executive to casual or contract workers. As discussed in the research problem, all employees connected and engaging in the phenomena of OSNs are the organisation's mouthpiece. This presents ethical and moral considerations concerning what information is shared to whom. The researcher first established the demographic of the employee and the frequency of the OSNs engaged with. Secondly, the research sought insight into the employee’s ethical and moral approach to representing themselves and the organisation through OSNs.

3.2.3 *The Sample*

For the qualitative research, the intention was to utilise a purposive sample of appropriate financial services and healthcare sector organisations. A series of in-depth interviews with relevant employees (senior management) was conducted. The selection of participants depended on the willingness and availability of the participants involved and is thus a purposeful convenient sample.

For the quantitative research, the researcher conducted an online survey that was sent to all targeted employees of the same organisations used in the qualitative research.

The online survey utilised the online tool, google forms, to reach and gather data from the sample through the web, smart phone or tablet. Further details on the sample and motivation thereof are discussed in the sections regarding qualitative and quantitative research methodologies.

3.2.4 *Objectives*

Meeting objectives two to six of the research is achieved through the research methodology as follows:

3.2.5 *Objective two*

To complete a qualitative study to explore through a literature review and interviews the perceptions of behaviour and adherence to current governance, policies and guidelines of employee OSN engagement in the selected industries.

3.2.5.1 Objectives three to six

- To use an instrument to gauge the opinions and perceptions of a sample of employees from selected industries towards factors that influence responsible behaviour when engaging in OSNs (objective three).
- To gauge employees' levels of awareness towards psychological and external factors affected by manipulated impulsive behaviour, habits, and OSN addiction on responsible OSN engagement (objective four).
- This instrument will further gauge the perceived effect of individual employees' online privacy literacy and security intentions on responsible OSN engagement (objective five).
- To gauge the perceived influence of the employees' awareness of the ethical climate within the organisation on responsible OSN engagement (objective six).

3.3 THE QUALITATIVE RESEARCH

3.3.1 *Motivation for Phenomenological Research*

The main purpose of this phenomenological research is to delve into the reality of the participants' understanding of their experiences and feelings in having to learn new protocols in communication.

3.3.1.1 OSNs as a Phenomenon

From the employer's perspective, a qualitative methodology was conducted as a series of interviews with the executive or senior management. The purpose was to achieve an in-depth perspective from the employer on the phenomenon of OSNs within the organisation regarding the ongoing representation of each organisation’s identity, company values, culture and conduct of both employer and employee within engaged social networking communities.

The concept of an OSN was first academically defined by Boyd et al. (2007), which implies that, for most executives in the financial and health sectors who are predominantly members of the Baby Boomers, X-Generation and Net-Generation, the concept or existence of an OSN can be seen as a phenomenon that is a novel experience.

3.3.1.2 The Lived Experience of the key Stakeholders

Introducing radical transparency through the facilitation of OSNs as a paradigm shift in communication and knowledge transfer is a frightening deviation from the traditionally structured communications methods that appear in the social networks that have been the norm in the 20th century. It is living through the experience as a forced adaption of this paradigm shift through the technological phenomenon of OSN that the researcher sees as key to the development of a governance and policies framework to facilitate a mindset change in the world of commerce and enterprise.

3.3.1.3 In-depth Appreciation of the change in Conduct and Behaviour

The statistical results and analysis from a quantitative study can go a long way in understanding critical facts in the adaptation of the business environment of radical transparency. However, the researcher tried to understand the business executive's in-depth apprehension about the required change of conduct and behaviour in communication, whether on a personal or business level.

It is the steps and measures taken by the executive to embrace this new technological communication platform by conquering the fear of adapting the change from the well-established 20th-century mindset of communication to that of adopting radical transparency by embracing the technology of the OSN platform in the 21st century, that the researcher sought to reveal through a phenomenological qualitative study.

3.3.2 *Core Characteristics that define Qualitative Research*

In qualitative research, the researcher reviews the common core characteristics and combinations thereof which are considered to be pertinent to the research taken from publications of leading researchers and authors, among other things (Creswell, 2013a; Groenewald, 2004; Roller and Lavrakas, 2015;Tracy, 2013). Next discussed are core characteristics the researcher took into account during the qualitative study. However, as seen later in the findings, aspects such as an additional data source to the recorded and transcribed primary data of the interview did not materialise.

3.3.3 *The Instrument*

> *"the researcher is the primary instrument for data collection and analysis"* (Merriam and Tisdell, 2016).

The Instrument in this qualitative research was the researcher. The researcher interpreted and analysed the data. Qualitative research explores the research constructs as the participants divulge information. Thus, the researcher must conduct interviews with the participants. "*The mind and body of a qualitative researcher literally serve as research instruments – absorbing, sifting through, and interpreting the world through observation, participation, and interviewing*" (Tracy, 2013: 3). The researcher and the participant effectively jointly own the "research space" during the interview process (Roller and Lavrakas, 2015). As information is revealed through the researcher's engagement with the participant, the researcher needs to be able to ask redirected questions and steer the conversation to maximize the exploration of all aspects of the discussion while staying focus on the research questions.

3.3.4 *The Data Sources*

The predominant data source would be that gathered through in-depth interviews with participants from the population sample. The nature of the qualitative methodology revealed some additional data sources in terms of participants as the research process evolved.

3.3.4.1 The Data Analysis and Reflexivity

The aim was to determine themes and clusters using horizonalisation (Leech and Onwuegbuzie, 2008), thus developing a conceptual framework for the government policies that enhance the corporation's interests whilst maintaining the ethics associated with the employees' right to freedom of speech and privacy. The researcher was able to look with sincerity and transparency, reflecting on the influence of the interviewee's own knowledge and interpretation of the information collected during the analysis thereof (Creswell, 2013a; Roller and Lavrakas, 2015; S. J. Tracy, 2010). To avoid bias of the researcher as the instrument of the qualitative research, the researcher applied phenomenological reduction in the form of epoché commonly translated as a "suspension of judgement" or more commonly known as bracketing as recently applied in phenomenological research in the use of social media support (Ruiz and Stadtlander, 2015) and the evaluation of character traits of company executives (CEOs) (Nyukorong and Quisenberry, 2016). It is noted, however, that researcher's knowledge and background regarding the phenomenological research of the subject matter remains embedded and possibly beyond his control. Vigilance concerning this factor may be required rather than trying to attain detached objectivity. This should not imply that the hermeneutic approach to phenomenological research should be given less reverence but instead follow the approach Heidegger and Gadamer (Gadamer, 2006) advocated and not be restricted by prescribed methodology but take note of one's biases in interpretation (Emiliussen *et al.*, 2021).

3.3.4.2 The Importance of Meaning and the Participants' Meanings

The researcher derived meaning by looking at the effect of the familiarity between the researcher and interviewee concerning any form of bias by either party (Patton, 2002) and the context and language used (Roller and Lavrakas, 2015). The researcher needed to concentrate on the meaning of the information provided by the participant (Creswell, 2013a).

3.3.4.3 The Evolving Process of Emergence

It is evident from the literature that the qualitative methodology is an evolving emergent process (Creswell, 2013a). This means that the researcher used supplementary sources in the form of documentation, media or additional participants who emerged during the research process (Patton, 2002; Roller and Lavrakas, 2015)..

3.3.4.4 The Full Picture a Holistic Approach

The researcher used multiple observations with the aim of gaining a holistic perspective of the phenomenon (Creswell, 2013a; Roller and Lavrakas, 2015).

3.3.5 *The Interview Process*

3.3.5.1 The Purposeful Convenience Sample

The researcher selected to use a purposeful convenience sample. This type of sample is extensively used when conducting qualitative research methods as it enables the researcher to select a sample with a wealth of information and experience through living the experience of the phenomena being researched (Patton, 2002). It was envisioned that a sample size of 12–30 from at least four financial services and healthcare sector organisations would yield a saturated consistency of themes and clusters to develop the essence (essential invariant structure) of the phenomena of OSNs in the workplace. Where, as discussed in the literature, the essence is and describes the phenomena (Dahlberg, 2006). The researcher gained insights and manifestations of the apprehensions of both the positive and negative impact on the organisation, such as having to manage the exposure of the organisation’s activities through social media and the exposure of the behaviour of the organisation’s employees both through the conduct of business as well private communication on OSNs at all times. A purposeful convenience sample ensured the optimal use of a limited selection of available willing participants who are not only knowledgeable and experienced in needing to manage the phenomenon of OSNs in their organisations but were also able to articulate their experiences and opinions (Palinkas *et al.*, 2013).

3.3.5.2 The Setting of the Interviews

A series of interviews were conducted with senior management at appointed times and at the convenience of the participants, whether at their place of work or in a more casual environment. A key element of the setting was an environment with as little distraction as possible and where a clear voice recording of the interview was obtained. The researcher felt it imperative to capture the tone and intensity of the participant's conversation and answers. The researcher was seeking to establish the current apprehensions or confidence of senior management in tackling the perceived problem found in the literature on the control (Lucero, Allen and Elzweig, 2013) or lack thereof (Zerfass, Fink and Linke, 2011; Trinkle and Crossler, 2014) of company information dissemination and general conduct at all times by stakeholders particularly employees engaging in OSNs. A direct self-assured as opposed to a hesitant apprehensive answer to a question or issue tells a different story regarding underlying confidence as opposed to scepticism regarding the ability of the participant's organisation to either cope or embrace stakeholder engagement on OSNs. This is a significant distinction between the tangible, measured outcomes from quantitative research as opposed to an imperceptible interpretation used in the qualitative research approach to understand the confidence levels concerning stakeholders' inability to restrain the use of OSNs.

3.3.5.3 Interview Guide and Themes to be discussed

In meeting objective two, the researcher developed a research guide similar to questionnaire guides used in the literature (Prat, 2014) that was continually refined and evolved after each interview. The key themes discussed in the literature review included, but were not limited to:

- 'Loss of control' over the engagement of OSNs by employees (Linke and Zerfass, 2013a).
- The approach to radical business transparency (Park and Blenkinsopp, 2011; Tapscott and Ticoll, 2012; Heemsbergen, 2016).
- Governance and policies concerning employee engagement on OSNs (Macnamara, 2011).
- Ethics and a moral code regarding business transparency through OSNs (Carroll, Brown and Buchholtz, 2018).
- Ethics towards the employee's right to freedom of speech and privacy as a company representative (Debatin *et al.*, 2009; O'Connor and Schmidt, 2015; Watson and Lopiano, 2016).

- Ethics and governance towards business partners and customers' right to privacy concerning data gathering (Carnegie Mellon University, 2016; Grimes, 2016; Orcutt, 2016a).
- The threat of employee workstations being compromised through phishing and botnets, and other malicious malware and computer viruses through the exposure of employee engagement on OSNs (Acohido and Swartz, 2008; OECD, 2008; Acohido, 2010; UNODC, 2013).
- The researcher’s classification of information dissemination, namely Spin Doctors, Whistle-Blowers, Pillow Talk and Careless Whispers from informal preliminary research (Dijck and Poell, 2013; Wolfe *et al.*, 2014; A Big Brother Watch report, 2015; Scott, 2016).

3.3.5.4 Interview Questions

In every interview, the notion of radical transparency in the context of OSN engagement was introduced and then discussed regarding the perceived problem found in the literature of loss or lack of control by the executive of an organisation.

The terms online privacy literacy, online self-awareness and organisational awareness regarding ethical climate were explained and discussed.

In keeping each interview consistent, the researcher referred to a skeleton of questions ensuring that the subject matter associated with objectives one to objective six was adequately addressed. The following questions were addressed during each interview.

1. *What is the current state of Governance regarding business transparency, particularly radical transparency, when engaging on OSN platforms?*
2. *What is the competency level of online privacy literacy perceived by management regarding both employees and management?*
    a) Do you feel they can protect themselves from piracy invasion? What is the competency level in privacy settings, and do they understand and read the terms and conditions when subscribing to an OSN platform?
    b) Do you feel that they can protect themselves from malware and virus

invasion? What are the competency levels in detecting malicious software invasion and antivirus software?

3. *Is OSN addiction a factor concerning business transparency and using OSNs within your organisation?*
   a) Are you, as a manager, aware of OSN addiction?
   b) Have you ever noticed the symptoms of OSN addiction?

4. *How do you feel the ethical climate of the organisation impacts responsible OSN engagement concerning appropriate business transparency regarding:*
   a) The organisation drives values.
   b) Professional adherence to industry conduct and regulations.
   c) The personal morals and ethics of the employees.
   d) The instrumental values are associated with running a profitable and successful organisation.

5. *What are the perceptions and experiences of the employees concerning the guidance of responsible OSN usage stipulated in the organisation's policies and procedures?*
   a) From your experience, do the employees in the organisations understand the need to adhere, understand and follow the organisation's policies and procedures when engaging in OSNs?
   b) From your experience, do the organisation's employees understand the implications of a privacy and confidentiality breach and the notion of radical transparency?

6. *How effective do you believe the organisation's procedures and policies regarding governance are in tackling the notion echoed in the literature of "Loss of Control" regarding OSN engagement within the organisation?*

7. *What effect do you believe generational or gender differences or educational qualifications have when it comes to responsible OSN engagement concerning:*
   a) Online privacy literacy competency.
   b) Online self-efficacy and self-esteem
   c) The ethical and moral approach of employees.

3.3.6 *Qualitative Data Analysis*

3.3.6.1 The Coding Process.

The qualitative data in the form of transcribed interviews were coded using a combination of the traditional Grounded theory pioneered by Glaser and Strauss (Glaser and Strauss, 1967) and Flexible coding (Constantinou, Georgiou and Perdikogianni, 2017; Deterding and Waters, 2021). The Grounded theory is in line with the inductive approach mentioned in 1.2. The theory is renowned as a theory qualitative researchers adapt to suit their research and achieve their objectives; however, its iterative, recursive practice in developing themes and categories is still relevant to this research study (Charmaz, 2008; Belgrave and Seide, 2019). This approach, together with the use of modern Qualitative Data Analysis Software (QDAS) in combination with the coding of modern office suite software applications such as Microsoft Office (Lapelle, 2004; Ose, 2016; Watkins, 2017), will enable the researcher to capitalize on features of the software through analytic coding examining respondent attributes of a derived data set of codes, categories and themes across all transcripts (Deterding and Waters, 2021).

3.3.6.2 Grounded Theory Process

Grounded Theory is generally known as a flexible approach to deriving new theories through the reductive process of recursive and iterative real-world data analysis, such as transcribed interviews into themes. Objective two of this research is to explore through a literature review and interviews the perceptions of behaviour and adherence to current governance, policies and guidelines of employee OSN engagement in the selected industries. To achieve this objective, data in the form of interview transcripts were collected and analysed through open coding (Corbin and Strauss, 1990) or what by other researchers is referred to as initial coding (Bryant and Charmaz, 2012). Codes derived were then used in the further collection of interview transcripts until code and theme saturation was achieved. Further analysis and code reduction into themes were then achieved using axial coding and selective coding, a process that reclusively iterated between open, axial and selective coding until core themes were developed, leading to the interpretation of the qualitative findings. This iterative process ensures that all abstraction retains an alignment with the data. The Grounded

Theory Process is regarded as a tried and tested robust methodology that is used to enter into and understand the interviewee's world thus achieving objective two.

The coding process used for this qualitative research is illustrated below in Figure 3.2, followed by a brief description as it was used in this research.

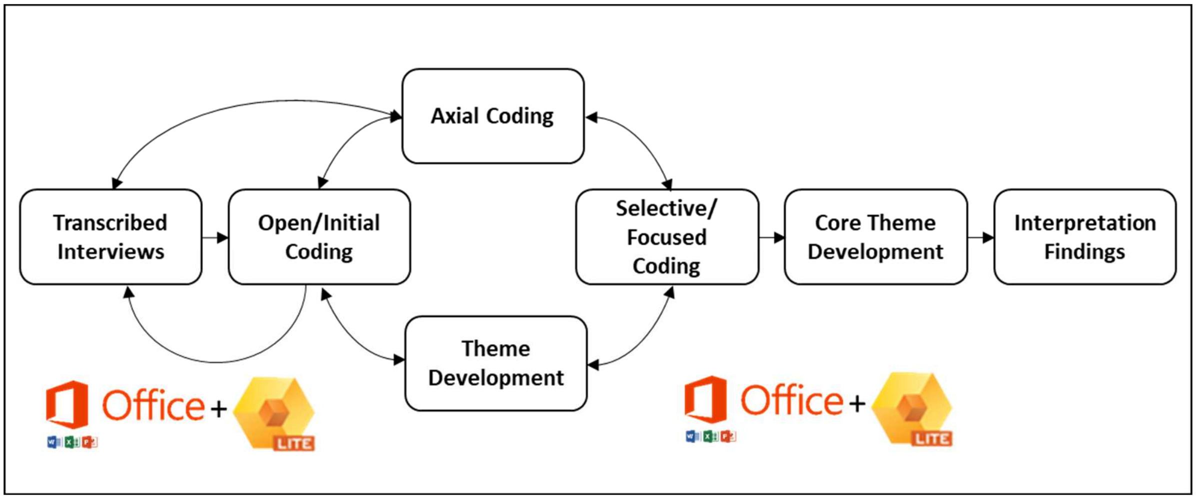


Figure 3.2 The process for Qualitative Research Coding

Adapted from Williams and Moser (2019)

3.3.6.3 Open/Initial Coding (Initial Analysis of Text)

Aggregating concepts and phenomena analyse the interview text data into discrete themes. Once a theme emerges, it is then assigned a code. This results in a list of distinguishing codes and categories supported by code notes explaining the codes.

3.3.6.4 Axial Coding

This is the second level of coding, where the open coding themes are further refined and aligned. At this level, the transition from open coding to axial coding results in affiliating connections between the codes and distinct thematic categories derived from the open coding. The codes are now aggregated into categories (Williams and Moser, 2019). The thematic categories are viewed as axes with their associated properties related to subcategories. Axial coding effectively reconstructs the lines of data of the transcribed interviews extracted through open coding (Charmaz, 2008).

3.3.6.5 Selective/Focused Coding

This is the third level of coding, where the detailed extraction and analysis of open and axial coding are transformed to a higher level of abstraction. This is done by selecting consistently recurrent codes and focusing on now-defined categories from the axial coding into one core category (Glaser, 2016).

3.3.7 *Limitations of the Qualitative Research*

3.3.7.1 Convenience Sample Bias.

The selection of financial services, healthcare sector organisations and key stakeholders would be limited to those willing to participate in this research and provide the necessary consent and approval.

3.3.7.2 Potential Bias in Answers and Interpretation thereof.

The researcher has been involved in the commercial use of OSNs in a business capacity. There is thus, the danger that the researcher may have strong views, opinions and biases on OSNs. To mitigate any possible influences of such biases, the researcher endeavoured to exercise strict personal bracketing during the interview process.

3.3.7.3 Volume of Data

The process of in-depth interviews and the analysis thereof is time-consuming and constrained to the availability of respondents, thus impacting the selection and size of the sample.

3.3.7.4 Qualitative Research may not be Statistically Representative.

Qualitative research tends to be an interpretation of perspective which makes it difficult to measure.

3.4 THE QUANTITATIVE RESEARCH

3.4.1 *Purpose of the Online Survey*

The purpose of the quantitative research is to establish OSN usage while simultaneously gauging the influences set out in objectives three, four, five and six developed and categorised in the literature review regarding responsible OSN engagement. Objective three seeks to gauge and understand the influence of the associated demographics of the employee regarding an industry, gender, generation and qualification. Objectives four, five and six seek to gauge and understand the influence through the validation of six scales of the levels of awareness regarding online self-awareness (objective four), online privacy literacy (objective five) and organisational awareness (objective six) of the employee towards responsible OSN engagement.

3.4.2 *The Constructs with Associated Objectives*

The constructs from the literature review establish what it is that we want to know. Three constructs from the literature review examine employees' perception and awareness of their moral and ethical obligations regarding representation and information dissemination to their employer or organisation. First, the constructs examine the employee’s notion of the individual right to privacy within the context of responsible OSN engagement (Haraty and Massalkhy, 2013; Kokolakis, 2017; Richey, Gonibeed and Ravishankar, 2018; Tsay-Vogel, Shanahan and Signorielli, 2018) namely, online self-awareness, online privacy literacy and Organisational awareness.

The following variables on the above constructs were examined:

- Online social network usage.
- Online privacy literacy and security behaviour intentions.
- Online social network addiction.
- Online privacy self-efficacy.
- Self-esteem scale.
- Ethical climate.

As per the literature review, this leads to meeting objectives three, four, five and six to be gauged regarding measurement scales.

3.4.3 *Gauging Online Self-Awareness*

As discussed in the literature review, the construct of online self-awareness within the context of the Cybersecurity Engagement Self-Efficacy Scale and the Self-Esteem Scale can influence responsible behaviour with OSN engagement.

3.4.4 *Cybersecurity Engagement Self-Efficacy Scale*

Based on the work on self-efficacy by Albert Bandura (Bandura, 1998), the researcher used the scales for General Self-Efficacy Scaletyh (GSE) (Schwarzer and Jerusalem, 2013) and Cybersecurity Engagement and Self-Efficacy Scale (CESES) (Amo, L.C. et al., 2016). In addition, questions were tailored for the OPLIS, SeBIS Scale, BSMAS and Online Social Network Usage questions.

3.4.5 *Self-Esteem Scale*

To gauge self-esteem, the Rosenberg self-esteem scale (RSES) was used. The RSES has been used with the BSMAS in recent studies where both OSN and Internet addiction are associated with self-esteem (Hawi and Samaha, 2016; Rosenberg, M. 1979; Rosenberg, M. 1965).

3.4.6 *Gauging Online Privacy Literacy*

The speed at which the technological platform of OSNs has been integrated into society questions the idea of online privacy literacy of this technology. In perusing this work, Philipp Masur, Doris Teutsch and Sabine Trepte have developed an online privacy literacy scale (OPLIS) to measure individuals' and organisations' online privacy literacy.

To gauge the awareness of individual’s rights to the privacy of their personal information when engaging in OSNs, the researcher used the validated online privacy literacy Scale (OPLIS) (Trepte *et al.*, 2015; Philipp K. Masur, Teutsch and Trepte, 2017). OPLIS examined the awareness and perceptions of the individual’s rights to protecting their private data and their knowledge regarding functional and technical aspects of their online privacy (Correia and Compeau, 2017).

There were five groups of questions comprising four or five questions. Twenty-five aspects of an individual’s rights to online privacy and data protection strategies and practice were tested. Each of twenty-five questions would be scored with one point if the correct answer was provided. During the pilot study of the questionnaire, the aims in the final development of the OPLIS were followed (Trepte *et al.*, 2015). Results from the pilot study of the questionnaire found that questions covering all aspects of the OPLIS were best styled, keeping part with the OPLIS format of the multiple-choice test type or true-false items regarding the efficiency of the general design of the questions. This type of layout lends itself to an efficient process of analysis. In keeping with the OPLIS format, the option “Not Sure” was presented for both the multiple-choice test and true-false questions allowing the respondent to avoid guessing. The consequence of reputational risk through a lack of technical knowledge and data protection strategies in the context of OSN engagement can be severe. Uncertainty is thus regarded as unfavourable regarding online privacy literacy, leaving an assessment of zero points for either an incorrect answer or if the respondent’s answer is ‘Not Sure’. This test-type approach enabled the researcher to determine a score of online privacy literacy competency for each respondent.

OPLIS is adapted and divided into the following five themes:

Theme	**Items**
Self-reported knowledge about institutional data collection practices through the use of OSNs.	Four questions
Technical aspects	Four questions
Data protection techniques	Five questions
Password protection	Four questions
Data law protection	Four questions (Adapted to PoPi)

In the context of this research, online privacy is defined as

> *“one’s ability to control the release of personally identifiable data in the context of institutional practices* (Park, 2015)*.”*

It follows from this definition that online privacy literacy can then be defined as the ability, an individual’s level of skill or level of expertise to determine how much of their personal data they are happy to share with an agent, whether it be a national, commercial or social entity through the engagement of an OSN. In determining how much personal data an individual is happy to share with an agent through an OSN, the individual's data privacy protection needs to be measured regarding 1.) Their awareness of exposure to the amount and type of data agents collected, and 2.) Their functional and technical competency levels of online privacy techniques and settings.

To gauge the employee's awareness of their rights to the privacy of their personal information when engaging in OSNs as discussed in the research methodology, the researcher adapted an online privacy literacy scale (OPLIS) (Trepte *et al.*, 2015; Philipp K Masur, Teutsch and Trepte, 2017a, 2017b). OPLIS aims to gauge the awareness and perceptions of the individual's rights to protect their private data and their knowledge regarding functional and technical aspects of their online privacy (Correia and Compeau, 2017).

As part of a lengthy questionnaire, it was necessary to reorganize and adapt the standard format of OPLIS, ensuring that all relevant aspects of the technical aspects and data protection aspects of online privacy literacy were covered. Technical aspects included understanding the purpose and use of terms and concepts when browsing the Internet, such as cache, cookies, browsing history, firewall and a Trojan virus. During the pilot study in the development and refinement of the quantitative instrument, several participants suggested including the concept of a Virtual Private Network (VPN). To assess the respondent's data protection strategies for password creation and use, OPLIS built-in two questions that covered four best practice techniques. As a result, OPLIS uses three questions to cover five data protection strategies when surfing the Internet. After several iterations of the questionnaire during the pilot study, it emerged that these best practice password creation techniques were best analysed through four and five questions for data protection strategies when surfing the Internet.

Information about data collection practices using OSNs by institutions like the USA's National Security Agency was found irrelevant within the South African context. Therefore, it was decided to adapt the OPLIS questions on institutional data collection practices through OSNs to that of an identifiable and the time a topical company such as Facebook. Likewise, questions on the knowledge of data protection law were adapted to questions on the South African POPI act in contrast to the OPLIS questions directed towards German and European data protection law.

3.4.7 *Gauging Online Security Behavioural Intentions*

Aligned with online privacy literacy the Security Behaviour Intentions Scale (SeBIS) (Egelman and Peer, 2015) was developed by Egelman and Peer and is a 16-item instrument scored on a 5-point Likert scale that gauges awareness through the intended behaviour about online privacy when engaging online with OSNs This scale was later reduced to four items (Egelman, Harbach and Peer, 2016), each corresponding following original themes.

3.4.7.1 Privacy Policies and Settings

Legal privacy policies, terms of service, and default privacy settings are arguably designed to rather legally protect the companies that provide an OSN platform service than the end user by using indirect legal terminology to exploit private data (Hartzog, 2017, 2018). The researcher added six questions to address the often-inattentive behavioural intentions of the user when reading and accepting privacy policies and terms of service of OSN platforms. The questions were adapted from a study by Obar and Oeldorf-Hirsch which examines the time taken to read the privacy policies and terms of service of OSN platforms (Obar and Oeldorf-Hirsch, 2018).

Scales are one of the most cost-effective proxies for observing human behaviour. As emphasized by DeVellis, scales

> *"are intended to measure elusive phenomena that cannot be observed directly."* (Devellis, 2017:105)

The security behaviour intentions scale (SeBIS) is used to gauge employees' privacy and security behaviours when engaging on OSN platforms, whether web-based or accessed on a desktop, notebook, or mobile device. As discussed in the research methodology, the researcher adopts the 16-item security behaviour intentions scale(SeBIS) (Egelman and Peer, 2015) developed by Egelman and Peer to gauge a users' self-assessment of their adherence to OSN online security and privacy advice or organizational procedures and policies. The SeBIS is divided into four themes, namely:

1. Password Generation: This asks the respondent about their vigilance in securing passwords that are unlikely to be cracked or hacked.
2. Device Securement: This asks the respondent how vigilant they are

regarding securing the device used OSN engagement, whether it be a desktop, notebook or mobile device. Typically, this will involve the lock of the device when not in use through a password, pin or biometrics.

3. Proactive Awareness is linked to awareness when using a web application such as OSN. This would typically question whether the respondent is vigilant to the web application URL they are engaged with or about to engage with.
4. Updating: This asks the respondent how vigilant they are regarding updating their software applications with the latest security patches.

Further analysis takes validation of this scale and the reduction from 16 items to 4 items, each relating to one of the four themes above (Egelman, Harbach and Peer, 2016). However, for this research, the researcher felt that the importance of measuring online security behavioural intentions warranted the inclusion of all the original 16 items.

For efficiency and ease on a mobile device and in keeping with the style of the questionnaire, the researcher adapted the 16 items into four groups of questions matching the themes and the items validated in the reduced scale, as seen in Table 3.1

Table 3.1 Four Themes of SeBIS

Theme	Theme Question	Item Validating
Password Generation	My Passwords…	Using Password phrases
Device Securement	My Device / Computer…	Vigilance about locking mobile with a PIN or Screen lock
Proactive Awareness	I will look at the URL of a website...	Awareness of a Phishing URL
Updating	When it comes to software updates, I...	Vigilant about maintaining the latest software updates

Each group of questions starts with the theme, which then assesses the various behaviours around that theme examined in the SeBIS. In keeping consistent in frequency usage assessment of the top 16 OSNs and assessment of the BSMAS frequency scale for OSN addiction and with that of the frequency scale of that of texting habits, it was appropriate to the gauge of responsible behavioural intent regarding the frequency of current, past and future intended behaviour. Therefore, the SeBIS responses were gauged on the frequency scale: Never (1), Rarely (2), Sometimes (3), Often (4) and Always (5).

3.4.7.1.1 Privacy Policies and Settings

Six items adapted from a study which examines the time taken to read the privacy policies and terms of service of OSN platforms (Obar and Oeldorf-Hirsch, 2018) were added to the SeBIS using the same frequency scale: Never (1), Rarely (2), Sometimes (3), Often (4), and Always (5),

Table 3.2 and Table 3.3

Table 3.2 Introducing Privacy Policies to SeBIS

Obar and Oeldorf-Hirsch:	**Research Questionnaire:**
	Regarding Social Network Apps Privacy Policies I...
I agree to privacy policies/Terms of Service agreements without reading them	*… agree to without reading them*
I read privacy policies/Terms of Service agreements thoroughly	*… read thoroughly*
I review privacy policies/Terms of Service agreements when notified that there have been updates	*… review if I'm notified of an update*

Table 3.3 Introducing OSN Apps Privacy Settings to SeBIS

Obar and Oeldorf-Hirsch	**Research Questionnaire:**
	Regarding Social Network Apps Privacy Settings I...

It is normal to sign up for websites/apps without reading the privacy policies	*… accept the default setting*
I’ve got nothing to hide	*… don’t care about them*
Most people don’t read privacy policies	*… go with the flow, as most people do*

SeBIS was adapted to consist of six themes, four from work done by Egelman and Peer and two from Obar and Oeldorf-Hirsch namely:

Theme	**Items**
Proactive Awareness	Awareness of phishing URLs
Updating	Vigilant about maintaining the latest software updates
Password Generation	Using password phrases
Device Securement	Vigilant about locking mobile with a PIN or screen lock
Privacy Policies	Reading and accepting privacy policies
Privacy Settings	Accepting default privacy settings

3.4.8 *Gauging Organisational Awareness*

Organisational awareness was gauged within the context of the Victor and Cullen ECQ. The ECQ assesses five themes through 26 questions fundamental to an organisation's ethical well-being amongst stakeholders. In addition, the topical issue of the invasion of privacy of personal information introduced in the workplace by OSN platforms prompted the researcher to add a sixth theme of three additional items regarding data privacy. This resulted in a total of 29 questions namely:

Theme	**Items**
Caring	Seven questions
Law and Code	Four questions
Rules	Four questions
Instrumentalism	Seven questions

Independence	Four questions
Privacy	Three questions

3.4.9 *Gauging OSN Addiction*

As discussed in the literature review, OSN addiction is increasingly becoming a factor affecting the inappropriate and irresponsible engagement of OSNs. Recent studies in OSN addiction at Bergen University have resulted in the Bergen social media addiction scale (BSMAS) (Andreassen, Pallesen and Griffiths, 2017), which is based on the previously validated Bergen Facebook Addiction Scale (Andreassen et al., 2012). This scale uses six addictive criteria: salience, tolerance, euphoria, withdrawal, relapse and conflict. This is in line with a study on addiction to social networking sites where Turel and Serenko consider conflict, withdrawal, relapse and reinstatement, and salience as factors associated with addictive behaviour (Turel and Serenko, 2012).

3.4.9.1 Texting Habits

While conducting the pilot study of the scales in the questionnaire, the researcher discussed OSN behaviour with the pilot respondents. Feedback questions often revolved around texting habits. This prompted the researcher for further feedback on what the pilot respondents regarded as concerning texting habits.

The researcher was initially reluctant to add additional items to the already lengthy questionnaire; however, it was decided to include the six items on texting habits.

Three factors were identified in texting habits. The first was the employee’s habits in personal vigilance, the second was the emotional state and lack of self-conscious control whilst conversing via texting, and the third was deliberate conscious high-risk texting behaviour.

Three themes of two items each were added with regards to texting habits namely, the employee’s habits in personal vigilance, the emotional state and lack of self-conscious control whilst texting, and deliberate conscious high-risk texting behaviour.

Two items addressed the first theme: accidentally sending a text to the wrong recipient and texting a contentious or provocative message without consciously thinking about the consequences.

The second theme was addressed with two items, the first by asking the respondent if they text whilst still angry, addressing the risk of an emotional knee-jerk reactive text. The second item asked the respondent whether they text under the influence, where one's loss of self-conscious inhibition may result in an emotional outcry or impulsive risqué message, image or video.

Two items addressed the third theme addressing deliberate conscious high-risk texting behaviour. The first asked the respondent how often they text whilst driving, and the second asked how often they message risqué texts, images or videos.

This resulted in six additional questions namely:

Theme	**Items**
Personal vigilance	Two questions
Emotional and self-conscious control	Two questions
Conscious high-risk texting behaviour	Two questions

3.4.10 *The Quantitative Research Sample*

The sample needs to fall within the same framework to complement, corroborate and support the quantitative research results and the results of the qualitative data. The sample to be surveyed would be employees of the organisations selected or similar and must have access to a OSN platforms.

3.4.11 *Statistical Mediation Analysis*

The model uses statistical mediation analysis to gauge how the dependent variable *X* in the form of OSN usage with demographics such as generation (age) and gender affect the dependent variable *Y,* Organisational response to appropriate OSN behaviour. The influence of awareness regarding (1) organisational ethics, (2) online privacy literacy and behavioural intentions, and (3) self-efficacy and self-esteem may act as a mediating factor, *M*, in how appropriate responsible behaviour is perceived when engaging with OSN platforms. Regression analysis in the form of a simple steps approach is used to determine the effect of *M* as the mediator of *X* on *Y*.

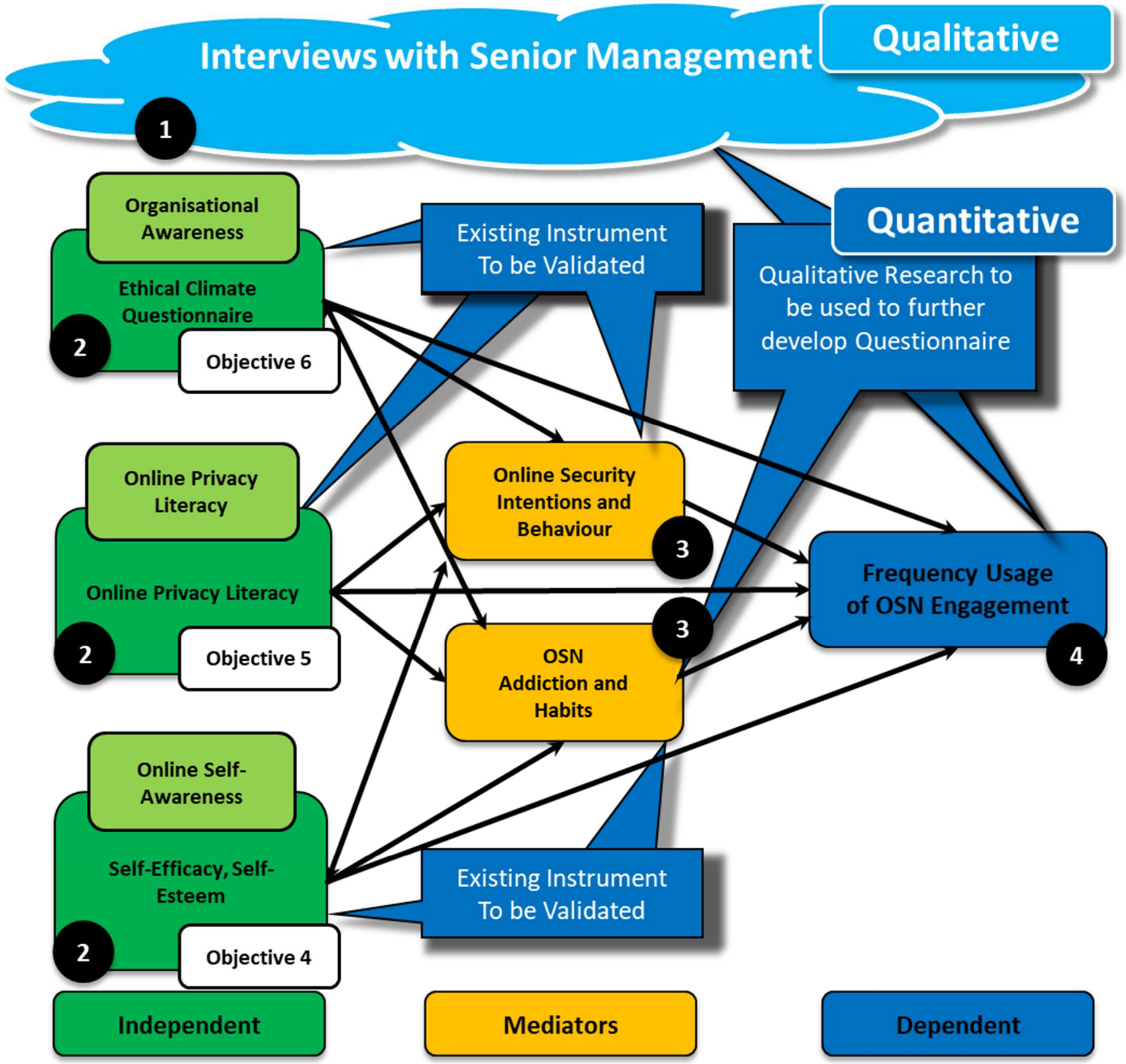

Interviews with Senior Management
Qualitative
1
Organisational Awareness
Ethical Climate Questionnaire
2
Objective 6
Existing Instrument To be Validated
Quantitative
Qualitative Research to be used to further develop Questionnaire
Online Privacy Literacy
Online Privacy Literacy
2
Objective 5
Online Security Intentions and Behaviour
3
Frequency Usage of OSN Engagement
3
OSN Addiction and Habits
4
Online Self-Awareness
Self-Efficacy, Self-Esteem
2
Objective 4
Existing Instrument To be Validated
Independent
Mediators
Dependent

Figure 3.3 The Path Flow of the Research Model

3.4.12 *3.5.12 Moderation Analysis*

While mediation analysis may be used to establish how the causal effect of organisation, online privacy and self-awareness determines the effect *X* has on *Y*, the demographic generational and gender factors may be now introduced as moderating variables *W* depicting the types of people and the circumstances having been born either before or into an era of technology computing, the Internet, smartphones and

Online Social networks. Thus being classified as digital immigrants versus digital natives (Prensky, 2001) and then as digital natives as part of either the Net Generation (Tapscott, 1998, 2009) or the iGeneration (Rosen, 2010) may have a moderating effect on the mediating variables *M* which will, in turn, affect *Y*. The same may apply to gender and then to a combination of gender and generation. It is envisioned that the research model will follow the paths as in Figure 3.4.

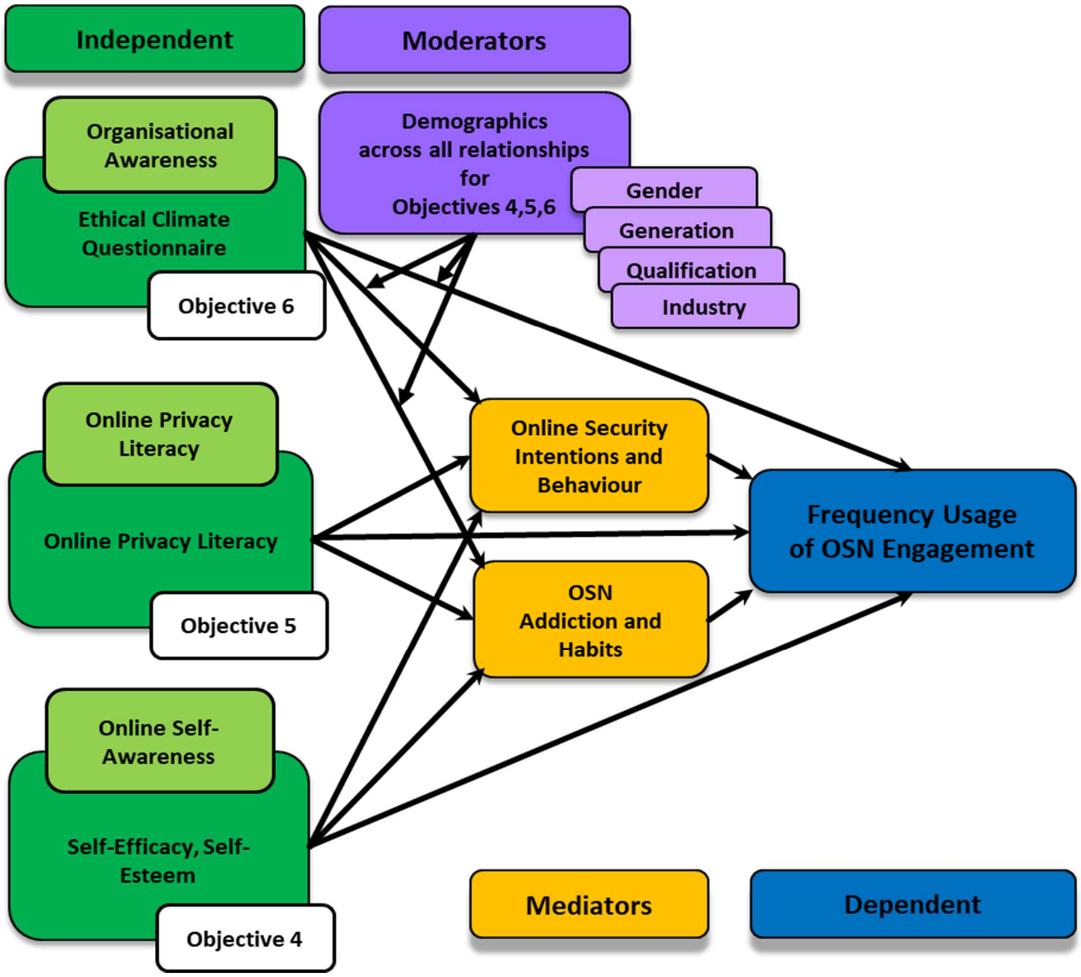


Figure 3.4 Moderation introduced in the Research Model

3.4.13 *The Development of the Organisational Response Instrument*

The successful design of a questionnaire is often far more complex than initially anticipated. To achieve a consistent and accurate answer to the questions explored in the research involves careful thought, reviewing themes and trends in similarly done the research, consulting with experts, doing qualitative research, whether preliminary or as part of a mixed-methods approach and an investigation of the state-of-the-art and research methods. In the literature reviewed, questionnaire design is sometimes referred to as an "art" (Synodinos, 2003). However, this "art" should rigorously follow a scientific method (Saris and Gallhofer, 2007). A process of understanding the outcomes, meaning and characteristics of the researcher's questions should be part of the development of the questionnaire. An iterative approach of reviewing and refining the questions and flow regarding question order with pilot respondents and experts in the field of the research and research methodology is outlined in Figure 3.5 and Figure 3.6

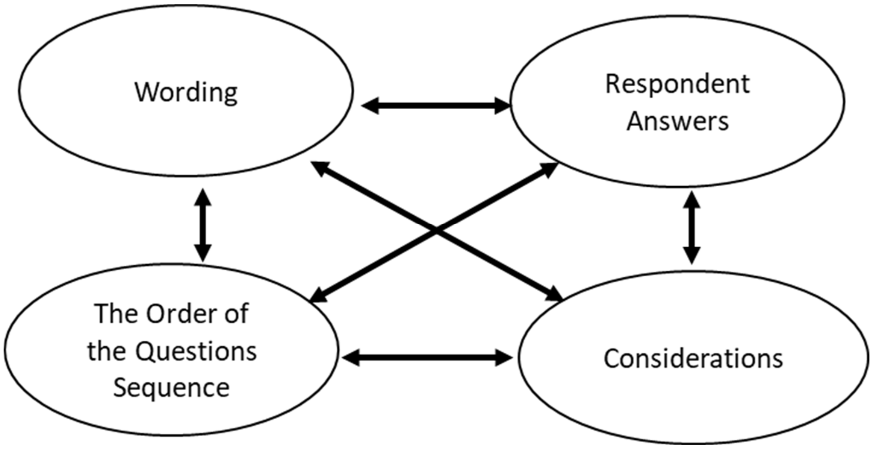


Figure 3.5 Refine and Tweak Questionnaire

Source (Synodinos, 2003)

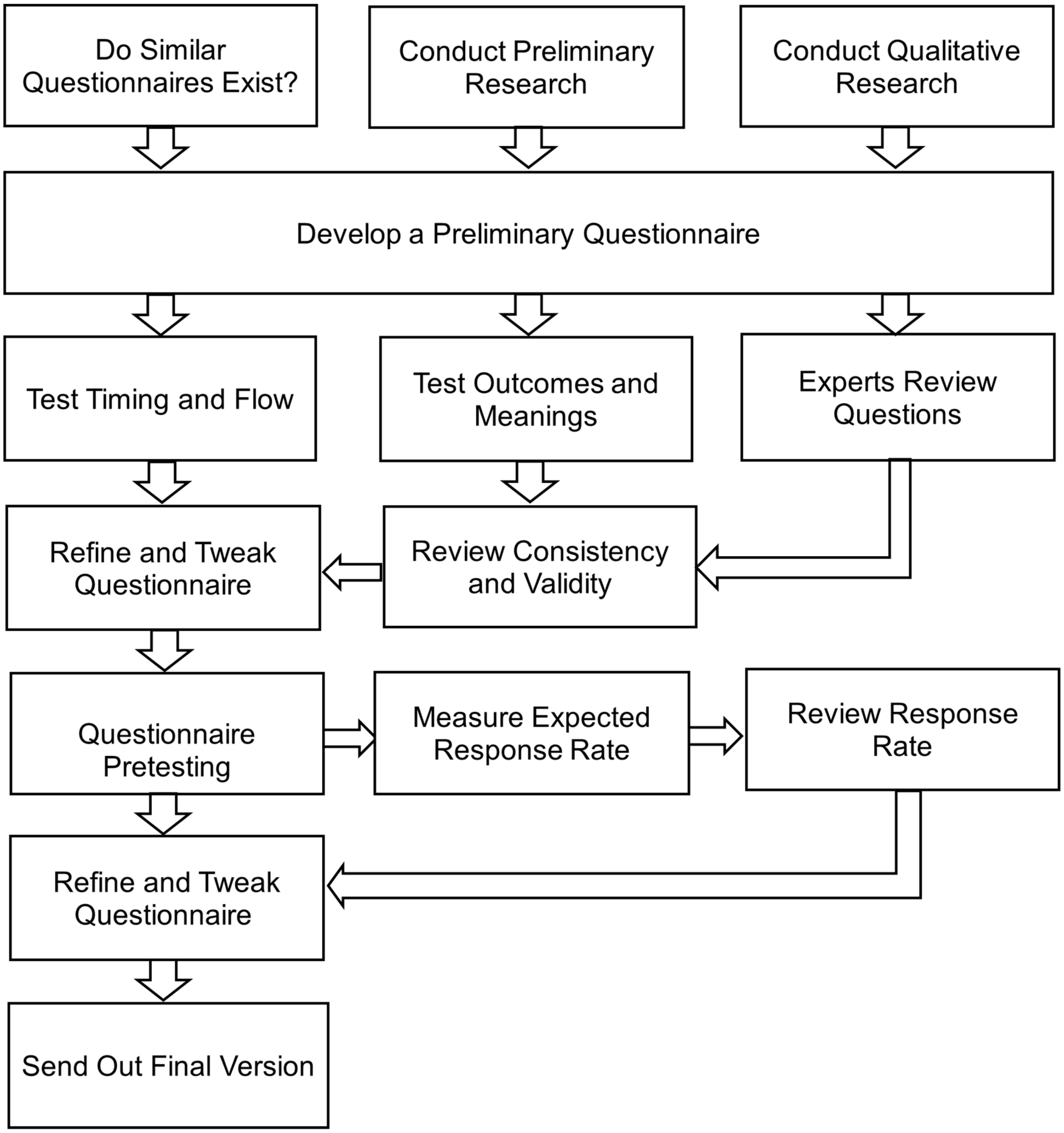

Do Similar Questionnaires Exist?
Conduct Preliminary Research
Conduct Qualitative Research
Develop a Preliminary Questionnaire
Test Timing and Flow
Test Outcomes and Meanings
Experts Review Questions
Refine and Tweak Questionnaire
Review Consistency and Validity
Questionnaire Pretesting
Measure Expected Response Rate
Review Response Rate
Refine and Tweak Questionnaire
Send Out Final Version

Figure 3.6 The Workflow for the Questionnaire Design

The approach to the questionnaire design is based on a mix of articles reviewed in the literature (Devellis, 2003; Synodinos, 2003; Barry *et al.*, 2011).

3.4.14 *Wording*

The wording of a question needs to be carefully considered regarding being clear, concise and accurate using a familiar word structure to the average user. During the iterative process of refining and tweaking the questionnaire, the literature suggests the researcher make use of focus groups or interviews with a pre-selection sample of respondents to see how they interpret and answer the questions (Tourangeau, Rips and Rasinski, 2000:23). Opportunity must be made during the qualitative research to gain insight in the respondents' approach to constructing of ethics and personal moral code.

The sequence of the mixed-methods research must be carefully planned. Although qualitative research precedes quantitative research, a preliminary questionnaire should be in place before the qualitative research is conducted. It is important from the wording of the questions that all respondents interpret and understand what is being asked as the same. It is vital to communicate in plain, understandable language rather than with an erudite style. It is crucial that the difference between subtle nuances evident to the researcher not be seen as a repeated question in different words to the respondent.

Questions must be objective, and “loaded” or “leading” questions must be avoided. For an accurate answer, a question must only contain a theme or issue. In addition, all questions need to be culturally reduced as far as possible. This may be particularly relevant in the cultural diversity of South Africa, especially when talking about ethics and moral code.

3.4.15 *Respondent Answers*

The questionnaire uses a closed-ended scale, as discussed earlier. Open-ended questions can be more onerous and seem like “hard work” to the respondent resulting in nebulous and vague answers that were not used. However, particularly in the questionnaire pretesting phase, an open-ended question provided insight into responses that were converted to closed-ended questions. In addition, the discussion of responses with field and subject experts benefitted from refining and tweaking the questionnaire.

3.4.16 *The Order of the Questions*

The researcher uses a question sequence that follows the standard introduction, body and characteristics (Synodinos, 2003). The question of a person’s individual right to freedom of speech and that of being a representative as an employee of an organisation, together with the ethics of business transparency, can be regarded as sensitive. The research construct is a key factor when designing the sequence of questions of the questionnaire. In tackling the complexities of ethical and moral behaviour, the researcher considered Babbie’s (2014: 282) approach to question sequence, “The safest solution is sensitivity to the problem”

Questions part of the questionnaire's introduction are critical in influencing the respondent’s enthusiasm and willingness to proceed and complete the survey. The introduction should engage the respondent with the theme of the questionnaire without being intrusive or burdensome (Krosnick and Stanley, 2010).

Before a rapport with the respondents has been established, the first set of questions in a questionnaire is possibly susceptible to not being taken seriously. The aim is thus to start with closed-ended demographic questions, both regarding personal details such as age, gender etc., and simple factual questions, such as what OSN’s the respondent engages with, which are likely to be answered accurately. Although it is suggested that background demographics be left to the end of a questionnaire (Krosnick and Stanley, 2010; Babbie, 2014), in this case, limiting personal demographics to three questions and then proceeding with the more enticing subject of the frequency use of OSN platforms will maintain interest and encourage the respondents to proceed in the questionnaire. Once led to the main body of the questionnaire, the respondent will have developed a rapport and feeling committed to the questionnaire (Babbie, 2014). They are now more likely to answer more sensitive questions and are willing to complete the survey by answering questions about their ethical behaviour and conduct when engaging with OSN platforms. Here the researcher maintains the use of close-ended responses easing any anxiety relating to the sensitivity of personal ethics and a moral code.

The software analysis tool IBM SPSS Statistics follows the three-step process suggested in ‘*Adventures in Social Research: Data Analysis Using IBM SPSS Statistics*’ to analyse the collected data (Babbie, Wagner III and Zaino, 2015).

3.4.17 *Further Considerations*

When considering the target population, the questionnaire design must make all questions applicable. Where questions are not answered by respondents, if appropriate, branching is applied to the next relevant question. The ascetics and professional appearance of the questionnaire may determine whether a respondent is enticed to partake.

3.4.18 *The Rating Scale*

The personal view on ethics may leave the participant in a quandary between personal freedom and privacy and what they perceive to be their duty and in the company's interest. This perception can be tenuous and contentious at times and is subject to personal interpretation of the context this quandary may present itself. As discussed by Krosnick and Stanley in “Questionnaire and questionnaire design” (Krosnick and Stanley, 2010), a dichotomous option (e.g. “agree” or “don’t agree”) is inappropriate in that one of the key points of this study is to provide a governance framework for grey areas in the ethics towards behaviour and conduct in engaging on OSNs. A trichotomous scale (e.g. “agree,” “maybe,” “don’t agree”) may again pose a problem to the respondent in that, although their view is not neutral, the respondent may not entirely agree or disagree, i.e. prefers to favour a lighter or darker shade of a grey area in what they perceive as appropriate behaviour or conduct on how they engage on their selected OSN platform.

The nature of ethical conduct or behaviour is a paradoxical abstraction that exists in the physical world defined by conventional systems of black or white, wrong or right. However, it simultaneously exists in the mental world where definitive statements such as absolutely wrong or right are at times difficult to reach. As eloquently stated by Feldman (1998) from the Routledge Encyclopaedia of Philosophy in the article “Epistemology and ethics.”

> *“Among ethicists who reject naturalistic definitions, on the basis of the open question argument or for other reasons, some contend that moral predicates do not have descriptive meaning and are instead used to express approval or disapproval or to prescribe or proscribe behaviour. On this view, known as non-cognitivism, evaluative sentences do not say anything that can*

> *be true or false. Rather, they express the speaker’s attitude (moral indignation or approbation).”* (Feldman, 1998).

It is thus pertinent when considering the respondents' mental representations (Krosnick and Stanley, 2010) as explored by Rockwell (2013) of the construct to use a scale that offers the opportunity to express a more fine-grained perception than that of an absolute value. Price and van der Walt (2013), researching attitudes toward South African business ethics, used a five-point Likert scale based on a previously commonly used ‘‘Attitudes Towards Business Ethics Questionnaire’’ (ATBEQ) in six similar research studies across four continents (Price and van der Walt, 2013). Attitudes towards whistleblowing disclosure (Park, Blenkinsopp and Park, 2014) also used a five-point Likert scale. In light of this research and for possible comparison purposes, the researcher used a five-point Likert scale in the questionnaire design.

3.4.19 *Reliability and Consistency of scales*

The quantitative instruments used are existing, adapted or newly developed scales.

The reliability and consistency of scales was evaluated as follows:

- IBM SPSS (Version 25) was used to assess Cronbach’s α.
- Cronbach’s α was used to test the internal consistency of appropriate existing and adapted scales.
- Cronbach’s α was used to verify the degree to which all the items measure the same notion or construct and its connected inter-relatedness with other items in the instrument.
- The validity or construct validity was used to assess to what extent the underlying construct is aligned to or represented by the observed data.
- Correlational analysis of the observed data was used to test the construct validity of constructs defined in the literature review.

3.4.20 *Factor Analysis and the Regression Analysis*

The researcher performed an exploratory factor analysis (EFA) to explore underlying constructs and concepts leading to sub-scale development. This was followed by a confirmatory factor analysis (CFA) to ascertain potential underlying factors or components to reduce the number of items on each scale to a more manageable number. A CFA is a multivariate technique that theoretically looks at how to analyse the structure of the interrelationship of a multiplicity of variables from questionnaire responses to identify underlying dimensions known as factors. The purpose of this research of using factor analysis is data summarisation and data reduction through a methodical interpretation of a multiplicity of correlated measures. The aim is to use factor analysis to present the data in a more orderly, structured and reduced form of the observed variables. This will lead to identifying measurable underlying patterns of item clusters aligned with the theoretical concepts from the literature in the development of better manageable instruments.

As a primary step in the scale development, principal component analysis (PCA) was used to reduce the data-set dimensionality through a covariance analysis between factors.

The reduction of variables may be seen to compromise accuracy; however, the benefit in exploring, analysing and visualising reduced data sets of both the maximum number and nature of factors enables the identification and alignment of factors with the constructs derived in the study. This justifies the trade-off of compromising accuracy for simplicity (Hair *et al.*, 2014).

The resulting data are effectively linear combinations of the original data but with the highest variance in the data (Jolliffe, 2002; Jollife and Cadima, 2016). This assisted in determining a goodness-of-fit of the self-reported observed data to the latent variable data. For further validation of the model was made using the Goodness-of-Fit Index (GFI), the Normed Fit Index (NFI), the Comparative Fit Index (CFI), and the Adjusted Goodness-of-Fit Index (AGFI). In addition, the Ratio of Chi-Square to Degrees of Freedom (CMIN / df) and the Root Mean Square Error of Approximation (RMSEA) were measured for model fit.

Regression analysis using Hayes's PROCESS macro on IBM SPSS (Version 25) was employed to test the various linear paths in conjunction with PCA and was employed to measure and analyse the relationships between observed and latent variables (Rajab, MatJafri and Lim, 2013).

3.4.21 *Limitations of an Online Survey*

The researcher uses an online survey to distribute the instrument for data collection for the data for the quantitative study.

In conducting an online survey, the researcher considers at least two possible limitations associated with online surveys (Patten and Perrin, 2015): 1. Coverage error; and 2. Nonresponse Errors (Baumgartner, 2013).

3.4.21.1 Coverage Error

To complete the questionnaire survey, the respondent must have online access. Employees of the companies/organisations being researched are given online access to the survey.

3.4.21.2 Nonresponse Errors

The respondent must be willing to complete an online survey. From an ethical standpoint, the researcher cannot force or prejudice any respondent to complete the questionnaire, let alone reveal the identity of such an employee to the employer (company/organisation). The researcher must exercise strict anonymity. Recent research by the Pew Research Center (2015) has revealed that the difference between a full sample and a web sample is negligible (Patten and Perrin, 2015).

3.4.22 *Limitations of the Quantitative Research*

The rights to freedom of speech within the workplace and corporate transparency viewed by the employee could be seen as sensitive and contentious. Even with the assurance of anonymity, employees may view an online survey with suspicion and not answer truthfully for fear of stakeholder and management conspiracy.

3.4.23 *Ethical considerations regarding the interviewees (Qualitative) and online survey participants (Quantitative)*

The outcome of this research is to develop a general framework for governance and ethics in the corporate for the use and restrictions by employees for OSNs. Of significance is the size, type and industry of the organisations researched. The actual identities of both the interviewees and names of the corporates have no bearing on the research findings and thus remain anonymous, maintaining the confidentiality of both the individuals interviewed and the organisations. The resulting transcripts and recordings of the research are only shared with trusted sources of the research, namely the researcher, supervisors and transcribers, and on completion of the analysis, all recordings and transcripts are secured in storage for a period of five years and then destroyed.

It is key that anonymity from the quantitative survey is maintained. The online surveys are done without revealing the participant. All electronic results are stored using a password only the researcher and the supervisor can access. This must be explained and agreed to by the stakeholders upfront.

CHAPTER 4 : RESEARCH FINDINGS

4.1 INTRODUCTION

Chapter 4 presents the findings from the qualitative and quantitative research that was used to analyse the effect of online social networks on Radical Business Transparency considering the ethical climate in the organisation with the view of a Conceptual Governance Framework.

The qualitative findings were conducted using 29 in-depth interviews by executive management in the health and financial sectors are analysed and presented. The process and the ground rules in conducting the interviews is explained. This is followed by discussing the use of axial, selective and focused coding to analyse the interviews. This leads to the emergence and development of three themes of behavioural intent discussed in the findings.

The quantitative analysis will then follow this as a result of the findings from the Online Survey conducted by employees within the same organisations. These finding include a statistical demographic analysis of OSN usage and a scale reliability assessment as well as a group difference identification of the existing scales. This followed by a factor analysis which results in OSN platform categorisation. Finally, a regression analysis is conducted.

The ethnicity and gender mix of respondents of both the qualitative and quantitate study was a fair representation of the South African business population.

4.2 QUALITATIVE STUDY

4.2.1 *The Purposeful Convenience Sample Process*

The researcher relied on personal relationships in both these industries regarding access to the appropriate personnel. This enabled the selection of candidates with knowledge and access to the organisation's online strategies and governance regarding the use of OSN platforms. Access to personnel using OSN platforms for public communication and marketing purposes was arranged. Candidates involved in environments with dire consequences of the irresponsible use of OSN platforms such as hospital theatres or trauma units were selected.

4.2.2 *The Interview Process*

The following section describes the process of analysing the qualitative data. The researcher conducted approximately 25 hours of comprehensive interviews in the designated health and financial sectors. Of the 31 interviews that were held, 29 were selected as appropriate for the analysis of the study. Two were inappropriate and thus discarded because the interviewees veered from the topic by avoiding relating their views to their organisation and the industry, simply focusing on their personal social engagement on OSN platforms. This resulted in approximately 25 hours of recorded interview time that was used.

Interviews were deemed appropriate if the following conditions were met:

1. They fell into the appropriate industry, namely the health and financial sectors.
2. The interviewees understood the purpose of the research and the research topic.
3. The interviewees were deemed to be giving honest and true opinions about the study.
4. The interviewees kept to the research topic and offered meaningful and useful responses regarding the topic to their organisation and the industrial sectors in which the study was undertaken.

4.2.3 *Ground Rules of the Interview process*

To address the sensitivity surrounding some past negative repercussions having occurred either intentional or unintentional through the engagement of OSNs by organisational stakeholders, it was made clear to the interviewee that all interviews would retain full anonymity concerning the identity of the interviewees and their organisation.

The following was clearly stated to the interviewees at the commencement of each interview.

- The recording of the interview and contents thereof would remain anonymous, and the interview recording would only be heard and reviewed by the researcher and the transcriber.
- The direct transcription of the interview would only be read and reviewed by the researcher, the researcher's supervisor(s) and the transcriber.
- The interviewee would at any time have access to the interview recording and transcription if they so desired.
- All transcriptions will follow the process of being coded into appropriate themes and would then be anonymised regarding the name and personal identification of the interviewees.
- The coded themes will then be combined with those of other coded themes from the other interviews to establish general organisational and industry perspectives.

As shown in Table 4.1 there were 29 out of 31 interviews that successfully met the criteria above. Interviews were selected using the researcher's previous

Table 4.1 Profile of Interviewees of Qualitative Findings (2018)

#	Month 2018	Management Level	Industry	Number of employees	Province	Generation
1	Aug	CEO	Health	200	Gauteng	X-Gen
2	Sep	CFO	Health	200	Gauteng	X-Gen
3	Sep	Manager	Health	200	Gauteng	Millennial
4	Sep	Director	Health	200	Gauteng	Baby Boomer
5	Sep	Manager	Health	200	Gauteng	Millennial
6	Sep	Director	Health	200	Gauteng	X-Gen
7	Oct	CIO	Health	17800	Gauteng	X-Gen
8	Oct	Regional Director	Health	6161	Gauteng	X-Gen
9	Oct	CEO	Health	17800	Gauteng	Baby Boomer
10	Oct	Regional Director	Health	4721	Gauteng	X-Gen
11	Oct	CEO	Health	1200	Gauteng	X-Gen
12	Oct	Manager	Health	6161	Gauteng	X-Gen
13	Oct	Manager	Health	6161	Gauteng	X-Gen
14	Oct	Manager	Health	6161	Gauteng	Millennial
15	Oct	Manager	Health	6161	Gauteng	X-Gen
16	Oct	Manager	Health	6010	KZN	X-Gen
17	Oct	Regional Director	Health	6010	KZN	X-Gen
18	Oct	Manager	Health	6010	KZN	X-Gen
19	Oct	Manager	Health	6010	KZN	X-Gen
20	Oct	Manager	Health	6010	KZN	X-Gen
21	Oct	COO	Health	1200	Gauteng	X-Gen
22	Nov	Director	Financial	10	Gauteng	X-Gen
23	Nov	CEO	Financial	10	Gauteng	Baby Boomer
24	Nov	CEO	Financial	100	Gauteng	X-Gen
25	Nov	Director Communications	Health	17800	Gauteng	X-Gen
26	Nov	Divisional Head	Financial	100	Gauteng	X-Gen

Table 4.1 Cont. Profile of Interviewees of Qualitative Findings (2019*)*

#	Month 2019	Management Level	Industry	Number of employees	Province	Generation
27	Jan	Chairman	Financial	12	Gauteng	X-Gen
28	Feb	Director Communications	Health	1500	Gauteng	Millennial
29	Feb	CIO	Financial	500	Gauteng	X-Gen

4.2.4 *The Analysis Process*

The researcher analysed the interviews using the following phased approach:

Interview 1

- Took notes during the original face-to-face interview.
- Open / Initial Coding
- Listened to the recording and took notes of possible themes and codes while reading the transcriptions. Creating notes and extracting quotes of relevance using comment markup in Microsoft word. Each extracted word or sentence was assigned an appropriate code.

Interviews 2 - 6

- Took notes during the original face-to-face interviews.
- Open / Initial Coding
  - Listening to the recording and taking notes of possible themes and codes while reading the transcriptions. Creating notes and extracting quotes of relevance using comment markup in Microsoft word. Each extracted word or sentence was assigned an appropriate code. Codes with the associated text were aggregated in a spreadsheet.
- Axial Coding
  - Conducted a rereading of the transcriptions and coded relevant passages from the full transcriptions, cross-checking previous notes and quotes extracted in this reading.

Interviews 7 -15

- Using themes and coded derived from interviews 1 – 6.

The open/initial and axial coding process was repeated with the transcriptions of interviews 1- 6.

- Imported the analysis and themes from interviews 1 – 15 into the software package QDA lite and recoded this into themes and with reworked and refined codes.

<u>Interviews 16 – 29</u>

- At this stage, clear themes based on codes emerged from interviews 7-15. It was important to abide by the interview structure of questions; however, there was an emphasis on what was emerging as dominant codes and themes.
- The open/initial and axial coding process was repeated with the transcriptions of interviews 16- 21.
- Imported the analysis and themes from interviews 1 – 15 into the software package QDA lite and recoded this into themes and new codes.
- Imported the analysis and themes into the software package QDA lite and recoded this into themes and new codes.
- All personal and company details from the analysis and themes were removed.
- Cross-checked the original notes and codes with the resultant QDA lite coding to check the frequency and recurrence of themes and codes.
- Aligned the findings to the proposed constructs in meeting the research objectives.

4.2.5 *Initial and Open Codes Derived from the Interviews*

The researcher did an initial scan of the transcripts extracting paragraphs, sentences and words into five initial broad codes identified in the first and subsequent five interview scripts, namely:

1) General view of OSNs
2) Behaviour towards OSN engagement Online Security
3) Online Security
4) OSN engagement within the Organisation
5) Ethical Behaviour of OSN engagement

From these initial codes, a total further 27 open codes emerged within the initial codes as listed in Figure 4.1.

Essential to the effectiveness initial and open coding was considering thematic fragments and coalescing concepts identified during data collection in an organized and systematic way. Prior to using qualitative research software programs, organizing data for open coding required a multifaceted research skill set.

4.2.6 *Axial Coding*

The next level of coding can be identified as axial coding. As opposed to initial and open coding, which focuses on gathering data under emergent themes, axial coding identifies dominant occurrences, merges similar codes and, in some cases, realigns codes. Here, relationships between the open codes are streamlined under four distinct thematic categories: Online Behaviour Intention, Online behaviour Awareness, Online Security and Organisational Online Ethics in preparation for selective and focused coding. For example, codes such as “Confidentiality and privacy of information” and “Artificial Intelligence (AI) and deep learning” are now in the context of the transcribed interviews realigned from the initial code “Ethical Behaviour of OSN engagement” to “Online Security.”

4.2.7 *Selective and Focused coding*

Selective coding integrates codes from thematic categories refined in axial coding into meaningful, cohesive expressions. “Selective coding continues the axial coding at a higher level of abstraction [through] actions that lead to an elaboration or formulation of the story of the case” (Flick, 2009, p. 310). Some codes, such as “Social media addiction”, are retained as a distinct expression throughout the cyclical coding process.

The coding process of initial, open, axial, and selective coding is recursive and cyclical, allowing the researcher to repeatedly reanalyse both the original and reduced data using data reduction.

4.2.8 *Theme Emergence and Development*

These focused dominant expressions from the selective coding process are encapsulated into a theme. In the case of this research, the following themes related to OSN engagement emerged: Personal online behaviour, Personal Online Privacy and Organisational Behaviour.

Each of the emergent three themes are concerned with an awareness of the employee’s intended behaviour when engaging with OSNs regarding personal, privacy and an organisational perspective. The core theme emanating from the coded analysis emerges as “Behavioural Intent Awareness.”

4.2.9 *Qualitative Findings*

This is a story predominantly of those belonging to the X-Generation adapting to and coming to terms with the emergence of the phenomena of online social networks. Except for six of the 29 interviews, all the interviewees were from the X-Generation, i.e. those born between 1963 and 1980. This would mean that the oldest X-Generation first started using a mobile device at the age of thirty, and the youngest were in their early teens. Although exposed to what the researcher regards as the earliest social network, namely email, the oldest X-Generation would have experienced the emergence of OSNs in their early forties and the youngest X-Generation in their early thirties.

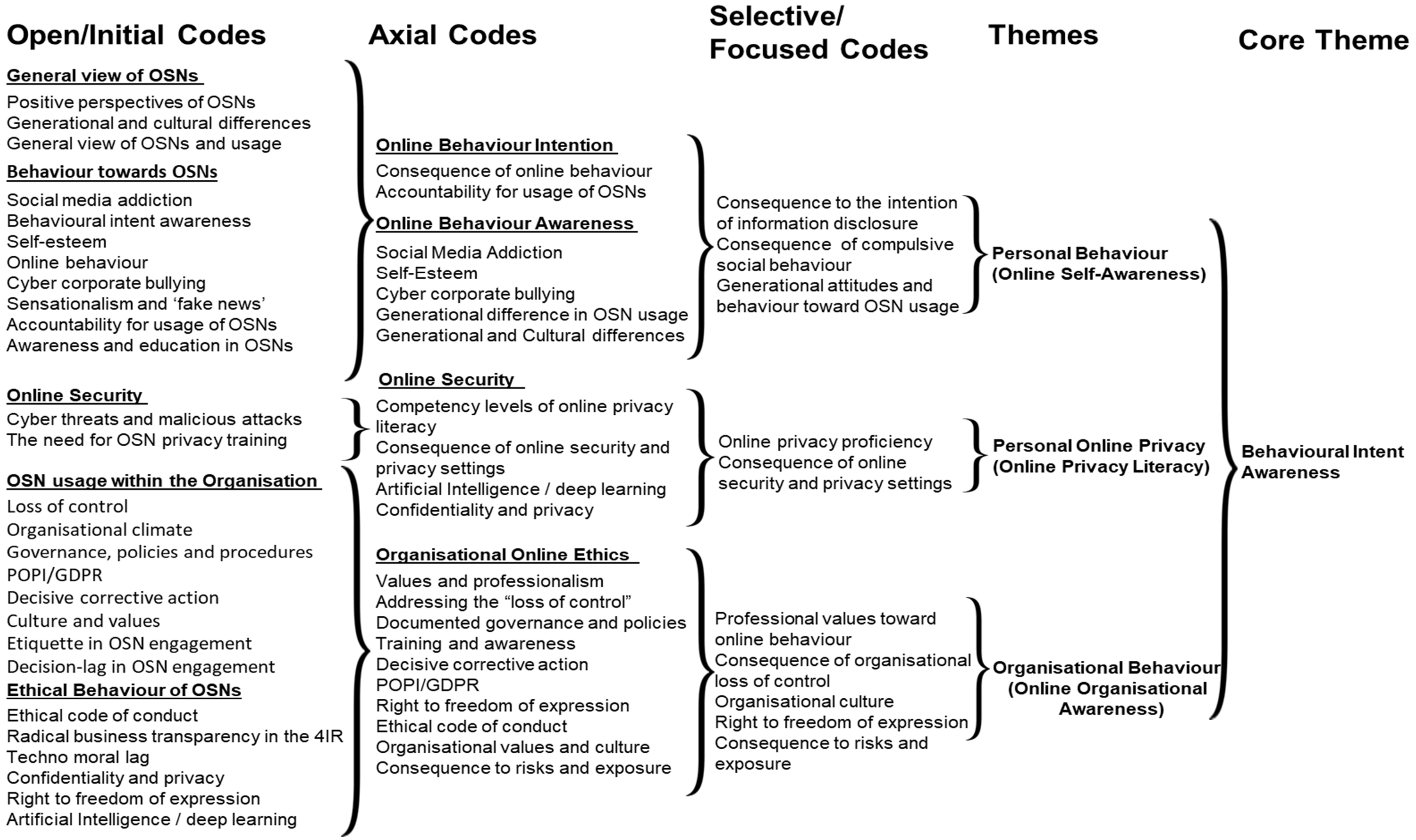
4.2.10 *Behavioural Intent Awareness*

Engaging on OSN platforms is primarily a social endeavour. A person engages on an OSN platform as a social endeavour to interact with another or a group of others. An interaction with another or others requires conduct classified as behaviour towards others.

The OSN platform's technology, however, can influence behaviour in how one conducts oneself and determine behaviour for you. This is in line with the three contexts of behaviour defined by the online dictionary Lexico.com powered by the Oxford dictionary (Lexico.com, 2019), namely:

1. How one acts or conducts oneself, especially towards others.
2. How a person behaves in response to a particular situation or stimulus.
3. How a machine or natural phenomenon works or functions.

For a business definition, an international standard for business behaviour set by the Caux Round Table, a group of international business leaders from the US, Europe and Japan, eludes to human dignity and the Japanese concept of kyosei, ‘‘living and working together for the common good’’ as defined by Canon Inc (Nguyen, 2016; Trevino and Nelson, 2017).



Open/Initial Codes

General view of OSNs

Positive perspectives of OSNs
Generational and cultural differences
General view of OSNs and usage

Behaviour towards OSNs

Social media addiction
Behavioural intent awareness
Self-esteem
Online behaviour
Cyber corporate bullying
Sensationalism and 'fake news'
Accountability for usage of OSNs
Awareness and education in OSNs

Online Security

Cyber threats and malicious attacks
The need for OSN privacy training

OSN usage within the Organisation

Loss of control
Organisational climate
Governance, policies and procedures
POPI/GDPR
Decisive corrective action
Culture and values
Etiquette in OSN engagement
Decision-lag in OSN engagement

Ethical Behaviour of OSNs

Ethical code of conduct
Radical business transparency in the 4IR
Techno moral lag
Confidentiality and privacy
Right to freedom of expression
Artificial Intelligence / deep learning

Axial Codes

Online Behaviour Intention

Consequence of online behaviour
Accountability for usage of OSNs

Online Behaviour Awareness

Social Media Addiction
Self-Esteem
Cyber corporate bullying
Generational difference in OSN usage
Generational and Cultural differences

Online Security

Competency levels of online privacy literacy
Consequence of online security and privacy settings
Artificial Intelligence / deep learning
Confidentiality and privacy

Organisational Online Ethics

Values and professionalism
Addressing the "loss of control"
Documented governance and policies
Training and awareness
Decisive corrective action
POPI/GDPR
Right to freedom of expression
Ethical code of conduct
Organisational values and culture
Consequence to risks and exposure

Selective/ Focused Codes

Consequence to the intention of information disclosure
Consequence of compulsive social behaviour
Generational attitudes and behaviour toward OSN usage

Online privacy proficiency
Consequence of online security and privacy settings

Professional values toward online behaviour
Consequence of organisational loss of control
Organisational culture
Right to freedom of expression
Consequence to risks and exposure

Themes

Personal Behaviour (Online Self-Awareness)

Personal Online Privacy (Online Privacy Literacy)

Organisational Behaviour (Online Organisational Awareness)

Core Theme

Behavioural Intent Awareness

Figure 4.1 Coding Process from Open Codes to the Core Theme

In considering the engagement of OSNs, behavioural intention can be defined as the likelihood of an individual's assumed or predicted behaviour when engaging with the OSN platform. This assumption or prediction in behaviour may be either planned or reactive. As defined by the Encyclopedia of Information Science and Technology,

> *"An individual's intention to use a particular technology directly affects actual usage."* (Iqbal, Nisha and Rifat, 2018).

For this research, Behavioural Intention Awareness can be defined as the recognition by an individual of their personal internal directives to achieve the desired outcome.

The interviews were re-analysed to identify any references to the interviewees' general theme of behaviour intent awareness.

From the literature on OSN engagement, the three dominant behavioural characteristics and the effects thereof were identified and earmarked for discussion during the interview process.

4.2.11 *Three Themes of Behavioural Intent Awareness*

From the findings, the three themes in line with influence responsible and abusive OSN engagement within the organisation follow the three constructs that affect and impact the levels of responsible behaviour when engaging on OSNs derived in the literature review, namely:

1) Personal online behaviour (online self-awareness).
2) Personal online privacy (Online privacy literacy).
3) Organisational behaviour (Organisational awareness).

The first theme, personal online behaviour towards responsible OSN engagement, is discussed by expanding the derived selective codes, namely:

- Intention of information disclosure.
- Compulsive social behaviour.
- Generational attitudes and behaviour toward OSN usage.

The second theme, personal online privacy, are measures taken by employees to ensure employees' online security and privacy setting proficiency will ensure maximum protection when engaging with OSNs. This theme is discussed by expanding the selected codes, namely:

1) Online privacy proficiency.
2) Online security and privacy settings.

The third theme, organisational behaviour, is an awareness of the organisation's values, professional code, procedures, and policies. This theme is discussed by expanding the selected codes, namely:

- Professional values of toward online behaviour.
- Organisational loss of control.
- The right to freedom of expression.
- Risks and exposure.

4.2.12 *Personal Online Behaviour*

For this study, Online Self-awareness is the capability of being responsive and confident about who you are in the virtual world. On the one hand, it is one's self-perception of one's behaviour and self–regulation toward responsible OSN engagement. On the other hand, it is one's perceived ability of self-control toward the susceptibility to the vulnerability of malicious intent by third-party fraudsters or scammers within the virtual world. This includes collecting private and confidential information by OSN service providers (Fire, Goldschmidt and Elovici, 2014; Ali *et al.*, 2018).

The literature review revealed that the commonly defined generation groups differed in attitudes and behaviour when engaging on OSN platforms. Although most of the interviewees belonged to the X-Generation, the researcher found an acute self-awareness of age and generation group concerning attitudes and behaviour when engaging on OSN platforms (Bolton, Parasuraman and Hoefnagels, 2013; Smith, A., Anderson, 2018).

4.2.12.1 The Intention of Information Disclosure

There was general anxiety about the urgency of this need for affinity and disclosed information, as discussed by one of the hospital managers,

> *"Someone said this once, when email first launched, whatever it used to take two or three days to get a reply on an email, today, it takes two minutes. There's this urgency to get a reply, to do*

> *everything now, stop and think and if you're driving, the person gets agitated, why don't you reply, well, I'm driving, and then I'll do it when I get. Yeah. So that urgency is crazy."*

In healthcare organisations, there was concern that this urgency and need for consistent connectedness compromised critical environments prompting more decisive measures like banning nursing staff from using mobile devices in theatre,

> *"We've tried to limit it and requested whether it should or shouldn't be used you know you if you're in theatre, please don't use your cell phone, they even at one stage in those, before I was here, but were confiscating cell phones before the staff went into theatre, that's a very extreme measure of dealing with it; perhaps it's appropriate in the theatre environment, I don't know."*

However, it was irresponsible disclosure of information when engaging on OSNs that was of major concern to all the interviewees, as succinctly expressed by a hospital manager,

> *"It's that semi-anonymous position you can place yourself in with social media and then really say whatever you want, whatever comes to mind with no filter and no regard for anyone or anything else, and I think that is a danger, and I don't necessarily believe that's a mitigable situation."*

Information disclosure engaging on OSN platforms was discussed on two levels. On the one hand, there is the disclosure of the general social interaction, which is daily conversation generally comprised of news, opinions, family life, meaningful conversation and friendly banter. On the other hand, there is OSN interaction that is business specific. This often includes both the intended and unintended disclosure of business-specific private and confidential information. The interviewees made a definite distinction that some OSN apps were more socially oriented, some more business-oriented, and some were a crossover of social and business, serving the dual purpose as a social and a business tool. This introduces the notion of the frequency usage of two purpose-specific OSN platforms: those used for general social

OSN interaction and those used for business-specific OSN interaction.

4.2.12.2 General Social OSN Interaction (Social apps)

All the interviewees acknowledged the need of almost every employee within an organisation, as a social being, to socially engage and disclose information through an OSN platform of a kind offered by Facebook Inc. suite of products as an integral part of their lives.

Most of the interviewees acknowledged that this by no means restricted how we as humans structure our social lives, whether it be social banter, meaningful or frivolous conversation, but that, in many ways, it has become fundamental as to how many people structure their family and work lives as iterated by the CEO of a financial services organisation,

> *"The reality is that everyone is on social media most of the day, and I don't actually have a problem with it. It's, I think, the policy is there to guard us against. You spoke about addiction earlier. And maybe it's because I'm a woman. But I believe that especially for the women in the office if they can make sure that their personal lives and their children are sorted out, they are happy to be at work. To cut them off from that and not allow them to be interacting with the other stuff that's going on in their lives has an impact on the way they operate their business."*

This sentiment was expressed by the CIO of a healthcare organisation, who explained how his organisation saw the necessity of coming to terms with the need for the use of OSNs as a part of the employee or other stakeholder's well-being of their private and social lives, thus embracing the OSN culture.

> *"But definitely, we've moved along and going forward, there's going to be a lot more that we need to do I believe, to attract new staff Into the organisation, even things like giving the staff access to get onto Facebook during certain times of the working day, It's becoming more important. It hasn't really been highlighted as an Issue to me yet, but I'm sure It Is. Um, but we*

> *are also looking at other ways of potentially giving staff access to their social lives, social media lives without utilising the corporate backbone Infrastructure by creating WI-FI off a separate network sort of thing which Is where we are at the moment, we're actually just about to launch that in a couple of weeks. So the staff don't know about it yet but I think it will be positive. We're wanting to embrace digitisation In Its entirety which Includes a big part of the digitisation Is the way people communicate on social media so that's certainly an area we are more focused on now than we ever have been. A big drive of our CEO and of the group is digitisation."*

The general difficulty expressed by the interviewees was the dangers associated with the proliferation of either intended or unintended irresponsible social banter through the notion of radical transparency, as stated by a hospital manager,

> *"… that the company is very like aware and very careful in what has, is being displayed out there and very like aware that anybody can just like say what they want and how they want it."*

There was an underlying concern that, due to the nature of OSNs, the information disclosure limited by the restriction of context is either unintentionally, intentionally misinterpreted, or misconstrued.

> *"I wouldn't just tweet today or WhatsApp to them because there's a lack of knowledge. It's incomplete answer information."*

There was a core awareness by the interviewees, that information is disclosed not just to the recipient that one may have been communicating with but that there may be further disclosure to third parties that may not understand the context.

> *"… because I put it on a WhatsApp, and I send it to you, and you show your wife, and tonight she sends it to her friend, says look I'm getting (earning) a million and it gets in the wrong, it's chaotic."*

There was, however, a consensus amongst the interviewees that there have been sufficient industry incidents that may have resulted in law cases and other less serious examples that have by now acclimatized the stakeholders within the organisation to the consequence of controversial or inappropriate information disclosure.

> *"In most companies, there's sort of an unknown threat that, if you release or talk about stuff that is not appropriate, it could be career limiting. That depends on how career-limiting or how brave you feel, regarding releasing."*

However, there was general concern by the interviewees of the risk of possible association with the organisation should controversial or inappropriate information be disclosed by an employee that can be either misinterpreted or misconstrued as clearly expressed by a hospital manager,

> *"And that's always going to be a risk. That people work in your organisations will have opinions out there. And unfortunately, the recipients of those opinions will find other ways to either heighten the sort of attention around it. And so instead of picking a fight with employee, the employee works for the organisation, well let's bring organisation into it'll, it will get more attention. So how do I get more attention to my little argument, I throw the organisation's brand in because I realized the employee works for organisation so guess what happens, I get a bigger audience because the world now picks up the organisation, not the employee.*

4.2.12.3 Business-Specific OSN Interaction (Business apps)

Business-specific OSN interaction was generally regarded by the interviewees of the three of the younger organisations, two of which were in the financial services sector and one in healthcare as an opportunity for competitive advantage over their larger counterparts. This was noted by the non-executive chairman of one of those small financial services,

> *"Social media is a competitive advantage for us. As a disruptive start-up, we look at it as an asset. We can differentiate, so yeah, we tweeting all the time, reaching a particular audience that we think is giving us an advantage… it's beneficial to your business*

> *because you can reach you, can reach a much broader audience."*

There was a view that older, larger organisations were slower to adapt to the disruptive strategic and business advantages OSNs platforms offer. As was echoed by a director from one of the smaller, younger financial services organisations with regard to competitors that may be primarily embedded in pre-OSN culture,

> *"Fairly regulated, fairly closed where communication is really sort of strictly monitored… Before social media and their businesses have developed and matured pre-social media."*

This pre-OSN culture was echoed by the hospital manager, who was adamant that other than WhatsApp groups, OSNs had no place in mixing business and social communication in the work environment.

> *"But social media should stay as the word social media is, it needs to be relaxed, it is not to be used for business purposes other than what we do in our WhatsApp group for the hospital for marketing. And these other things which are happening."*

However, this view was not shared by the executive management of this healthcare organisation, who have decided to embrace the new communication medium through the engagement of OSN platforms. This was confirmed by the CIO of this healthcare organisation, talking about the need to embrace OSNs within the organisation a sentiment similar from the interviewees of the larger organisations,

> *"I Mean WhatsApp we now realize even though it is not a social media platform but I mean WhatsApp is so prevalent I guess in most businesses but in healthcare it is just used absolutely everywhere for communication purposes."*

All the interviewees well recognised the need for an OSN presence, and here the emphasis in the financial services sector tended towards a purposely business type of OSN App such as LinkedIn, as stated by the CEO of a financial services organisation,

> *"So, I recognise that it's important. And we've actually all done a course, the planning side, on using social networks to develop*

> *our business, LinkedIn specifically, and the people doing the course said that, for given our business, that's probably the best place to be. I had intentions of posting a lot more actively than I have been. I'm very; I'm personally always concerned about spamming people and sending them stuff that is drivel or that is not relevant to them. So, LinkedIn is different because you post it, and people can choose to read it or not read it. I've put a few things up, but not too much."*

In contrast, there seemed to be more emphasis in the healthcare sector on the more socially oriented OSN, Facebook. This is because the nature of interaction by a healthcare patient rather than that of a financial services client would be more to post their experience, good or bad, on a platform such as Facebook. This was explained by the information communications manager of the healthcare organisation.

> *"So I think as an organisation, we have moved on quite quickly from where we were a couple of years ago; I mean, we monitor our Facebook stats quite closely now; it's monitored at the group Exco on a monthly basis. We go through all the statistics of the usage, who's liking our page, who's looking at our posts."*

However, acknowledgement is made for the need to have a business presence and goes on to say,

> *"I think there's still a lot more we can do, we don't have a strong LinkedIn presence, and we don't have a strong Twitter presence. It was actually the organisation's emergency services division, I think that had Twitter at one point, and there was an unfortunate post (let's call It that) or message made by one of the paramedics, and this was going back a good three years, I think that sort of stopped our progress with certain of these platforms, because It can go wrong very quickly and how you manage that fall out can be quite difficult."*

What is important to note is that business information content disclosure from profiles dedicated to the organisation is formal and controlled by persons designated by the organisation. However, the individual employee's personal profile is almost impossible to control. Business information disclosure from an employee’s personal profile can be subject to policies and procedures defined by the organisation, but, because of the nature of OSN platforms, these policies and procedures are at the employee's discretion.

As discussed in the literature review, this can be exacerbated by controversial ownership and control of data uploaded and exchanged by the OSN organisations such as Facebook, Google, Twitter, etc. Currently, these OSN organisations claim only to use the data to personalise targeted marketing to individuals. The fact, however, remains that these OSN organisations own all data that is uploaded and exchanged. Suppose a confidential picture taken of an infected organ or of possible symptoms of an infectious disease is sent as medically beneficial information to a responding medical specialist in a WhatsApp group of practitioners. In that case, the confidential picture effectively now belongs to WhatsApp and its parent company Facebook. This is a dilemma healthcare organisations face where information is disclosed using a platform that violates a patient personal data but is of vital importance, as stated by a former trauma nurse now appointed to control the OSN channels within her healthcare organisation,

> *“It is medically beneficial. I mean, I have a transplant group that the entire organ donor management is communicated to a large number of people around what’s happening with the organ donor. It is beneficial, because that team knows what to do, that teams knows what to do and this team knows what to do and the coordinator is actually able to share that information. But I don’t have any other platforms.”*

This is reiterated by the communications director and paramedic of the emergency services of this healthcare organisation,

> *“We work all hours of the early morning”,* **chuckling, “***that’s when all the big accidents happen. You take pic and send out an APB with some vitals to all surgeons on your WhatsApp contacts that you know and have worked with. Yes, my job is to*

> *save a life first then worry minor contentious legalities that as yet have had no effect on their personal lives."*

Using an OSN to disclose information to a patient can potentially not only be accidentally sent to the wrong recipient but be seen by prying eyes of a briefly unattended phone, as discussed by a hospital manager,

> *"One hand corporate governance, on the one hand we are saying this is how we act, this is how we behave, this is what our values are, and on the other hand people think social media's Facebook, it's not just Facebook, like you said, it's everything else. I mean, WhatsApp belongs to Facebook; all you have to do is look at WhatsApp, there is patient information on WhatsApp, people talk about people, about complaints about doctors on the WhatsApp; it goes totally against what our values are saying".*

Using an OSN platform to communicate with a patient is becoming more prevalent and seems to be placing some medical practitioners in an awkward dilemma, as raised with a director of a healthcare organisation who, as a practising general practitioner, stated,

> *"I try not to do so it actually almost never, I might send the odd message that blood tests are fine or that sort of thing, but I don't normally send results, so anything like that over the phone."*

Who then goes on to note,

> *"Look, I'm sure practitioners do send results over the phone and say well, this is the result and that sort of thing. But personally, my feeling is I try to avoid that we're just for various reasons, people don't understand results."*

This concern was reiterated by a manager from one of the healthcare groups,

> *"We have no control over the information that is disseminated or controlled by or whatever by the doctors. I can give you*

> *numerous instances where doctors have shared information with patients that has not been appropriate."*

Mention was made about taking the appropriate measure to avoid the danger of being held accountable for a message via an OSN that was seen to be delivered and read at an inappropriate time,

> *"I've taken read receipts off my WhatsApp because nothing stopping a patient messaging you at 12 o'clock at night with chest pain and you kind of half-hearted read and fall asleep you're now responsible because you read that message so…"*

As within the healthcare organisations, the financial services were as stringent in their approach and addressing business and client confidentiality when engaging on OSNs as an interviewee stated.

> *"I think having confidentiality is… client confidentiality is everything… you constantly aware… it is top of mind all the time."*

And then goes on to confidently say,

> *"I really think that is a there's an understanding and in the team of the criticality of confidentiality."*

When questioned about the exposure of client information on OSN platforms, one of the financial services managers expressed concern about client confidentiality being breached outside of the organisation.

> *"I mean if you think about it from our perspective, from a banking perspective from a peer perspective; we've been running now for nearly 2 years on it and so there is a lot of awareness around that and what we need to do. The concern around that absolutely."*

As with the CIO of a healthcare organisation, the CIO of a large financial services was confident in maintaining strict information disclosure within in the IT infrastructure of the organisation and saying a breach of client confidentiality through the information disclosure through OSN platforms is unlikely due to the direct and private business relationship between a portfolio manager and their client.

> *"So our portfolio managers, yea, I mean yea, if they deal with clients on social media it's only with their own clients and that is generally all who they communicate on social media with. I mean if you give someone your money to look after… it becomes a personal thing yea. I mean like a real business but close relationship. Yea. It's a trust thing and that's why we're a successful company. So a breach in confidentiality is very unlikely. We professionals!"*

4.2.12.4 Crossing over between Social and Business Interaction (Dual apps)

The crossover between using specific ubiquitous social media apps and both social for business communication can be fraught with difficulties. This is aptly described in a recent article on the online publishing website lifewire.com,

> *"The increasing adoption of social networking sites like Facebook, Twitter, and LinkedIn presents an interesting quandary for people who want to use social media for both personal (keep in touch with family and friends) and professional (network with colleagues) purposes."* (Pinola, 2019)

All the interviewees understood that the quandary facing an employee or other stakeholders engaging on an OSN platform on both a business and social level, though impossible to manage, needs to be acknowledged by the organisation as a part of the modern way we connect and communicate whether it be for business or socially. Here it was the smaller organisations that were able to adapt not only to accept the use of OSNs as a communication mechanism, whether social or business, but to exploit it as a disruptive technology much sooner than their larger counterparts. For example, the CEO of a financial services start-up noted when asked whether, as a start-up entity, they had the opportunity to structure their business regarding the disruptive nature of OSNs:

> *"Correct and, and a lot of it is timing because you know, they obviously started a helleva long time ago before social media*

> *and their businesses has developed and matured pre social media. So social media for them is, is, is not necessarily an asset. I would say that internally they may see social media as a liability whereas we look at it as an asset. We look at it as something that we can we can use in a positive way. And as I said that we can differentiate, so yeah, we tweeting all the time. We reaching a particular audience that we think is giving us an advantage."*

Consequently, the CEO of a large healthcare organisation quickly pointed out that acknowledging and adapting OSN engagement was a lengthy process.

> *"So I think the organisation historically, we've been more conservative when It comes to the social media channels, there's definitely been an understanding or an acknowledgment now at all levels, that we need to pursue that avenue, because I mean this Is the way the new generation are communicating primarily, via the social media platforms."*

There was a clear distinction made by all interviewees between what was deemed to be business and what was deemed as social information disclosure. The consensus was that when engaging on OSNs, business and social information disclosure should ideally remain separate as far as possible. How much one should separate business from social or pleasure is difficult to manage from a personal perspective, let alone by the organisation.

Consequently, others see a mix of online social and business interaction as a positive approach. Therefore, crossing the boundary between social and business whilst engaging on OSN platforms has become particularly relevant when using WhatsApp.

The use of WhatsApp groups has transformed what started as and is often still primarily used as a social-based OSN to a business tool managing group discussions within the organisation. The findings showed that within the organisation this boundary is clearly defined and that the members of the OSN group govern non-relevant social information disclosure.

> *“We’ve had cases like that where silly things have been posted or put into WhatsApp. We've had to make sure that the teams understand that it's a tool used for business only, and again in that, if that is brought to our attention, we deal with it immediately, so the guys understand that you can't pass stupid comments on WhatsApp when it’s related to business, patients, people, colleagues.”*

This crossover of OSNs serves the dual purpose of social and business-specific interaction where unintended infringements are most likely to occur. For example, implied or mentioned throughout the interviews were instances of an unintended irresponsible tweet posted by an employee and then being associated with the organisation, a message accidentally sent to the wrong recipient, or an online confidential trail of email correspondence inappropriately copied to a newly included recipient.

> *“…we do we do especially we had a thing where actually the PA sent out the wrong email to the wrong person, wrong company, which she wasn't supposed to and that just folded the entire thread. And so, we then had a whole tech of what is the implications, what could happen. Legal actually sat in and said, if you take it from this point, this point, this point that can actually happen.”*

This could also result from unintentionally sending a word prompted by predictive text that may offend or be taken out of context.

> *“Yeah, I actually told my boss about balls the other day because I was actually trying to tell him the guy from a company was balled over.”*

The fact that OSN conversations are being recorded means that what is being said on an OSN platform is subject to being read or heard by unintended or un-expectant recipients of the conversation. This is demonstrated in the example from a manager of a healthcare centre below, whereby suddenly including a recipient in the copy “cc” of an email can result in unintended consequences.

> *“We had one incident here where certain comments were made on an email about a practitioner, and it was a little bit derogatory but not the end of the world but it was between staff that we're making fun of this, and then at some stage one of the staff members added the practitioner in as the cc.”*

The general sentiment, however, was that OSNs are here to stay, and the more familiar employees become with the consequences of irresponsible behaviour within the business community, the more they will adopt responsible behaviour.

As a regional director of a healthcare organisation expressed about adapting to OSNs

> *“It's about balance in life. And definitely, people do not have the skills.”*

4.2.12.5 Compulsive Social behaviour

The theme of Compulsive Social Behaviour emerged as an aggregation of the axial codes of social media addiction, self-esteem and cyber corporate bullying grouped as Online Behaviour Awareness. From the respondents, the compulsive behaviours resulting from social media addiction and cyberbullying can affect the workplace differently and are thus discussed separately.

4.2.12.5.1 Social Media Addiction

When asked about the propensity and effect of online social media addiction in both the employee’s private life and workplace, it became apparent that very few of the interviewees had considered this type of behaviour formally as an addiction.

At least ninety per cent of the interviewees, however, were aware and said they had observed a sporadic prevalence of behaviour miming OSN addiction. The remainder were partially aware of such behaviour.

Except for two senior executives in the health sector, the rest of the interviewees appear to be unaware that OSN applications are currently being developed to maximize usage by the user by employing addictive techniques. These techniques can lead to a compulsive need to consistently monitor OSN apps. This addiction is associated with continually seeking responsive feedback, which fuels a habitual, often uncontrollable drive to engage with an OSN to post or send a message.

When asked about the effect of social media addiction in the health and financial sector workplace, the sentiment was somewhat mixed. This was particularly more evident in the health sector, where there was a dominant sentiment towards OSN addiction as a factor compromising the workplace.

> *"I can assure you it happens everywhere; inwards, are nurses checking monitors or charts or are they looking at their phone and playing on social media or interacting with family and friends and what is the answer?"*

This was contrasted by some interviewees who felt that although OSN addiction was evident, it was controlled enough not to compromise the work environment.

> *"Never experienced it, they're, I think they're focused enough that that hasn't interfered, well aware of the social addiction stuff though because I mean I've seen quite a few people that have, are that distracted."*

Interviewees in the health sector acknowledged OSN addiction as a potential problem amongst healthcare workers who worked directly with patients. However, most interviewees tied the potential work compromise of OSN addiction when the nature of the work of the healthcare worker revolves around caring for and monitoring patients. This type of work environment is categorised by long periods of idle monitoring, which often leaves these employees with time during which they start fidgeting with their phones.

> *"It's more the anaesthetic nurses that in fact, have long periods of nothing to do, where they're expected to be somewhat vigilant; I would say your other setting is potentially your ICU nurses who are expected to be vigilant for long periods of time with long periods of not performing tasks other than vigilance and there the distractor may be strong…."*

This effectively opens a door into the cyber world where the addictive nature of the OSN apps entraps the individual in that world for longer than intended:

> *"I'll just go onto social media for a little bit, Chews up 10 minutes which becomes longer."*

This type of behaviour would result in unintentional neglect of patients in their care and failure in their responsibilities to other medical practitioners and hospital management.

> *"I've had I've had complaints from patients where a patient says to me your nurse was more interested in her phone than me."*

> *"…we've had a few of those, where we say the nurse is hardly here, she's just on her phone all the time."*

> *"Yes, absolutely, you would just have a meeting with your doctors and your doctors would tell you and say you would be busy with a procedure, and you would ask where's the staff, where's the staff? And then when you quickly go to the bathroom here, they are around the corner sitting at the desk and quickly like on their phones."*

However, as mentioned, this type of awareness experienced by the interviewees was of a mixed nature. Focusing on the health sector, three respondents thought that although OSN addiction may appear to manifest itself in the daily life of health workers, as professionals, whether it be a nurse, ambulance assistants, paramedics, medical doctors or specialists, attention to the job at hand would take precedence to unwarranted time spent on an OSN platform.

Eighty per cent of the health sector interviewees recognise the conservative perspective associated with stigma typical of the notoriously ungovernable traits of addiction. However, this perspective may be skewed due to the danger of an addiction in work environments where attentiveness to work on hand can mean the difference between life and death.

The possibility of a professional err on the side of caution due to the destructive nature of addiction in the healthcare sector can be contrasted to the unanimous view by the interviewees in the financial sector that they did not feel OSN addiction significantly compromised the work environment. In this regard, the consensus was that as social beings, everyone with access to OSN platforms, whether through a mobile device or web access, is driven by the need to connect with others and thus at times, may to some extent fall prey to the addictive tendencies of OSN platforms. Analysing the financial and health-sector interviews, about a third of the interviewees openly acknowledged their self-awareness of a tendency to at times be personally addicted to engaging on OSNs. This was acquiesced to by a senior director in healthcare in the opening stages of the interview process:

> *"So I would count myself as one of the people in my generation where I'm addicted to my cell phone definitely I will not be able to function without my phone."*

The respondent then went on to say that given this need to be attached to connectivity through OSN platforms,

> *"…like anything else in life, I need to have the skills to find balance where that is."*

Successfully adapting both our private and work lives to the persuasive and addictive nature of the phenomena of OSNs by balancing appropriate time spent engaging in work activities with family, close friends or socially was a key underlying theme throughout the interview process.

The latest research from the developers of the Bergen social media addiction scale used in several studies in OSN addiction found the most significant controllable variable amongst other demographics such as age, gender, income, companionship, and narcissism was low self-esteem (Andreassen, Pallesen, and Grif, 2017). Unfortunately, views on the type of demographics susceptible to OSN addictions were not directly addressed in the interviews by the researcher. However, three interviewees' responses supported the latest research from Andreassen *et al*. tying low self-esteem as a possibly significant factor to OSN addiction.

> *"So that comes in with the whole thing about how addicted people are to social media so the introvert characters would generally want to hide themselves because of their esteem issues, or just maybe introvert in nature, want you just sort of use social media as their main platforms to communicate and be present."*

> *"…but also sometimes where their posts are disturbing, and that you can see that they emotionally looking for support, and it's not the place to do it."*

In drawing a further comparison between the health and financial sectors regarding possible compromise in the workspace as a result of OSN addiction, the nature of work can play a significant role.

Re-emphasising the critical environment of a hospital's operating theatre, ICU ward or even just the monitoring and care of patients in a general ward or that of emergency services and trauma units may be far more susceptible to dire life or death consequences to an unintended ineluctable behaviour as a result of OSN addiction.

As mentioned earlier, this is exacerbated by the temptation to engage in OSN activity while spending the idle time often required in monitoring and caring for patients whether in a ward or during a medical procedure. Vigilance concerning job performance in this environment is crucial.

OSN addiction though limited could have dire consequences in more critical medical environments. Thus, it is understandable that the threat of compromise in the work environment due to OSN addiction in healthcare employees was of great concern, particularly to hospital managers.

4.2.12.5.2 Self-Esteem and Corporate Cyber Bullying

In discussing irresponsible or negligent behaviour through the engagement of OSNs, the researcher asked whether the interviewees were aware of or thought that a lack of self-esteem might be a factor. It was evident that as a notion, self-esteem as a factor in the use or abuse of OSN activity had not occurred to most of the interviewees. Some interviewees, however, immediately related instances of what they thought may be due to the lack of self-esteem manifesting in irresponsible OSN behaviour. When discussing self-esteem, the conversation often moved to an underlying link to cyberbullying. Two interviewees were quite adamant that a lack of self-esteem had no effect on irresponsible OSN behaviour but rather directed the conversation to cyber bullying as a behavioural problem engaging one OSN platform.

Though the link between low self-esteem to cyberbullying was supported in the discussion by the interviewees, the lack of self-esteem and cyberbullying do not necessarily imply one or the other. A lack of self-esteem may manifest itself through a superficial misrepresentation of oneself through an OSN platform, as related by an executive in the healthcare sector:

> *“So, one example was a young gentleman who created this personality of a medical student and a paramedic and a whole bunch of things which he wasn't really picked up on by anybody because it's just another one of the mess, but he wasn't anyone of those things. And it got to the point that he walked into a hospital to try and behave as a doctor.”*

As mentioned by another interviewee, it is often the introverted personality that is susceptible to using

> *“social media as their main platforms to communicate and be present.”*

This may be a positive factor that enables employees whose low self-esteem prevents direct face-to-face communication with others to effectively make their opinions and voices heard through OSN platforms.

The majority of interviewees understood the potential problems and were unaware of the prevalence of cyberbullying within their work environments. There were, however, a few of the interviewees in the health sector who attested to the presence of cyber-bullying.

> *“That’s what I was going to say, bullying is the issue here. I mean, whether you're bullying on cyber or bullying one on one it’s going to have the same impact because even I mean, you can read when people are writing in their responses or their emoticons or their how they say stuff, you’re hurting people. So whether you see it one on one or you see it on the reply, you're going to feel it. So cyberbullying and one on one bullying, I think, I don't know which one is worse.”*

As explained by an interviewee, when engaged in an activity deemed as bullying, the would-be bully is

> *“not aware of their behaviour, they were either trying to be funny or trying to be dominant or whatever the fact is, but they not aware they kind of hurt someone’s feelings.”*

This is particularly relevant in the lack of physical presence when communicating using an OSN platform where the emotional or physical reaction of ‘social cues’ through body language cannot be witnessed. One of the interviewees related bullish behaviour on WhatsApp groups by using short, sharp, and colloquial language. This is a tone which may have very easily been misconstrued in many cases as cyberbullying, although not intended as such. This interviewee goes on to say

> *“... the point of email, it's very easy to stand behind that. You can be, even if you are not a particularly firm person face-to-face, you can be very firm in that.”*

There is a sinister side to cyberbullying, however, where the root cause is not linked to a lack of self-esteem but instead a result of malicious or manipulative behaviour through intimidation or discrediting fellow employees for self-gain. This type of behaviour is often considered to be office and corporate politics and is known as such.

> *“I don’t think self-esteem has got anything, but I do know that there is cyberbullying. I know that people forward your message to other people which might be read out of context, you know”.*

Online self-awareness, as defined in this research, includes both self-esteem and online self-efficacy. The assessment of the levels of self-efficacy is most effectively evaluated using self-reporting techniques in quantitative research and was not directly addressed in qualitative research. Even when mentioned in passing during the interviews, there was not much contribution from interviewees except for one medical practitioner, a director of a medical centre, who raised a concern with regard to low self-esteem in the form of emotional neediness,

> *“There's still one newish individual who's not an employee she does our Discovery interface for us and I think emotionally she may be in need of some attention but I haven't looked at her Facebook posts but I would imagine that if I did, I’d see possibly*

> *reason for concern, so alarm bells like whether they need emotional support?"*

It is noteworthy that recent research findings have shown that higher levels of self-efficacy correlate with lower susceptibility to cyberbullying (Jones, 2019; Kokkinos and Antoniadou, 2019).

4.2.12.6 Generational Attitudes and Behaviour toward OSN usage

The influence of generational differences in the approach and adoption of OSN usage as part of online self-awareness was analysed. This was divided into the digital natives, those who have grown up with the medium of OSNs as a communication medium and the digital immigrants, who have learnt to adapt and adopt OSNs as a communication medium. The frustration of grappling with the different approaches to the use of OSN by different generations was clearly expressed by an X-generation senior manager in the financial services,

> *"…we talk a lot about like millennials by way of example, you know, and behaviour around millennials. We tend to do that more in a corporate context of the role. But, I think that there is a real differentiation between the use of a person, say my age or beyond, late forties, fifties and beyond. What we put out on social media would be more out of ignorance or mistake potentially, right – and there's something to do to combat that. Then if you take a look at the millennials, they might put something intentionally out there, but not understand the full consequence of why it is out there."*

The frustration, however, was not restricted to the Baby boomers or X-generations but was also expressed as an issue by millennial interviewees who felt the divide between the digital immigrant and digital native is impossible to bridge. This frustration was expressed in the comments by one of the millennial hospital managers,

> *"I think the generational as opposed even associate economics to a degree and aspect has come into play here, because if you have not been raised with a smart device and we connected all the time we have smart watches, smartphones, you know,*

> *interconnectivity where we go Wi-Fi, where we wonder if you haven't been raised with those, those luxuries to large degree in this country or with that sort of understanding I think about my, my mother she wouldn't she wouldn't yeah, it's probably a generation, she's a baby boomer, so it's, it's not something that they were familiar with until towards the end of there, in fact after their work lives and to get that level of understanding embedded I think is near impossible….”*

When discussing generational differences, the interviewees distinguished between the concept of digital immigrants, Baby Boomers, X-Generations and some older Millennials versus digital natives, Millennials born in the late nineteen eighties. However, the following general views emerged when discussing the concept of radical transparency distinguishing between digital immigrants and digital natives.

The X-Generation/Baby Boomers (digital immigrants) developed their social communication skills without OSNs. Their development was familiar with privacy and confidentiality. Transparency was guarded in that transparency was not always automatic. Radical transparency was, at best, often in the form of the gossip frequently referred to as the “bush telegraph” or the grapevine that was reputed to be riddled with sensational inaccuracies and exaggerations.

The younger generation, the Millennials (digital natives), have a different approach to engaging with OSNs regarding communication and what is communicated. First, they become familiar with OSNs from a younger age. They effectively developed their social skills based on OSN engagement, where the radical transparency of an original message through the use of the technology of an OSN is transmitted not only faster than what was known as gossip but with precise accuracy and with a possible unlimited reach within a matter of minutes.

> *“I didn't grow up with a cell phone initially, that came towards my teenage years, if I look at, you know, a lot of the staff we're currently employing, they don't, they’re almost surgically bonded with their mobile devices and then that social network connectivity and there's that filter that I certainly was raised with*

> *and this is respected, these are boundaries etc., don't necessarily exist in that same fashion in the virtual space."*

As stated by a paramedic in executive management, there was an underlying concern from more than half of the interviewees that OSNs are limiting the millennial generation's effective communication techniques.

> *"older generations value communication a whole bunch more because it was more deliberate, whereas the younger generations, communication is like a background noise almost, you don't have to be deliberate about it, you don't have to think about what you say because like, it's just more communication. It's not as deliberate as previous generations had to make it."*

Furthermore, there was a concern that the millennial generation lacked the foresight or experience to fully comprehend the consequences of inappropriate OSN usage.

> *"I think for me as well, you know, we talk a lot about like millennials by way of example, you know, and behaviour around millennials. We tend to do that more in a corporate context of role. But I think that there is a real differentiation between the use of a person, say my age or beyond, late 40s, 50s and beyond. What we put out on social media would be more out of ignorance or mistake potentially, right – and there's something to do to combat that. Then if you take a look at the millennials, they might put something intentionally out there, but not understand the full consequence of why it is out there."*

In contrast, a few older interviewees were only too happy to draw on the more tech-savvy skills of the younger generation in the assistance of OSN usage and security settings. What was clear from the discussions regarding the different defined generation groups was the divide between digital immigrants and digital natives, with challenging elements on both sides. The challenges are possibly more apparent to the digital immigrants who have had the benefit of experiencing the structure of social circles and communication both with and without digitisation or, more specifically, OSN platforms. This was aptly put with a digital immigrant from the emergency services.

> *"I think I'm more cognisant of what's going on in their world because it makes it or it helps me understand how it works so you can't force down what we used to do and how it used to be; it's an illogical thing but also in saying that you can learn so much more from their world, things that are complex for us or questions we don't have answers to now are easily resolved, like a simple thing you can Google anything. If you're not literate on your smart device and you play that you can't or you don't know something or you there's nothing you can't find out. That's what's important now is to understand that there is a mechanism to be able to find out anything, there is nothing you can't find out but it doesn't, it wasn't the world we came from we used to read from encyclopaedias and have time on your bicycle in the park. They don't have that."*

Researcher: *Any other comments?*

> *"I think it's a world or a time where we just have to understand different segments of this world, you can't live in how the world used to, you can't live in the world how it is now, there has to be a balance between everyone and I suppose the sharing of what we do in different platforms whether it's direct one-on-one contact or it's cyber contact you just got to be careful that's my only message, the risk right now is probably 10 times worse than it's ever been."*

4.2.13 *Personal Online Privacy*

When questioned on the competency levels of employee online privacy literacy and privacy settings within the organisation, the interviewees had very little knowledge. They were thus a little reluctant to provide an assessment of online privacy literacy. However, where mention was made, the following findings were made.

4.2.13.1 Online Privacy Proficiency

The perceived level of competency of online privacy literacy of employees by the majority of interviewees, particularly in the health sector, leaned toward discomfort rather than comfort. This was typified by a healthcare centre manager when asked how well the staff was at knowing their online privacy settings, replying:

> *“Well on their phone, some of them.”*

In most cases, online privacy literacy was associated with the interviewee’s perceived level of online privacy literacy and vulnerability when engaging with OSN platforms on mobile devices.

> *“I know that we've totally missed the boat regarding cell phone security we've missed it completely because every person coming into our environment, whether it be the doctors and not just staff, doctors as well, haven't got a clue the danger of this thing.”*

Executive management was generally happy to entrust the levels of secured privacy of the network infrastructure to the competency of the Information Technology (IT) department. However, as the majority pointed out, the IT department can only control up to the end of organisational communications devices such as workstations, notebooks and company-owned mobile devices. The concern was the use of privately owned mobile devices and company-owned mobile devices used by executive management. This sentiment is reiterated by a senior executive in the healthcare sector.

> *“… every morning when you plug it into the network you would see group IT would try to push down the encryption software and my laptop ‘skops’ (kicks) it out, wouldn't take it for whatever reason, so they eventually worked away around that, a patch by putting in at that time it was windows ten which came with really good encryption so they were happy with that and at least my hard drive is encrypted. My cell phone is not encrypted.”*

The same interviewee, however, continues considering the quandary between exposure to a breach of company security by an employee through the engagement of OSNs and the employee’s constitutional right to privacy and to freedom of expression through the engagement of OSNs when engaging with their personally owned mobile devices then went on to say

> *“…our IT systems, our work IT systems prohibit you from getting onto social media platforms okay so our staff are accessing social media through their own personal devices. Is it not overreach by the employer to now want access to those personal devices or to monitor them?”*

In the financial sector, there was more comfort in the competency of online privacy literacy in the organisation, as stated by the chairman of a prominent financial services organisation:

> *“Yeah, I think, I think that they’re fairly, fairly savvy when it comes to this stuff. I wouldn't say that I've thought. I've actually checked you know, I haven't I haven't necessarily I’m making assumptions based on age yeah you know type of calibre yeah, yeah okay you know these guys so they will be well educated… it may be a good idea to do just a bit of a refresher in a way I suppose to what, what the dangers are.”*

The discomfort regarding online privacy literacy competency not only with the employees by the interviewees themselves is a clear indication that this is an ongoing training issue that needs to be addressed by today’s organisation.

4.2.13.2 Online Security and Privacy Settings

The behavioural intent awareness of online security is the personal acknowledgement of measures taken by an employee in protecting both personal and company privacy when engaging on OSN platforms. The level of personal acknowledgement is manifested by the likely behavioural pattern an individual will follow concerning adhering to best practice security precautions and habits. Eight interviews acknowledged personal and organisational concerns regarding the difficulties regarding the privacy settings of OSN apps in contrast to the ease of use.

> *“Because the app is so easy to use, nobody really understands the settings and privacy and all of that. So, I think it would concern me quite significantly, ja.”*

Or just simply stated by an organisation’s head of communications:

> *“Mm…privacy settings, browsing issues, fishing…, I think it would concern me quite significantly.”*

Of the younger interviewees, a general manager of a prominent hospital expressed frustration in effectively being trapped into accepting privacy settings to attend to his job with the least disruption.

> *“Apple sent me another update, I have to accept, if I don’t accept this thing doesn’t install. I have to press accept. I haven't read 15 pages that procedure terms of what they'll be doing with my information potentially.”*

A similar sentiment was expressed by an X-Gen compatriot general manager of a prominent hospital from a different province:

> *“For example, I'm sitting here I have a Facebook page, a Twitter page, I'm on WhatsApp, I'm on Facebook Messenger and because I'm not an IT guy, I hardly pay attention on my settings you know even though you know someone can hack and post something on my account.”*

And then goes on to say,

> *“In fact, recently someone cloned my Facebook account.”*

And then also expressed frustration with being trapped into accepting privacy settings that are too complex to understand:

> *“because I'm not an IT person and really we struggle as human beings to go through things that like T's and C's, things that are written in fine print so we always assume that it won't happen to me and we always assume that okay fine I'm safe, no one is looking at me, who am I to be looked by anyone, or to be but there is people out there that are phishing around the social media, even the internet for that arguments sake.”*

Even though there was a generally positive sentiment toward training and awareness, as mentioned earlier, only one mentioned training and awareness of privacy settings as a priority.

> *"And… people are really not aware enough of the privacy settings. So, and ultimately, I honestly believe that maybe like a an organisation like ours can even take up a position. We've got everybody's cell numbers on our HR books, so we can make people aware and say send out communication."*

Of particular concern was how to secure an employee's mobile device access. Again, a clear distinction was made between being able to secure the organisation's network infrastructure by enforcing and controlling employee password "best practice behaviour" on workstations and laptops through the IT department in contrast to having no control over an employee's behaviour in securing their mobile devices as expressed by a regional healthcare director,

> *"…business has got no control over which phones have got passwords, but they do have control of this* ***(pointing to his computer notebook****), because the passwords automatically expired every month for your main login credentials. And also for all other business systems, you're forced by the system to renew it. And you're forced to have a complex password regarding the nature of the password letters, characters and numbers and stuff. The system forces you to have something that's very secure. You don't accept a simple password."*

A further concern is not only at the ease that a mobile device can be compromised but holding an employee accountable for a compromise:

> *"…but one would have to then test was there gross negligence in the breach of my personal device, or had I really taken reasonable, was taken from me at gunpoint, and some Russian hackers could get through the phone and get all that information or, you know, what is the extreme you know."*

Within the healthcare services, access to formal organisation correspondence, such as an organisation email address through an OSN on mobile devices, was restricted to senior management, as explained by a hospital manager,

> *"…regarding email and the organisation like implemented like all the little security measures obviously if you have access on your phone, your work email, there's additional passwords and all that, so and not too many people are allowed to have that, to see their emails on the phone; it's mostly your senior management."*

In summary, regarding online security and privacy settings, the general view of management in both the financial and health sectors is that, although the organisation's IT division is confident in securing the organisation's network, it is limited to desktops and notebooks. Employee mobile devices are beyond their control. Access to organisational-based OSNs, such as email on a mobile device, is thus limited to senior management. Furthermore, there is concern over the exposure of the complexity of terms and conditions and privacy settings for the use of specific OSN applications resulting in most employees accepting default settings, as summed up by a hospital manager when talking about privacy settings,

> *"Everybody just agrees."*

4.2.14 *Organisational Behaviour*

The ethical climate of an organisation is the level of morals and ethics practised in the work environment of that organisation. This is often reflected as the moral fibre that determines the behaviour of stakeholders in the organisation and can be categorized as five types of ethical climate, namely; caring, observing law and order, following rules, instrumental values, and personals morals independent of the organisation (Victor and Cullen, 1988).

4.2.14.1 Professional Values of Online Behaviour

Organisational values and professionalism reflected the ethical climate within the organisation and were thus a key theme discussed with the interviewees. Coding organisational values and professionalism as a theme was linked to the code organisational awareness 16 times and behaviour 12 times. Awareness of organisational values and professional conduct regarding behaviour was vital to responsible engagement with OSN platforms. Interviewees emphasised that employee awareness of the expected professional conduct need not be specific do’s and don’ts for responsible OSN engagement but rather the expected type of conduct that would reflect the organisation’s values. This was clearly expressed by a regional director of a healthcare organisation as follows,

> *“I walk into those doors understanding that I am our organisation and I’m going to live up to those values, so yes they have they are numerous connotations to everything that we do in terms of our behaviours and one is to continuously create awareness around that. Yeah so the value system Yeah, it's central to everything we do.”*

And then reiterates a little later:

> *“The key thing is how do you drive the behaviour? The big drive is around the values and they are like seven underpinning behaviours that we focus on to say, how do we live up to those values so for example, you have a name badge to be able to identify myself you know, those type of things. I wash my hands to care, so that’s how do you bring the values in that so there is underpinning behaviours that we keep reminding our staff about and what that the hope that people live up to the values so when there's a decision to send an email or to post something on Facebook we remember those values, remember those behaviours. I live up to those and one hopes that those behaviours change over time.”*

This view typified the interviewees' approach, particularly from organisations in the healthcare sector. There was an underlying belief that creating a culture based on the values of the organisation would result in mannerisms and conduct that would naturally promote responsible OSN engagement, as reasoned by the general manager of one of the healthcare organisation’s hospitals,

> *“So again, the social ethos or the organisation’s value structure and just common sense is embedded into everybody. And everybody must surely at some point, understand what is right and wrong. And when you know that you're doing something that isn't correct and you are, so my theory is slightly different, is to say that you should behave in a certain manner all the time, not only when you're being watched. So we shouldn't have to be watching you all the time to be sure you acting in a manner that is acceptable.”*

Then going on to say:

> *“This veil, this thin line of anonymity when you're posting or communicating via social media that challenges that, what I certainly was raised on as a norms of respecting what you would or wouldn't share.”*

Later concluding:

> *“It's not that people are purposely transgressing unethical, norm or values. It's just their perception of that norm is just quite different from what we perceive, and I think that's where we have this clash of policy and reality.”*

User behavioural intention is not to compromise the organisation; however, it is the lack of awareness of the employee or other stakeholder’s personal information privacy (PIP) and organisational privacy that may be susceptible to being compromised resulting in a behavioural intention that may lead to a breach of private and company data. It has been stated that norms and behaviours regarding private and public domains may differ across diverse cultures.

When questioned about the attitude toward the OSN engagement by employees, approximately half of the interviewees believed that the organisation's values following its associated code of conduct as a professional offering were the critical factor influencing the expected behavioural intent of its employees. This was in contrast to less than a third that cited a more personal approach to personal privacy rights and moral values as the key factor. Although not directly stated, there was an underlying theme from most of the interviewees that the threat of consequence was actually the key factor that dominated behavioural intent. One respondent asserted that:

> *"I think it's the values and the behaviours, you know, like if you look at our seven behaviours that we put out there regarding respect and dignity and you know, how we interact with the patients and so I think yeah the values and behaviours do play a big role I do also think that people are nervous about getting themselves into trouble as well you know, that's the one aspect so say personal safety, but I also think that they, that staff have also become a lot more aware of patients' rights and patient's rights to privacy so all of that awareness regarding what the patient is entitled to."*

The response from interviewees was mixed. Some did not see the inappropriate use of OSNs as part of actual behavioural intent but rather as the lack of awareness of such intent. Others saw that behavioural intent resulted from a careless approach in the engagement of OSNs, disregarding the consequences. The researcher found restrained anxiety when the interviewees expressed views on behavioural intent when engaging in OSNs as a communication medium. It was evident that most, if not all, of the interviewees are still trying to negotiate both the benefits and dangers of OSN platforms as a medium that is now controlling how they communicate in both their work and private lives, as articulated by a chief information officer of a large healthcare group.

As a communication medium, there was an underlying uneasiness of the enigmatic nature in the use of OSN, particularly when the unforeseen consequence of an intended or unintended message or post unintentionally spirals out of control, creating reputational harm. The awareness of this potentially unintended consequence is an ethical predicament to which both the organisation and the employee are still acclimatizing themselves. This equivocal theme, often conveyed implicitly by the vast number of interviewees, makes behavioural intent in the context of OSN engagement challenging to prescribe and govern.

A few interviewees were open about the uncertainty and difficulty in developing an employee behavioural framework of do's and don'ts regarding OSN usage. Although three of the four organisations had clear governance regarding organisational policies and procedures regarding do’s and don’ts, the difficulty expressed by the interviewees is that OSNs have become a medium for expressing an individual’s personal views and opinions, whether it be in a private, work or public capacity. Part of the difficulty is that the implications and consequences of using OSNs as a communication medium is difficult to predict and often unforeseen. Usually, when organisational or personal confidentiality is breached or a reputational damaging remark is posted on an OSN, the consequence becomes apparent and understood. This will happen even if the post is misinterpreted and taken out of context.

This leaves the organisation to adopt a learning process of continually adapting its policies and procedures through a trial-and-error basis. As a result, reliance is often left to the individual employee’s personal morals and values or tacit knowledge of what should or should not be said. The CEO of one of the healthcare organisations expressed the frustration of this approach of dealing with a type of “Catch-22” situation.

> *“There’s enough emphasis on the risks associated with the, with the social media side. And I don't think we've given enough guidance to, to be able to sit back and relax and say that we think we can have given enough that people would be responsible and be able to be held accountable for their behaviour without, you know, the finger kind of first pointing at us to say, Well, what did you do to ensure that everybody understood that and I mean, our views have always been to make sure that whatever we do whatever you do on social media, make sure that you behave beyond reproach given that it's such a fluid kind of medium I think that's the kind of stuff that we've seen… I mean, we've seen horrendous knee jerk reactions about things that if it was in the day of the postage system, I mean then these things would never even come to light I mean one person would aerated it.”*

This highlights an underlying implicit concern as to exactly what and to what extent do’s and don’ts are incorporated in the organisations' governance, procedures and policies. The question posed by some interviewees was to what extent the do’s and don’ts start infringing in the in-between grey area that may compromise employees’ individual right to Section 16 of their constitutional right to freedom of expression. This is further complicated when a message or post on an OSN is unintentionally articulated ambiguously, by an error sent to the wrong recipient, finds itself on an unintended public forum, or purposely taken or manipulated out of context as expressed by a manager from the health sector.

> *“It's a complex, it's a complex situation that requires, you know, sensitive navigation to be honest, something that, to be honest with you, I mean, I'm not sure that we as organisations are well equipped to handle.”*

It is when considering an individual’s right of freedom of expression that a unanimous consensus from the interviewees was that this freedom comes with the responsibility of when, where and how to exercise this right appropriately or as directly conveyed by a hospital manager

> *“Yes, freedom of speech is a right that comes with responsibilities.”*

And goes on to say:

> *“…but responsibly understand, again, the target audience and their ability to comprehend and understand and, and never put things in isolation have the background and obviously, I think our values per say this company of integrity, truth and so forth, need to underlie that. I mean, you can't say out of, you're not free to lie.”*

Or in the case of the CEO of a financial services company

> *“I think right to freedom of speech, as long as it's not going to offend anyone. Sexual, racial, political, so freedom of speech, but be aware of the impression that's being created about the business.”*

A few interviewees highlighted the dilemma of appropriate content sharing concerning what is acceptable to one culture but not necessarily to another culture. The complexities of this dilemma have been explored as a concern regarding the right to personal privacy.

This is where all interviewees would fall back on underlying the theme that was both explicitly and implicitly threaded through all the interview transcripts of the threat of consequence. This threat of the consequence of your actions engaging on OSN platforms is not restricted to the consequential action by the organisation but from your personal social circles and society as a whole. This means you may be answerable for whatever you share engaging on an OSN platform, not just as an employee but as a private individual.

Several well-known isolated incidents were alluded to by interviewees emphasising that losing a job because of an inappropriate post or message may be far less severe than an outcry and wrath of public members (Sunday Independent, 2019). The concern of the interviewee as management within an organisation was that the consequential rebuke of such an incident is not limited to the individual but often implicates the organisation, the employee, or other stakeholders by association. However, the threat of such a possible devastating consequence was on the side of responsible behavioural intent when engaging on OSN platforms that go beyond the do’s and don’ts laid out in the organisation’s procedures and policies.

Pushing for further discussion around the consequence of irresponsible behavioural intent when engaging OSN platforms, it became apparent that there was an uneasiness around how one governs and addresses the threat of unforeseen consequences through policies and procedures. The best approach by the interviewees as managers and leaders within the organisation was to create and emphasise a guideline of online self-awareness by the employee of their intended behaviour.

> *“…there’s again awareness that we’re creating on that where people need to understand that as much as you’ve got your own private life and we respect that and you’ve got freedom of speech all these things that’s very important in our demographic society, the organisation’s got clear standards, clear morals, clear guidelines and even if you contravene those morals and*

> *ethics in your personal capacity away from work, there's going to be consequences."*

Of noted importance in the above response is that even though an employee's personal life is respected as private, once in the employ of or as a stakeholder of the organisation, all employees or other stakeholders are held accountable for their behavioural intent to the organisation for all activity on any OSN platforms even when engaging in a private capacity. This is again supported by an interviewee who emphasizes an employee's accountability when engaging on OSNs on their personal social networks when matters involve mention and association of the organisation.

> *"We've circulated many policies, informing staff of the do's and don'ts, even on your own private social networks. If your communication involves the company's name, if it involves the work that you, if it involves any of the clients that are treated in this company, they clearly know and where they've infringed those policies we have taken appropriate sanction including dismissal and the hate speech and all those sorts of things. So yeah, if it any way relates to your work to the company, it's investigated, appropriately."*

Governing an employee's private life with do's and don'ts was potentially recognised as a grey area when relating to the interviewee's personal moral code and values concerning an individual's right to freedom of expression or speech. It is here where the nature of OSN as a communication medium interferes with what may be viewed as an individual's autonomy to live and say what they see fit in their private life. This autonomy is often characterized by idioms mentioned by some interviewees, such as "what happens in Vegas stays in Vegas" or "what goes on tour stays on tour." However, with the advent of the OSN phenomena, this type of autonomy in behaviour is becoming increasingly difficult to manage. A parallel drawn by one interviewee when engaging and sharing on OSN platforms to what was previously imagined as life in a village whereby the nature of the proximity within the bounds of a village environment, an individual finds it difficult to be differentiated by their life in a professional capacity to their life in a private capacity. In the words of the interviewee explaining:

> *“I mean, I'm the paramedic that has a social life and I’m married and does, helps out with the Scouts on weekends, you can never divide that up. You can never say well my opinion is only as me is in this corner. It's that whole person, so whatever you put out there, represents that whole person, so, and that's the trade-off that comes with social media, you're not able to differentiate between this personal person and this professional person.”*

It was inferred from the above that in this type of environment, “everybody knows everyone’s business.” A view that was supported by another interviewee responding to the previous analogy of the exposure of one’s personal space living within the confounds of a village,

> *“One hundred per cent. Because that’s what I’m saying. If I get caught drunk-driving and somebody takes a picture of me and puts it on Facebook as I am being arrested for drunk-driving – I didn’t give them permission, but I didn’t have to give them permission, because it’s in the public space, but that will affect me at work. You know? So, sometimes I think it is better not to belong to these platforms, but if you don’t belong to them, then you don’t know what other people are saying.”*

In subsequent interviews, the interviewees appeared to agree that living in a social structure exposed within the confines of a village is analogous to belonging to the world of virtual social networks of ONS platforms. Furthermore, from a personal morals viewpoint, a few interviewees seemed to identify and gather some comfort in the familiarity associated with the sensitivities and complexities of living in a close-knit community.

A recent study on the effect of OSN usage on personal well-being revealed that passive use of OSNs observing the social status of others could lead to jealousy and envy, resulting in unhappiness. Whereas active usage of OSNs can increase the feeling of connectedness and increase bridging social capital where the individual feels part of a broader community having access and exposure to emerging information and different thinking.

When looking at how an organisation should govern this environment of close virtual proximity enabled through the advent of OSNs, again, the interviewees believed that posting inappropriate messages or content is governed by society itself, as observed and stated by a manager in the healthcare sector.

> *"So that it's a widespread across a case law already shows you that we didn't have to strictly govern this as governing it. It is a behaviour that you need to be made aware of and society will punish you, if you on a social side misbehave, society will turn against us; almost like a narcissist behaviour, society will turn around against you and punish you not as much as law, society will punish you more."*

When discussing governing the exposure to institutional risk through the use of OSNs by all stakeholders of an organisation within the context of the individual stakeholder's constitutional right to freedom of expression, the consensus amongst all interviewees was that the well-being of the organisation supersedes that of the individual stakeholder's right to freedom of expression. One can draw a parallel to the West African Akan and Southern African Ubuntu philosophies which draw on the community's well-being before that of the individual (Etieyibo, 2016; Molefe, 2016; Wiredu, 2019).

> *"The value of a person in Akan traditional life and thought thus represents an attempt to resolve issues of identity, freedom, and morality in favour of a communalistic way of life."* (Antwi, 2017)

The introduction and adoption of the OSN phenomena as a medium within a social network infrastructure within a social philosophy of communalism in an African context is of vital importance.

> *"In an attempt to finding a solution to these and other social problems facing Africa, an appeal must be made to Akan traditional and living philosophy of communalism. Communalism, as defined by Gyekye, is the doctrine that the group or society constitutes the focus of the activities of the individual members of the society. As a social construct,*

> *communalism insists that the good of all determines the good of each. It is therefore expected that every member of the society will work for the good of all, which also takes into account the individual good."* (Antwi, 2017)

This would suggest that the traditional African approach to social networks may need to adapt to the notion through the technology of radical transparency when engaging on an OSN. As one of the interviewees explained:

> *"… there is no such thing as the invitation when you have a ceremony or whatever you know. So you don't go out to neighbours and sent them invitations because as soon as you slaughter, yeah, basically it's for everyone to eat. Yeah, yeah. So you'll find that people will share because they still believe in that, they're sharing information whereas now they need to think that, you know, this information is confidential, it cannot be shared but they still share it, because in the back of their minds they thinking that is part of what I do at my township or where I stay on the farm or whatever you know."*

This was reiterated by a compatriot hospital manager within the same healthcare organisation:

> *"I do feel there's a different view on sharing of that kind of information and what it means to share information and I've recently in some leadership forums discussed and looked into the different views be it westernized views of certain interactions versus more Africanized or African views of interaction and the community concept poses an interesting question regarding social media, I believe, because it you know, inherently there's a greater sense of community in African culture and it sort of what is out there and is social media not just an extension of that, an extension of interacting and connecting and speaking, and then what we might see as an organisation, as sharing inappropriate information such as head of state or, you know, a very important person, etc. in a hospital is sort of being shared*

> *in a sense of respect, not to brag, not to show off, not to breach confidentiality, but to say, you know, we're proud of what we're doing this is who is with us, a part of our community, heritage, history, etc.”*

Within the Akan traditional and living philosophy of communalism, as defined by Gyekye, the emphasis on the benefit of all within the social network determines the ultimate benefit of the individual belonging to the social network. Whilst the concept of sharing information may be embedded within the Akan traditional and living philosophy of communalism, the potential damage caused by the concept of radical transparency should be considered by adapting traditional values to the unfolding of the technologically created phenomena of OSNs. As noted earlier by one of the interviewees, the sharing of inappropriate content is governed by the social network itself.

The potential consequences will govern behavioural intentions, whether it be through fear of losing their job through legislated case laws, being shamed within the organisation, or worse still, being publicly shamed. All instances of discussion of the organisation's governance, policies and procedures regarding responsible OSN engagement revolved around the dominant behavioural intent by all employees being ultimately controlled through consequences of sharing inappropriate content, as summed up by an interviewee:

> *“That's the only way that we will overcome all the problems that we have, but to put the restrictions of you can't see this, you may not say that, you can't say, so it’s the same with the derogatory remarks people say. Let them say that and see it's the society will sort out people that is behaving inappropriately.”*

Organisational values and culture are not just a reflection of the organisation’s ethical climate but are used to protect the moral fibre of the organisation and its stakeholders. This moral fibre needs to be akin to and respect the diverse values and cultures in modern organisations, particularly the diversity in South African organisations. Irresponsible engagement on OSN platforms can threaten this moral fibre. An underlying message from all the interviewees is that tightly aligning OSN engagement with the organisation’s values and culture is the bastion against irresponsible OSN engagement.

Professional values of online behaviour represent the employee’s professionalism within the organisation’s value system and culture. Therefore, as an employee, an awareness of the organisation’s digital presence on sites such as Facebook, LinkedIn and other industry-related sites and an awareness of the approach to engaging with OSNs in a professional manner that reflects the professional values will maintain the integrity of the organisation’s values and culture.

> *“We talk about the fact that you carry your professional brand with you everywhere, so don’t ever think of your professional brand being work only and your personal-. The two are so intertwined. A mistake on one directly impacts the other. We talk about that a lot.”*

4.2.14.2 Organisational Loss of Control

In addressing the notion of “loss of control” by the organisation when it comes to responsible employee engagement on OSN platforms (Linke and Zerfass, 2013a; Swerling, Thorson and Zerfass, 2014; Zerfass and Schramm, 2014), there were three direct approaches that were uncovered namely:

1. Defining clear, documented governance and policies on OSN engagement as an employee and stakeholder.
2. Training and Awareness of OSN engagement.
3. Decisive action whenever there is a breach of compliance with the organisation’s governance or policy.

The researcher now unpacks each direct approach to addressing the notion of “loss of control.”

4.2.14.3 Defining Clear Documented Governance and Policies

All larger organisations have a social media policy that outlines what you can and cannot say and what you should or shouldn't do on various or specific OSN platforms, such as Twitter, Facebook or LinkedIn etc.

These policies invariably form part of the organisation's induction programme and are often part of the annual compulsory compliance training for all employees. It is thus conceivable that most of the organisation’s employees should know the basics of the OSN policy. As with the evolving nature of OSNs regarding technology and use, these policies are regularly adapted. This can often be on a trial-and-error approach by reacting to incidents that may occur within the organisation or other organisations in the same or other industries. The approach is thus more reactive and preventative than proactive.

> *“It could always be better so I mean again from an awareness and policy point of view and all of that, I mean we try our utmost best to be as effective as possible but I mean it could always be better there’s always gaps, where you get a gap and sometimes it’s trial and error, which is not the best approach.”*

There is a three-phase general approach to the development and implementation of procedures and policies about the phenomena of evolving OSN platforms.

The first is to develop the policy by adapting industry standards to the organisation.

The second is to continually enhance the policies as new vulnerabilities regarding loopholes are discovered through the exposure of incidents in the organisation or the macro-environment.

The third is regular training and awareness of the current policies and updates.

This was succinctly stated as:

> *“There’s a policy, there are tests on the policy, and there’s training, that’s the three mechanisms.”*

As with the development of most governance and policies, when it comes to OSN engagement, there is a reliance on professional industry standards and norms concerning business transparency and privacy and confidentiality. Industry-specific standards are followed within both the South African and International contexts as per the examples which follow:

South Africa

a. Health Professions Council of South Africa (HPCSA).

b. The Medical Protection Society Limited (MPS).
c. National Health Act 2003.
d. Protection Of Personal Information Act, 2013 (POPI).

International

e. General Data Protection Regulation (GDPR).

Throughout the interview process, it was clear that in both the health and financial sector, the confidentiality and privacy of the organisation's clients, as one would expect, is of paramount importance. Protection of client confidentiality has been a business standard in these sectors since its inception. The invasion of privacy and exploitation of privacy through the advent of the OSN phenomena (Cadwalladr, 2018; Francis and Wagner, 2018; Gruzd, Jacobson, Mai, and Dubois, 2018; Wolverton, 2019) has given rise to both The Protection of Personal Information (PoPI) Act in South Africa, as well the Europe Union's General Data Protection Regulation (GDPR). Both aim to defend the individual's constitutional right to privacy, through the protection of personal information entrusted to a reliable and professional third party.

In the health sector, however, the history of patient confidentiality goes back to the Hippocratic Oath embedded in today's code of ethics practised by medical practitioners (Higgins, 1989). Certified South African medical practitioners subscribe to the Health Professions Council of South Africa (HPCSA), and the Medical Protection Society Limited (MPS) and in turn to the National Health Act (2003) (South Africa, 2004)

In particular, Chapter 2, Clause 14 of the National Health Act (2003) has a stringent patient confidentiality clause regarding a patient's health status and health records. As quoted below, this already gives the health sector's governance and policies a "one-up" regarding privacy and confidentiality.

> *"…in the healthcare market, I think there we're one up because you know, throughout the ages it's not a POPI Act or what's happening now, I mean, the Healthcare Act has been out and again, your nursing staff and those people are trained in that Act when they're at university and colleges so there's a bit more*

> *guidelines in healthcare regarding what is the do's and the don'ts."*

Three of the interviewees authored their organisation's Social Media policy in which they found guidance in templates of policies using industry standards, as stated by an interviewee from the financial sector.

> *"I used some templates. But I wanted to have something for us because our data is also so important to our business."*

Or, in some ways, a more cynical comment from the director of communications from a healthcare organisation:

> *"And I can tell you that I wrote the social media policy. Okay. I can guarantee you, nobody reads it, including these okes that have told you that we need an induction. Ask them to show you where to find it and what it says."*

The general sentiment from the interviewees is that all organisations need formal governance that sets clear boundaries of organisational practices and industry standards, particularly regarding the privacy and confidentiality of patients/customers in the healthcare sector or clients in financial services.

4.2.14.4 Training and Awareness

As a best practice in today's corporate governance, training and awareness of governance and policies should be part of the ongoing process of an organisation's induction programme for both new and existing employees (Grobler, 2005).

The need for training and awareness regarding the do's and don'ts of OSN engagement by employees and the risks of viral exposure of both intentional and unintentional use of OSNs by the interviewees was overwhelmingly unanimous.

The interviewees generally agree that their organisations guide the use and risks of OSN usage. However, most interviewees had a general feeling that current programs do not sufficiently address the risks associated with evolving nature of OSN engagement, both technologically and regarding our changing social and behavioural norms. This perceived shortfall in training and awareness is not seen as negligence by the organisation. It is rather associated with the difficulties in foreseeing the possible loopholes that occur as social behaviours adapt and change to the development of new technologies that, in most cases, are either untested or unregulated within the business environment (DeNardis and Hackl, 2015; Obar and Wildman, 2015).

A knowledge gap regarding awareness and unfamiliarity of the risks and implications of unintentional OSN engagement became apparent from the start of the interview process. In particular, the researcher had to take the time to point out the potential danger of OSN usage through innocent examples.

An example used in all the healthcare and some of the financial organisation interviews was of using the WhatsApp OSN platform to disseminate patient information directly from an accident regarding patient vitals and possible photographs of an injury to a medical practitioner to determine the most appropriate practitioner or specialist for treatment.

The National Health Act (Act No. 61 of 2003) (South Africa, 2004) is clear that the patient's information belongs primarily to the patient and that all healthcare professionals are required to protect the patient's right to confidentiality as stated in the Guidelines Practice for the Good Practice in the Healthcare Professions by the HPCSA

All the interviewees with whom this example was discussed agreed that efficiencies gained in speed to disseminate this type of critical information using an OSN platform could be medically beneficial and potentially lifesaving.

> *"We know that at three o'clock in the morning if you send the whole ECG to the cardiologist, he gets out of bed, and he'll be there earlier to take the patient to Cath Lab. There's a definite medical benefit."*

When asked who owned the disseminated information, only three interviewees cited WhatsApp Inc. and its parent company Facebook, in theory, owning or having the most recourse to the patient's data and possible image. Therefore, to understand the ramifications of a possible breach of patient confidentiality as stated in the National

Health Act, we need to briefly explore the terms and conditions a user agrees to when using WhatsApp as an OSN platform. The following extract appears on the current terms and conditions found on the WhatsApp website:

> *"Facebook and the other companies in the Facebook family also may use information from us (WhatsApp) to improve your experiences within their services, such as making product suggestions (for example, of friends or connections, or of interesting content) and showing relevant offers and ads."* (WhatsApp, n.d.).

Examining the full legal implications regarding the exposure of patient information in an emergency situation using the WhatsApp OSN platform is beyond the scope of this research.

Throughout the interview process, there was a lack of awareness or confusion about potential patient confidentiality violations when an emergency services medical practitioner, hospital manager, general medical practitioner or specialist innocently disseminates patient information on OSN messaging platforms. This is identified by the sentiments of a hospital manager when talking about using WhatsApp group functionality to manage hospital staff information and disseminate information.

> *"I'll give you a classic example; if I, if we go onto WhatsApp now there are, I belong probably to about 12 groups, hospital groups, hospital-specific groups and I can scroll through on any particular day and I can guarantee you there's sensitive information on that WhatsApp, so if we saying in the one hand corporate governance in the one hand we saying this is how we act, this is how we behave, this is what our values are, and in the other hand people think social media's Facebook, it's not just Facebook,… I mean, WhatsApp belongs to Facebook; all you have to do is look at WhatsApp, there is patient information on WhatsApp, people talk about people, about complaints about doctors on the WhatsApp; it goes totally against what our values are saying, and these are not staff members that you talk about in the ward, nurses and, these are senior managers that we*

> *talking about, so there is stuff on there that should never ever be on there, ever."*

This lack of awareness of such violations is apparent in the financial sector but less so than in the medical sector. Consideration must be made that the need to disseminate confidential information is not as critical in the financial sector as in the medical sector.

For the professional in the financial sector, it should be noted that when dealing with a client's finances requires both professional and business acumen and a cordial setting. In the medical sector, even though the HPCSA binds all healthcare professionals, the nature of healthcare not only exposes the patient to a lower stature, but the environment of a hospital, health centre or public emergency such as an accident scene also exposes the patient to the public. Induction programmes covering OSN organisation governance and policies, although not sufficient, appeared to be more formally organised in the financial sector than the health sector, as stated by a divisional head of a financial services organisation:

> *"So we certainly getting better. I don't think that we are where we need to be, but I think as an organisation, for me, the big thing would be around awareness and training. I don't think it's as front of mind as it probably should be for the organisation. There's a feeling that I get across the organisation… It's been a long time since I was inducted, but it absolutely must. I think it absolutely must."*

As mentioned earlier, the difficulties associated with the health sector with a higher staff turnover and dealing with nursing agencies are balanced by complying with the National Health Act, HPCSA and MPS.

A crucial finding is that both the health and financial sectors acknowledge that training and awareness of OSN governance and organisational policies need to be a key factor in the induction programmes and regularly be reinforced as stated by the financial sector:

> *"Some individuals just don't see it and the consequences of it. So how do you create that awareness and make people fully understand."*

And as stated in the medical sector:

> *“I think there's a big gap for some social media education, which may result in a couple of, you know, policies coming out of it, but it almost automatically would, I guess, result in some policies, but it's really around the education.”*

In addition, the larger organisations provide training by educating, in particular, the more senior employees on the effective use of what and how to say on the preferred selected OSN platforms the organisation is comfortable engaging with.

> *“… more senior levels, goes through training on what to do on these various platforms, which one the bank likes us to use versus, you know, please stay away from, and things like media training, because again, same thing, the radio adverts, or radio interview, can get out of hand quite quickly.”*

In contrast, for some of the interviewees, this lack of training and awareness echoed the frustration that paranoia and fear limit the proactive use of OSN engagement, as echoed by the following interviewee

> *“We're not doing well at educating people on how to use social media we are still leaning towards if you're unsure, rather don't and we just have to look across like the senior management team within the company. None of them engage in social media proactively. They're all rather hesitant and I think they scared, not scared, is scared, too cautious, yeah, cautious, but cautious, in my opinion, being too far cautious in engaging with social media, they’d either rather wouldn’t, or they sort of go create a profile and that's all that ever happens to it.”*

All interviewees made it clear that as an evolving, often unknown phenomenon, training whether internal or external regarding all aspects of engagement with OSN platforms is crucial within the organisation.

4.2.14.5 Decisive action in breach of compliance with governance or policy

All interviewees had a non-tolerance approach should any employee breach the organisation’s OSN policy and governance. All the interviewees agreed that OSNs have now become part of how the modern individual functions and communicates both in business and privately. They were in unison that access and engagement of the individual have become a personal right to be respected:

> *“We are also looking at other ways of potentially giving staff access to their social lives, social media lives without utilising the corporate backbone Infrastructure by creating WI-FI off a separate network sort of thing… We’re wanting to embrace digitisation in Its entirety and includes a big part of the digitisation, which is the way people communicate on social media, so that’s certainly an area we are more focused on now than we ever have been”*

It was noticeably evident from the interviewees that OSN usage needs to be embraced as a norm that is now entrenched in how society functions. The debate about the legal right to access social media and the internet in the workplace continues to be debated in various counties within the confines of the current law (Rosalind Davey, 2016). However, respecting the employee’s right of access to the engagement on OSNs is a discretion associated with the expectation of being accountable for responsible OSN engagement in compliance with the organisation’s policies and governance. The interviewees were in unison that should this discretion be infringed upon or the compliance of the organisation’s policies and governance be ignored, swift, decisive action against the employee should be taken.

The consensus from the interviewees was twofold. Firstly, it was evident from the responses that to limit the implications and reputational damage to the organisation through a breach in the policy of OSN engagement, it is best curtailed through an immediate and decisive action on the part of the organisation.

Secondly, swift, decisive action by the organisation sends a clear message that any abuse of an employee’s given rights of access to OSN engagement, whether intentional or not, will not be tolerated.

> *“Look I think there's a mature approach to your private life, I don’t ascribe to regulating people's private worlds. They obviously have access to the media platform or the social platform they choose but when they start linking that to the organisation and discrediting the organisation, we’re very decisive, whether it's in a private capacity wearing a company uniform it doesn't matter you've linked it to and then it becomes our problem.”*

The general view of the majority of interviewees was that the most effective way to limit the consequential damage suffered by an organisation when associated with an inappropriate OSN post or message by an employee is to disassociate the organisation from the employee immediately. It does not matter whether it may have been a simple expression that may have been publicly perceived as hate speech or sensationalism or whether it was sharing a personal conviction or fake news. This type of action will usually take the form of an agreed resignation or dismissal.

> *“If it’s linked to the company, I promise you it's decisive. They’ll no longer work here.”*

Though some interviewees sympathised with an accidental thoughtless unintentional engagement on an OSN, all interviewees seem to agree that limiting the reputational risk to the organisation required sending both a public and organisational non-negotiable message of disassociation and decisive action.

4.2.14.6 The Right to Freedom of Expression

In keeping consistent throughout the interview process, the researcher opened each interview by asking each interviewee how effective their organisation’s governance, policies and procedures are in tackling the notion of radical transparency engaging OSN platforms. The invariable response of the interviewees reflected the academic literature that controlling the impulsive human nature to voice one’s convictions and disseminate information on an OSN platform can be challenging.

Whether this type of engagement on an OSN platform by the employee is intentional or unintentional, controlling the resultant notion of radical transparency through employee representation can become problematic when relying on strict adherence to governance, policies and procedures. As a result, most interviewees' approach to controlling OSN engagement almost always shifted to reliance on company values and culture.

> *"So, I honestly believe that we cannot put rules and regulations and stop it. The only control that we will be able to get is to create the culture of take the person into consideration before you post, before you say, before you WhatsApp, because that is what it is about. So, it's all about creating the culture of strong values."*

Further discussion with the interviewees exploring the organisation's values and culture would inextricably shift towards the organisation's ethical quandary of protecting reputational risk in the context of an employee's constitutional and moral right to freedom of speech when engaging on an OSN platform.

Every interviewee understood that from the corporate ethics view, the organisation's reputational risk is to be protected at all times. This, however, is not to say the personal moral convictions of the interviewee as an individual did not sympathize with an employee who may have inappropriately, whether unintentionally or intentionally, exercised their personal right to express an opinion or belief that by association and having done so may bring the organisation into disrepute and possible litigation.

> *"…and it's difficult, it is difficult, and that's why I say I'm not calling it, either way, I'm not I'm not I'm not predicting how this company would react to it to something I'm not what I'm saying is what I'm saying is that this is a very good chance that if what a person has said is causing damage to the company, and again that goes to the audience, who's the audience? Because, because, because ultimately one needs to look at it and say, well, it goes back to this capitalism 101 because the company is about shareholders, so of course, of course employees matter, of course customers matter, but shareholders… we start at shareholders so what's the impact on shareholders…."*

Voicing one's convictions is directly linked to freedom of speech, often referred to as freedom of expression, as outlined in article 19 of the Universal Declaration of Human Rights (UDHR).

Interviewees from the Baby Boomer and X-generations born before the seventies, whose informative years from a social development perspective were not affected by the age of digitization, appeared more observant of the paradigm shift emerging through the development of social communication via the phenomenon of OSNs. As alluded to earlier, information dissemination from an OSN platform is an exact transcription. This is unlike what previously was known as the “bush telegraph”, which invariably tended to be flawed with inaccuracies and exaggerations. However, ~~the~~ like the “bush telegraph”, the transcribed message from OSN engagement often lacks the full context the message is intended to convey.

> *“I think we also need to remember that it's also because of how things have changed… because 20 years ago, putting out your own convictions would have been done in a way that was much more nuanced. Much more, you know, maybe it's in the context of a room of 5 people, ten people, 100 people is how you put it across. It comes with nuance, it comes with emotion, whereas today… and 140 characters leaving you, to what you do what you're putting on there… you need to understand what you putting on there is probably at least 80% chance that it will be perceived differently to what you meant.”*

Where does this leave the organisation in addressing how to control the reputational risk of employee engagement on OSN platforms whilst protecting the employee’s constitutional right to freedom of expression?

When employing an employee, whether permanently or on contract by the organisation, there is an implicitly expected duty by the employee to make decisions for the good of the organisation. Before the emergence of OSNs, the organisation would control its media relations through an appointed media professional who, as the public voice of the company, understood the moral obligations in upholding company values such as “*don’t lie to the media” and “use language responsibly, free from intentional obfuscation.”* (Bivins, 2006). In contrast, the organisation is now vulnerable to representation by every employee with access to the open nature of the OSN platform. When engaging on an OSN platform, the moral obligations of the employee expected by the organisation would be aligned with the organisation’s values and culture. Most interviewees stressed the importance of promoting and instilling the organisation’s values and culture and not just relying on governance and policies.

> *“It is what it is, it's about the values, it's the culture. If that culture is embraced and understood by each and everyone they will do what is best for the person and they will post accordingly, and they will tweet accordingly, and they will defend, and they will go out and be ambassadors for the organisation, for whoever, for themselves, for person-centred care, for a patient, for healthcare, for Greenpeace, or whatever.”*

From the interviewees, however, caution was expressed by certain of the more senior executive management that the expectations of good OSN usage driven through a value-based culture may be somewhat idealistic and still has many shortfalls. They emphasised that continued education on responsible OSN usage and highlighting the dangers associated with negligent ONS engagement is a far more pragmatic approach than only relying upon organisational values and culture.

> *“I can't say that, under the current economic climate, I don’t think a lot of people out there working for the sake of a job, not necessarily because they want to help care for people necessarily. So, you may have people that they don't necessarily believe in our values. I mean, can we say, put our hand on our hearts, that we always treat everybody with respect? For example, we don't, I'm guilty of it sometimes, and I forget that respect factor. So yeah, our values are great. And they are part of what we are and part of our DNA. But I don't think that that's sufficient. It's maybe an extra layer of comfort. But it's not the catch-all that I think I think we need; I believe that we should be doing more from an education perspective to the staff concerning the dangers of social media.”*

As reiterated by another interviewee,

> *“So I don't think so we can purely rely on our values; as I said, I think it should be part of, and you should always sign*

> *acknowledgement of that you understand the organisation's policy concerning social media.”*

All interviewees endorsed the individual’s human right to freedom of expression. However, they were adamant that this should not be to the organisation's detriment or expense through direct or indirect association.

4.2.14.7 Risks and Exposure

There was underlying confidence and positive sentiment by most interviewees that as long as there was an allegiance or loyalty by employees and other stakeholders to the organisation, there would be intended responsible OSN engagement. This means that the notion of “loss of control” is more manageable than imagined or projected; however, the fragility of an unintentional message or post, confidential or inappropriate, lurked quietly in the minds of senior management as explained:

> *“I mean, I'll give you this example. And I think it immediately raised the concern, we take a screengrab of a particular problem that we have, with a particular account, not even concentrating on the clinical information that may be there …. but there's an HIV or health status, that patient is actually being portrayed to parties within the organisation and outside that should not be portrayed at all. And that’s it exactly, but it's done, not the intention, but it's done.”*

Another concern was the impossible task of managing disgruntled employees once they left the organisation. Should the employee feel disgruntled by the organisation, there is the concern of the now ex-employee lashing out at their previous employer by exposing confidential information or public shaming the organisation.

> *“I agree, and I disagree. I think I mean, people may or may not understand the consequences at certain points in time, people may or may not care about the consequences, and I think that that's almost the bigger risk is, the less mitigated risk is that the ex-employee, the person with the insight no longer has an allegiance or loyalty you could, sure the loyal employee.”*

And then goes on to say

> *"How do you deal with the disgruntled, bitter ex-employee with knowledge inside information, names…."*

This emphasises the need, where possible, to manage and address employees' grievances once the employee-organisation relationship has gone sour. It may be wise to prepare management for effective exit conversations. A recent study has shown that taking the time to listen to an employee who has resigned may limit public exposure via an OSN once they have expressed their grievance (Kulik *et al.*, 2015).

4.3 QUANTITATIVE STUDY

4.3.1 *The Online Survey*

The quantitative survey used in the study was in the form of a questionnaire developed in Google Forms. This survey was distributed online through email or WhatsApp that could be accessed and completed on a mobile device such as a smartphone or tablet using the WhatsApp Messenger application or a webpage on a desktop workstation or Notebook. The questionnaire was developed during the period between July and September 2018. As outlined in the research methodology, the researcher has drawn on a pool of current and previous colleagues who were eager to participate and contribute to an evolving version of the survey ensuring ease of use, efficiency and effectiveness of the questionnaire. The test respondents were a representative mix regarding gender and age.

The final survey was sent out and facilitated through the management of the same respective organisations used for the qualitative research from October 2018 until February 2019. In all, a sample size of approximately 2000 employees was targeted. One of the financial services organisations asked that the ECQ of 29 questions be removed from the survey. As a result, the researcher received 348 responses, of which 328 were fully completed, and 234 included the ECQ. This equates to approximately a 16% response rate.

A PDF version of the online questionnaire can be found in the appendix. The following is the format of the data collected through the different sections of the questionnaire:

4.3.1.1 How the Survey data were analysed

The survey data was analysed in four interlinking phases, as shown in Figure 4.2 below. The data was analysed and assessed by Microsoft Excel, IBM SPSS (Version 25) and IBM AMOS (Version 25).

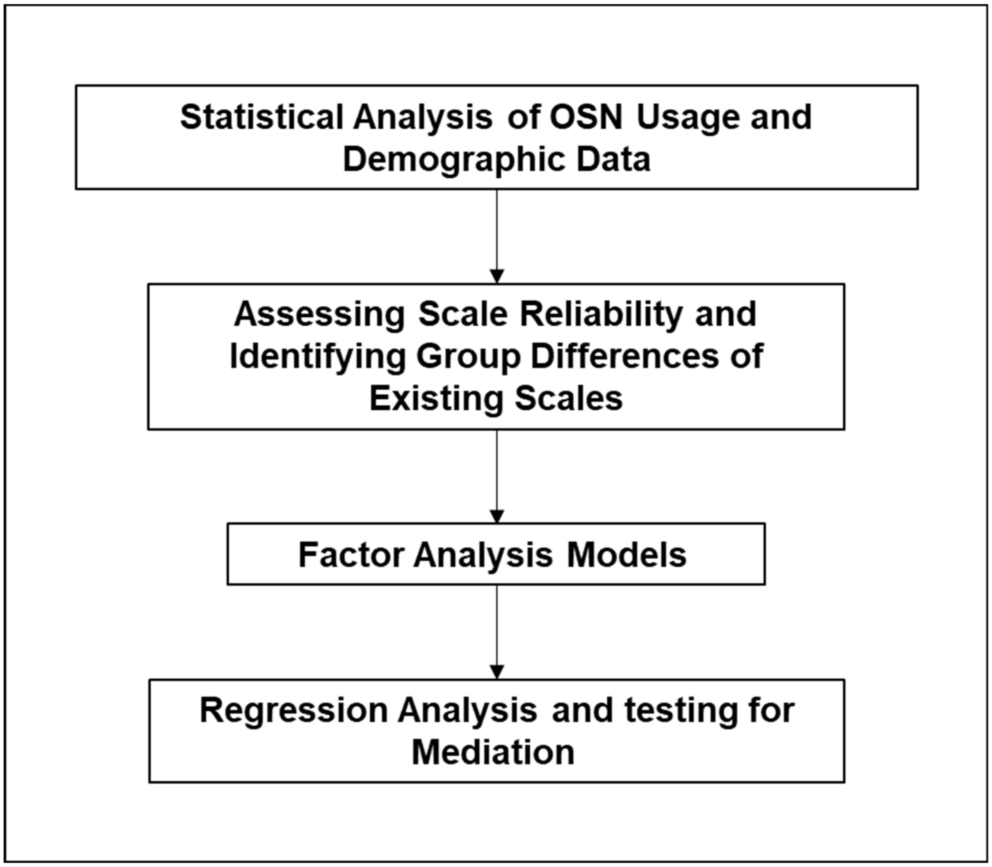

Statistical Analysis of OSN Usage and Demographic Data
Assessing Scale Reliability and Identifying Group Differences of Existing Scales
Factor Analysis Models
Regression Analysis and testing for Mediation

Figure 4.2 How the survey data were analysed

4.3.1.2 Gauging the factors influencing responsible OSN usage

In gauging the factors influencing responsible OSN usage, the result of the survey are analysed in four parts as follows:

1) Statistical Analysis of OSN Usage concerning Demographic Data: To assess the most used OSNs by employees in the financial and health sectors. To assess the most and less used OSNs regarding an industry, gender, generation and qualification levels.

2) Reliability and consistency, significant correlations and moderation effects

of the findings from the scales used in the survey: The assessment of Cronbach α using IBM SPSS was used to assess the internal consistency of the scales. The validity or construct validity gauges how well the data represents the assessed underlying construct. The quantitative analysis technique correlational analysis of the observed data are used to assess the construct validity of constructs defined in the literature review.

3) Factor analysis models: Factor analysis was used to ascertain potential underlying factors or components to reduce the number of items on each scale to a more manageable number. These are possible meaningful factors that are not explicitly observed but can be derived and inferred as underlying combinations of variables through the use of a mathematical model.
4) Regression analysis: Regression analysis was used to gauge and analyse the relationships between observed and latent variables. Regression analysis is used to test and evaluate multivariate causal relationships.

4.3.1.3 The measures and scales used in the survey

Table 4.2 Measures and Scales Used to Gauge Responsible OSN Usage

Category	Construct	Data Type
Demographics	Basic Information	Nominal
App usage	General Usage of most popular mobile and web OSNs	Interval / Scale (Likert type scale ranging from 1=Never to 5=Hourly)
Online Privacy Literacy	How literate is the respondent with regard to Online Privacy	Nominal
Security Behaviour Intentions Scale	What are the respondent's habits with regard to online privacy	Ordinal (Frequency Likert type scale ranging from based on 1=frequency of Never to 5=Always)
Texting Habits	The respondent's usage of hazardous texting habits	Interval / Scale Ordinal (Likert type scale

		ranging from 1=Never to 7=100% of the time)
OSN Addiction	Does the respondent suffer from OSN addiction	Ordinal (Frequency Likert type scale ranging from based on 1=frequency of Never to 5=Always)
Self-Efficacy	Self-Efficacy with regard to online privacy literacy	Ordinal (Frequency Likert type scale ranging from based on 1=frequency of Never to 5=Always)
Self-Esteem	The respondent’s self-esteem	Ordinal (Frequency Likert type scale ranging from based on 1=frequency of Never to 5=Always)
Ethical Climate	What is the respondent’s view on the Ethical Climate of the Organisation	Ordinal (Likert type scale ranging from 1=Strongly disagree to 7=Strongly agree)

4.3.1.4 The profile mix of the respondents

Table 4.3 Profile Mix of Resposndents (n = 328)

	Frequency	Percent
Industry		
Healthcare	143	43.6%
Financial Services	185	56.4%
Gender		
Female	183	55.8%
Male	145	44.2%
Generations		
Baby Boomer	41	12.5%
X-Gen	146	44.5%
Millennial	141	43.0%

Highest Qualification		
Matric	58	17.7%
Diploma	63	19.2%
Graduate	49	14.9%
Postgraduate	108	32.9%

4.3.1.5 The profile mix between industries

As a percentage proportion of the total healthcare sample (*n*=143) surveyed, there was no difference in gender representation, whereas in the financial sector sample surveyed, there was a 60% to 40% split in the representation of females in relation to males. About 50% of the respondents in the healthcare sector belonged to the millennial generation, whereas they represented 38% of the financial sector. The X-Generation represented 37% of the healthcare sector, whereas the X-Generation cohort represented 50% of the financial sector sample surveys. Baby Boomers represented 14% and 11% of the healthcare and financial sectors, respectively. Representation of highest qualification levels was in proportion to the sample sizes and was similar from both sectors, with the only significant difference being that 44% more respondents from the financial sector sample held diplomas. There was no significant representation of graduate and postgraduate representation between the two industry sectors under consideration.

In meeting objective three, gauging the opinions and perceptions from the sample of employees surveyed from the selected industries towards factors that influence responsible OSN engagement, the results were analysed in meeting objectives four, five and six by gauging

1. The perceived effect of individual employees’ online privacy literacy and security intentions.
2. The employees' levels of awareness towards psychological and external factors are affected by manipulated impulsive behaviour, habits, and OSN addiction.
3. The perceived influence of the employees' awareness of the ethical climate within the organisation.

4.3.2 *Statistical Analysis of OSN Usage and Demographic Data*

The researcher used Microsoft Excel, IBM SPSS (Version 25) and IBM AMOS (Version 25).to statistically analyse the responses from the questionnaire.

4.3.2.1 Gauging OSN usage

The respondents were asked to indicate the estimated frequency engaged on each of the sixteen most popular OSNs applications identified in the survey. Frequency engagement on each of the sixteen OSN applications was assessed as either hourly, daily, weekly or monthly. If the respondent was either unaware of the OSN or had never engaged with the OSN, they could select the option of “never”.

4.3.2.2 The purpose of gauging OSN usage.

OSN usage was identified as a variable in determining the validity of the objectives to gauge the level of responsible OSN engagement regarding the employee’s awareness regarding organisational awareness, online privacy literacy and online self-awareness. In measuring responsible OSN engagement, it is crucial to understand what type of OSNs are engaged with and the frequency of engagement.

OSN applications can be categorized into types used for social communication, such as Facebook, Instagram, WhatsApp or Snapchat or those utilized for business communication, such as Email, LinkedIn and WhatsApp. Other OSNs, such as YouTube, are recognized as video-sharing content applications that have been popularized for entertainment. It is also well-known as a marketing tool enabling the promotion of business concepts, products or services through indirect advertising, ‘*serving as a powerful tool for maintaining a product brand identity* (Cambridge, 2019).

In addition, YouTube is an effective and popular medium for education (Jaworski, 2019), whether it be a traditional documentary or a recorded lecture from universities such as Harvard, Yale or Oxford. Tutorials can be specifically tailored to this medium (Korich, 2016). Well known is the Khan Academy, founded by Salman Khan in 2009, where he explains its formula,

> *“That way, it doesn’t seem like I’m up on a stage lecturing down at you,” he says. “It’s intimate like we’re both sitting at a table*

> *and we're working through something together, writing on a piece of paper."* (Thompson, 2011).

When contrasting the usage of an OSN in the context of business communication to that of social communication, the impact of the employee's awareness of online privacy literacy and intentional privacy behaviour is critical in minimizing the risk of reputational damage. When an OSN is used as a business tool and not solely for social communication, the risk of exposure to the phenomena of radical transparency through the breach of organizational or client confidentiality can have devastating consequences.

4.3.2.3 Analysis of OSN's frequency application usage

As a study on the effect of OSN usage where usage is gauged using self-reported frequency engagement, whether it be hourly, daily, weekly or monthly or never, the impact of the work on organizational transparency and privacy led the researcher to believe that it was pertinent to assess the frequency usage and the time spent engaging with the more popular and well-known OSN platforms that would be utilized by employees within the organisations researched. As an employee of the organisation, whether OSN engagement be responsible, courteous, irresponsible, compulsive or addictive is representative of not only the calibre of person employed but the influence or level of control over the employee's online behaviour becoming to the organisation. Gauging OSN self-reported frequency engagement is as a representative irrespective of whether the engagement is for business or personal use.

Time engaged by the respondent on each OSN is correlated to the respondent's propensity to factors such as OSN addiction and texting habits. Other key correlations would be the respondent's competency regarding online privacy literacy and the respondents' past, current and future online security behavioural intentions.

Of the 16 OSN applications surveyed, six of the OSN applications, namely Google+, Tumblr, Viber, WeChat, Snap Chat and Tinder, were reported to have less than 10% frequency engagement by the respondents. For this research, OSN applications that less than 10% of respondents currently engage with were deemed not to have had a significant impact on the organisation and were thus excluded from the further in-depth analysis. This left ten OSN applications with their associated frequency usage, which are depicted in Figure 4.3

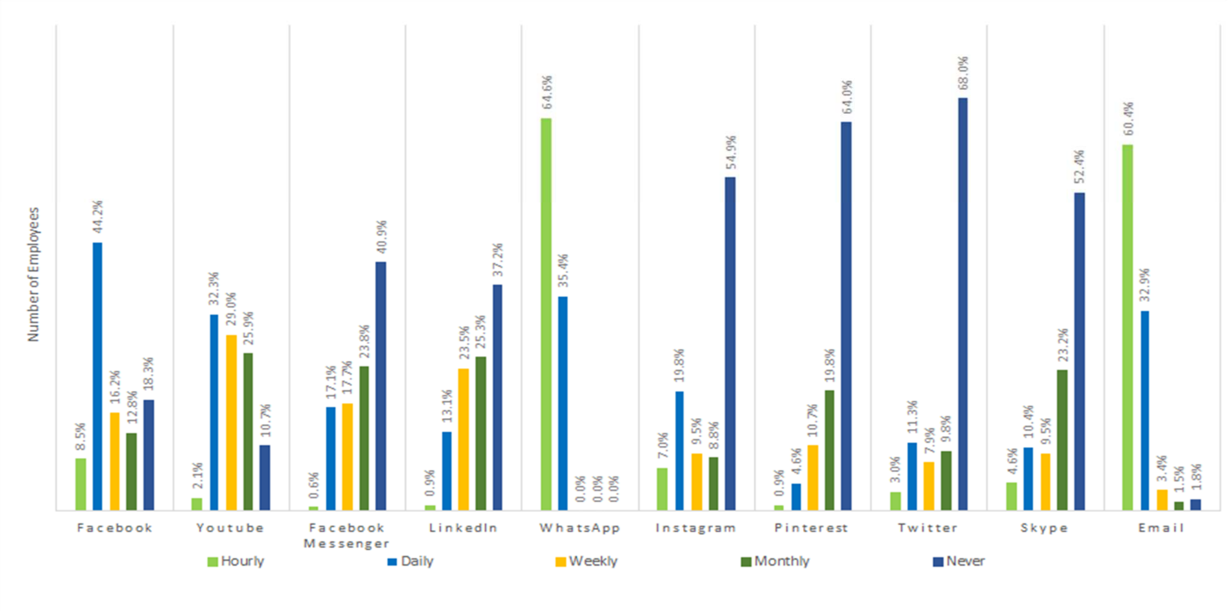


Figure 4.3 Usage of the top ten OSN Apps

The results seen in Figure 4.3 were ordered regarding popularity to determine the popularity of OSN applications amongst employees contrasting OSN usage with no usage at all, i.e. “Never”. Then, any regular usage, whether it was “Hourly”, “Daily”, “Weekly”, or “Monthly”, was grouped as shown in Figure 4.4.

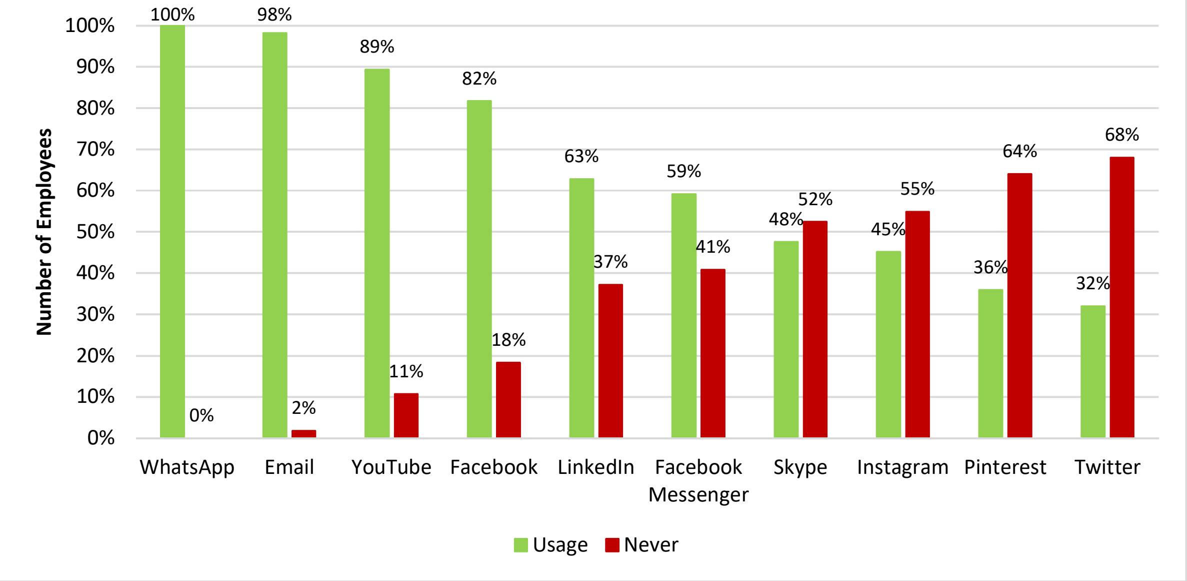


Figure 4.4 Usage versus Non-Usage

The results of OSN frequency usage were dominated by OSN apps associated with business communication, such as WhatsApp and Email, followed by the promotional, entertainment and educational OSN, YouTube. Facebook, a predominantly social OSN, was fourth regarding frequency engagement. Regarding popularity and usage, LinkedIn, regarded as a business OSN application, was ranked fifth in frequency usage among the top ten used OSNs surveyed.

The first two options in the survey regarding frequency usage were hourly and daily use, followed by weekly, monthly and never. Hourly use would likely fall in working time. Daily use, although not as frequent as hourly, was likely to still fall during work hours. It follows that hourly use would be used daily, adding to daily use, enabling a comprehensive view of daily use as seen in the stacked bar graph shown in Figure 4.5.

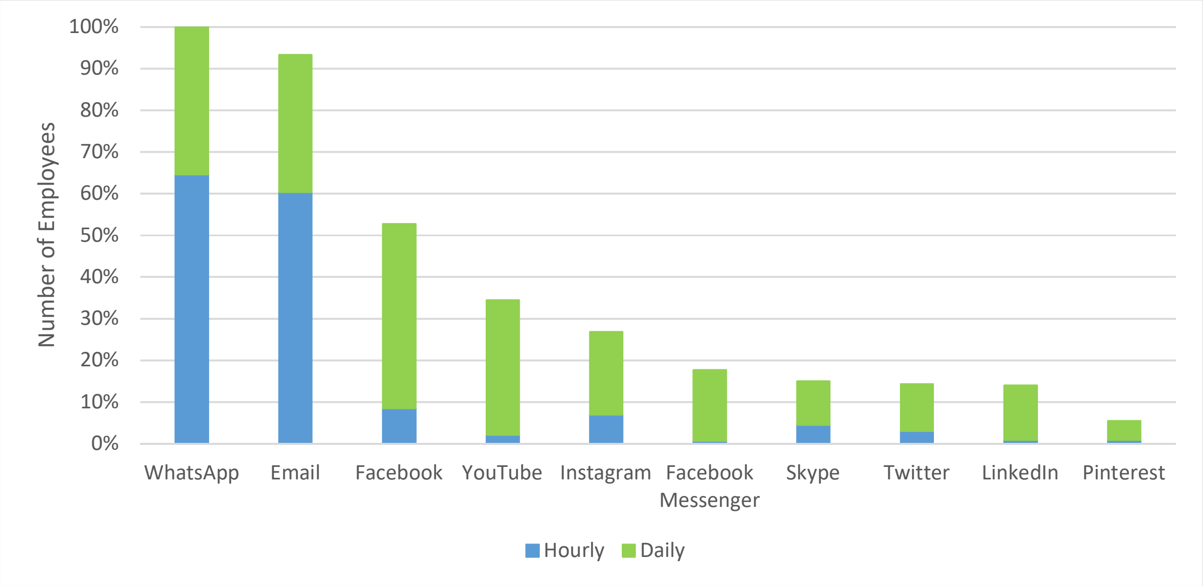


Figure 4.5 Daily and Hourly Usage

The use of OSN for business communication is dominant, where 100% of all the respondents use WhatApp at least daily. Of which 64.6% claim to use WhatsApp hourly. Email follows closely, where 93.3% of all the respondents use Email at least once daily, and 64.7% claim to use Email hourly. In comparing WhatsApp to Email, it should be noted that Email is traditionally not a mobile device application. Approximately half (52.7%) and a third (34.5%) of the respondents claimed to use the more social and entertainment-based OSNs, Facebook and YouTube, respectively.

However, less than 10% of the total respondents' self-reported hourly usage of Facebook (8.5%) and less than 3% of YouTube (2.1%) self-reported usage.

As a strictly business OSN platform, LinkedIn was self-reported to be used daily by 14.0% of the respondents and a mere 0.9% self-reported hourly use.

4.3.2.4 OSN Usage - Research Findings versus General Usage in South Africa 2018 – 2019

The OSN usage data were collected from October 2018 until April 2019. This allows a comparison of this study with the general findings of Social Media usage in South Africa from the *We Are Social and Hootsuite* reports from February 2018 and January 2019 (We Are Social and Hootsuite., 2018, 2019). In addition, the top ten usage apps in this research, except for email, which is not regarded as an OSN, were compared to the usage reported by *We Are Social and Hootsuite.*

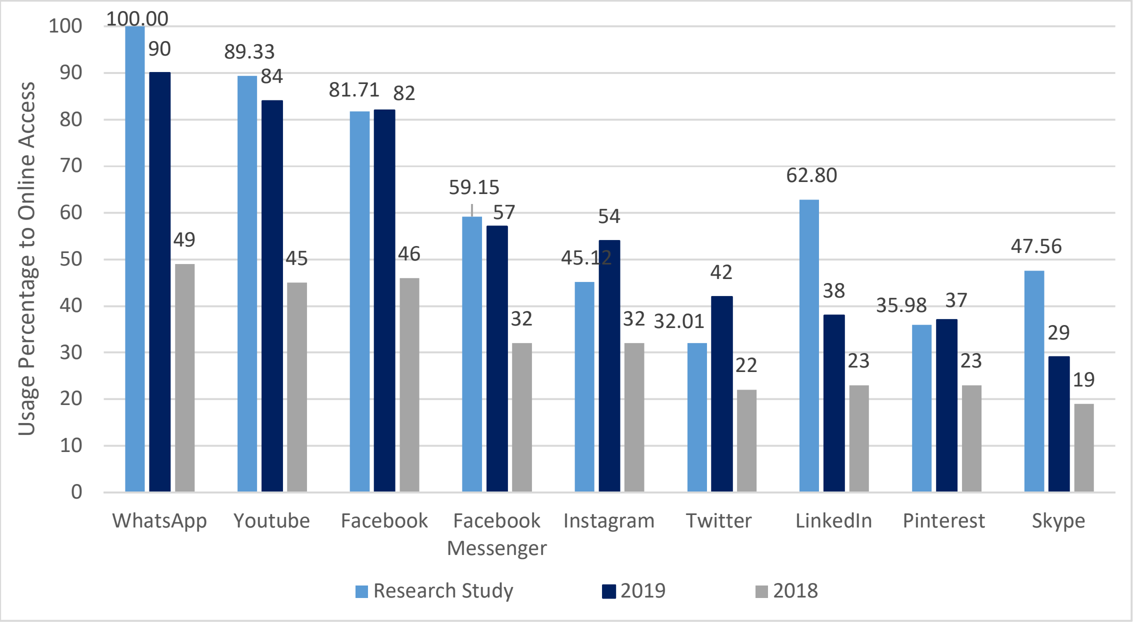


Figure 4.6 Research Findings versus General Usage in South Africa

As shown in Figure 4.6, the usage percentages from the research study follow a similar trend line to that of the general South African social media usage of 31.18 and 30.81 million South Africans that have internet access as of January 2019 and February 2018, respectively. It should be noted that the research study sample was of industry employees, where 82.2% had a minimum of a post-matric certificate or diploma, and 47.8% were graduates or postgraduates, indicative of the educational level of the research study sample. In contrast, the results presented by *We Are Social and Hootsuite* cover the general population regardless of education. This may account for the slightly higher usage of OSN platforms such as WhatsApp, LinkedIn and Skype geared toward business communication in this study sample of business users. The percentage usage of Facebook, Facebook Messenger, YouTube and Pinterest were almost identical. The research study results were of particular interest to the researcher, confirming an almost suspiciously high increase in OSN usage compared to the increase in South Africans who have Internet access from February 2018 to January 2019 revealed in the *We Are Social and Hootsuite* reports.

These results indicate that research sample study results align with those of other professional research organisations.

OSN Usage by Industry, Gender, Generation and Qualification Levels

4.3.2.5 Summary of OSN Usage by Industry, Gender, Generation and Qualification Levels

4.3.2.5.1 Industry

Healthcare shows a slightly greater usage of social-based OSNs as a collective than those in the financial sector. Of note, there is a higher engagement with Facebook by healthcare compared to financial services, with overall higher engagement with LinkedIn.

4.3.2.5.2 Generation

The findings show that over 80% of the Millennials, 76% of the X-Generation and 64% of Baby Boomers prefer text over voice notifications (Reyes, 2019). Furthermore, this research study shows that text communication is not only preferred but is used across the generations concerning business communication daily.

Generational differences are predominantly in the social and content-based OSN platforms dominated by the Millennials in daily frequency engagement. This would be consistent with the findings of the “Need to Know, Want it Now” (Bolton *et al.*, 2013) culture that has fuelled today’s mindset of millennials.

General usage by millennials is only approximately two times greater than the other two generations. Millennials, however, engage eight times more daily than the Baby Boomers and two and a half times more than the X-Generation on the OSN Instagram. This is likely due to the nature of Instagram being a different medium of instant communication through images and *like* “👍” or *not like* “👎”emojis rather than the typed word.

4.3.2.5.3 Gender

Females dominate the daily frequency usage of the more socially orientated OSN platforms, namely; Facebook and Facebook Messenger which show 19.4% and 29.6% greater daily engagement, respectively, to that of their male counter parts.

Males dominate the daily frequency usage of the business-oriented orientated OSN platforms, namely; LinkedIn and YouTube which show a 15.4% and 28.6% greater daily engagement, respectively, to that of their female counter parts.

The frequency usage of Twitter is more than three times higher for males in daily engagement than that of females.

These gender differences in the frequency of OSN engagement are in keeping with the research on gender differences and OSN engagement (Atanasova, 2016; Karatsoli and Nathanail, 2020). In addition, women gravitate to OSNs with more visual content, whereas men gravitate to text-orientated content.

4.3.2.5.4 Highest Qualification

Results show that those with a matric or certificate qualification have a higher daily engagement with the social-orientated OSNs Facebook, Facebook Messenger and Instagram. In contrast, graduates and postgraduates show a higher level of engagement with the business-orientated OSN app Email, LinkedIn, Skype and Twitter.

Lower education and qualification levels tend to favour the social-orientated OSNs, whereas graduates and postgraduates favour the business-orientated OSNs.

4.3.3 *Assessing Scale Reliability and Identifying Group Differences of Existing Scales*

Assessing scale reliability and identifying group differences (of existing scales). The results from the scales adapted and tweaked gauging the influencing factors towards responsible engagement as described in the methodology chapter regarding reliability, where reliability is an assessment of the consistency and dependability of the construct defined regarding the objectives.

4.3.3.1 The Interpretation of a Correlation Coefficient

The interpretation of a correlation coefficient conventional approach of Pearson correlation coefficient (r) strengths and ranges for the purposes of this study are, very strong (0.9–1.0), strong (0.7–0.89), moderate (0.4–0.69), weak (0.2–0.39) and very weak (0–0.19) (Schober and Schwarte, 2018; Liang *et al.*, 2019).

4.3.3.2 Online Self-Awareness

Assessing the construct defined in the literature review under 2.7 “A Case for Online Self-Awareness as an Influencing Factor”, as an observable exogenous variable of online self-awareness lends itself to using the Rosenberg self-esteem scale (RSES) (Rosenberg, 1965) commonly used in recent studies on OSN addiction (Hawi and Samaha, 2017a) in combination with a self-efficacy scale adapted from the General Self-Efficacy Scale (GSE) (Schwarzer and Jerusalem, 2013) and Cybersecurity Engagement and Self-Efficacy Scale (CESES) (Amo, L., Zhuo, Wilde, Murray, Cleary, Upadhyaya, 2016). These scales were used to gauge research objective four, where employees' levels of awareness towards psychological and external factors are affected by manipulated impulsive behaviour, habits, and OSN addiction on responsible OSN engagement.

4.3.3.2.1 Rosenberg’s Self-Esteem scale (RSES)

The results of the RSES showed a Cronbach α =.863 for reliability and consistency with an Inter-Item Correlations (IIC) mean of .407. Pallant (2018) recommends a minimum alpha value of .7 as generally acceptable. This consistency allowed the researcher to average the items to form an overall gauge that could be correlated with the other survey scales.

4.3.3.2.2 Online Self-Efficacy Scale (OSES)

The OSES was adapted using items taken from the General Self-Efficacy Scale (GSE) and Cybersecurity Engagement and Self-Efficacy Scale (CESES). This resulted in a 10-item scale tailored to gauge the respondent's self-efficacy, with five items relating to knowing online privacy legal rights and protecting personal information and five items relating to protection from cyber threats and resolving online security breaches.

The results of the OSES showed a Cronbach α =.870 for reliability and consistency with inter-item correlations mean of .405. This consistency allowed the researcher to average the items to form an overall assessment that could be correlated with the other survey scales.

4.3.3.2.3 OSN Addiction (BSMAS)

Results for the six items BSMAS frequency scale for OSN addiction showed consistency of Cronbach's α =.801 with an inter-item correlation of .401. The BSMAS is a concise and direct scale that provides a well-known validated assessment of OSN addiction (Lin *et al.*, 2017; Monacis *et al.*, 2017; D'Arienzo, Boursier and Griffiths, 2019). From a 5-point, Likert scale that ranges from "very rarely" (1) to "very often (5), the scores from each of the six items are aggregated, ranging from 6 to 30. The higher this aggregated value, the higher the risk of problematic OSN addiction. Recent studies from different international regions have suggested that an aggregated value of over 19 is associated with the danger of the risk of problematic OSN addiction (Bányai *et al.*, 2017; Lin *et al.*, 2017; Monacis *et al.*, 2017). The self-reporting survey of the sample of *n*=328 found that a low 4.8% of the respondents across both industries showed a risk of problematic OSN addiction. The financial services sector (*n*=185) shows a marginally less of 4.32% than the healthcare sector (*n*=143) at 5.59% risk of problematic OSN addiction.

4.3.3.2.4 Texting Behavioural Habits

General feedback from a significant number of employees responding to the online survey expressed suspicious concerns to the questions relating to whether they engaged in risky and potentially illegal behaviour when using OSN platforms. Responses from these two items were thus not considered.

However, the results for the four items evaluated showed a low consistency with Cronbach's α below .6 (α =.511). This was possibly due to the number of items N = 4 being less than 10 and the low average inter-item correlation of .202 (Pallant, 2020). However, when adding the four texting habit items to the OSN addiction scale, adjusting the range of responses of texting habits in line with the BSMAS revealed a far more acceptable Cronbach's α below α =.761 and an inter-item correlation of .237.

Correlations between online self-awareness regarding self-efficacy and texting habit items were examined for significant correlations; however, only two items of texting habits were significant (p <.001) and both had a weak correlation above .2 for two behavioural intentions themes (Pallant, 2020). Both texting habit items addressed the direct consequences of the texting habit, viz., accidentally sending to the wrong recipient and texting without thinking the consequences through. Both had weak negative correlations of -.263 and -.244, respectively, to the behavioural intentions theme regarding password generation. On the other hand, accidentally sent to the wrong recipient or texting without thinking about the consequences had weak negative correlations of -.200 and -.249 (Pallant, 2020), respectively, to the proactive awareness behavioural intentions theme.

4.3.3.3 Online Privacy Literacy

Assessing the level of competency of the construct online privacy literacy defined in the literature review under "A Case for Online Privacy Literacy as an Influencing Factor", as an observable exogenous variable of online privacy literacy lends itself to using the online privacy literacy scale (OPLIS) in combination with the security intentions behavioural scale (SeBIS) was used to gauge the perceived effect of individual employees' online privacy literacy and security intentions on responsible OSN engagement within the organisation.

4.3.3.3.1 Online Privacy Literacy Scale (OPLIS)

Using a special case of Cronbach's α through Kuder-Richardson's coefficient revealed a consistency of the dichotomous literacy scores using the moderating influences regarding demographic data revealed high reliability and consistency.

4.3.3.3.2 Online Security Behaviour Intentions (SeBIS)

The analysis of the findings of the online security behaviour intentions was gauged in two phases. In the first phase, the 16 items relating to the SeBIS were analysed, followed by the second phase, which included the items relating to the respondents' behavioural intentions regarding the terms of service and privacy settings.

4.3.3.3.3 SeBIS Reliability and Consistency

First, the scale reliability was examined. Cronbach's α for the full scale showed α = .880.

Second, the item-total Pearson's correlation was assessed. An average inter-item correlation should fall in a range between .20 and .40. This would imply that, though the items are similar, they possess a large enough variance in one form or the other to be distinct from each other. Items less than .20 in inter-item correlation are likely not to fall into the same content domain. Items greater than .40 in inter-item correlation may be that a strong relationship may be restricted to aspects between the items that fall outside the construct (Martins, 2014). The average inter-item correlations of all 16 SeBIS items fall within the .20 and .40.

Third, the inter-item correlation average was computed at .313, which falls within the "exemplary" range above .3 for consistency. (Robinson, Shaver and Wrightsman, 2013).

4.3.3.3.4 Privacy Policies and Settings Reliability and Consistency

For an evaluation for consistency in the privacy policies and settings reliability items, Cronbach's α was computed to be just below .800 .α = .795. The average inter-item correlation was .393, where each item correlated on average with the individual items were all above .3 where two of the items were above .4. When combined with the SeBIS, the overall Cronbach's α was computed to be α = .875 and the average inter-item correlation was .24.

The analysis of consistency used satisfied the researcher that the sub-scales generally have reasonable high reliability.

Table 4.4 Cronbach α for all the Online Security Behaviour Item Themes

Theme	Theme Question	Cronbach's α
Password Generation	My Passwords…	.750
Device Securement	My Device / Computer…	.759
Proactive Awareness	I will look at the URL of a website...	.897
Updating	When it comes to software updates, I...	.820
Privacy Policies and Settings	Privacy policies and settings	.795

4.3.3.3.5 Significant Correlations

To examine research objectives four and five, where responsible engagement of OSNs within the organisation is influenced by the constructs of online privacy literacy and online self-awareness, the correlation between the average score of online privacy literacy, behavioural intentions toward online security against the online self-awareness using the self-esteem, self-efficacy, OSN addiction and texting habits scales.

Table 4.5 Most correlated significant behavioural intentions questions per theme to Self-Efficacy

Theme Question	Self-Efficacy r
1. My Passwords [I change, even if I don't have to.]	.377
2. My Device / Computer [I manually lock it when I step away from it.]	.211
3. I will look at the URL of a website... [to check for https: or lock icon to submit data]	.306
4. When it comes to software updates, I... [make sure my anti-virus updates itself]	.308

6. Regarding Social Network Apps Privacy Settings, I... [go with the flow as most people do]	.297

Correlation is significant at the p<0.01 level (2-tailed)

4.3.3.4 Organisational awareness

Victor and Cullen’s ethical climate questionnaire (ECQ) (Victor and Cullen, 1988) was used to gauge the construct defined in the literature review under A Case for Online Organisational Awareness as an Influencing Factor,” as an observable exogenous variable of organisational awareness to gauge the perceived influence of the employees' awareness of the ethical climate within the organisation on responsible OSN engagement meeting objective six.

4.3.3.4.1 The Ethical Climate Questionnaire (ECQ)

The ECQ assesses the following five themes through 26 questions fundamental to an organisation's ethical well-being amongst stakeholders: caring, law and code, rules (procedures and policies), instrumentalism (abiding by societal norms) and independence. In addition, the topical issue of the invasion of privacy of personal information as a new phenomenological theme introduced in the workplace by OSN platforms prompted the researcher to add a sixth theme of three additional items regarding privacy ethics.

Each theme was then gauged for reliability and consistency, as shown below

Table 4.6 Cronbach α for all the Ethical Climate Item Themes

Theme	Cronbach’s α	*IIC
Caring	.850	.446
Law and Code	.861	.609
Rules	.848	.587
Instrumentalism	.685	.217
Instrumentalism**	.840	.465
Independence	.778	.466
Privacy	.708	.548

**Question: ‘The major responsibility of people in this company is to control costs’ removed, resulting in α = .840 from α = .685,*

**Inter-Item Correlations*

The results of the standard ECQ showed a Cronbach α = .887 for reliability and consistency with an inter-item correlations mean of .248. Adding the two items on privacy gave the extended ECQ a Cronbach α = .901 for reliability and consistency with an inter-item correlation of .259.

This consistency allowed the researcher to aggregate the items of each of the themes examined and form an overall assessment that could be correlated with the other survey scales.

Correlations of the ECQ against scales associated with online privacy literacy and online self-awareness only showed a 2-tailed significance against OSN addiction and texting habit items. Of these correlations, all were relatively weak, the highest being texting habits with caring, which correlated at .229. Other weaker correlations above Pearson's correlation of .2 were law and code, rules and independence.

Correlating all the ECQ items against both SeBIS and the privacy and policies items shows Cronbach α = .89 for reliability and consistency when correlating all 51 items. Of the 51 inter-item correlations, there were 16 relatively weak correlations above .2 with a 2-tailed significance; however, the researcher fails to conclude any meaningful correlations from these weak correlations.

Correlating the five themes of the ECQ with the Privacy theme against the four SeBIS themes with the privacy and policies theme show Cronbach α = .743 for reliability and consistency and an inter-item correlation mean of .204.

The only significant relatively weak theme item correlations were found to be between the ECQ Law theme with that of the SeBIS updating theme, which showed a correlation of .222 and the added theme of privacy to the ECQ with that of the proactive awareness theme in n the SeBIS of .223 both with a 2-tailed significance of less than $p < .001$.

4.3.3.5 Summary of Reliability, Consistency and Validity

The defined construct of online self-awareness was measured using the RSES, and OSES displayed high reliability and consistency with an ideal range of average inter-item correlation. Self-esteem and self-efficacy both showed 2-tailed significance against behavioural intentions and some of the texting habit items. Self-esteem showed a negative 2-tailed significance against OSN addiction. Moderating influences regarding demographic data such as gender, industry, generation and qualification between the exogenous variable of Online Self Awareness and the OSN platform usage did not display significant differences between the financial and health sector. The BSMAS scale gauging OSN addictions displayed reliability and consistency with an excellent inter-item correlation. The data showed very low levels of respondents across both industries have a low risk of problematic OSN addiction. Texting habits displayed low reliability and consistency. Nevertheless, the data showed weak negative correlations to the behavioural intentions theme regarding password generation and not considering the consequence of OSN engagement.

Online privacy literacy displays an online privacy literacy competency for the entire sample overall twenty-five questions with an average score of 55%, where knowledge of data collection practices of OSNs scored close to 40% and close to 70% on data protection strategies. Significant correlations were displayed for gender and highest qualification, where males achieved an overall competency level of 63% versus 49% of females. The highest qualification revealed a matric or one certificate scored much lower than respondents with a diploma or degree. The SeBIS was adapted to include six questions covering the two themes of privacy policies and privacy settings, displaying high consistency, reliability, and good inter-item correlation. The overall score for the four themes of the SeBIS, male respondents scored between 10% and 20% higher than their counterparts concerning vigilance in online security behaviour. In contrast, females scored slightly higher in their behavioural intentions towards privacy policies and settings.

The ECQ with two additional items on OSN privacy showed high reliability and consistency with a good inter-item correlation mean. Correlations of the ECQ against scales associated with online privacy literacy and online self-awareness showed significance against OSN addiction and the texting habits items, where the highest was texting habits with caring from the ECQ. Correlating the five themes of the ECQ with the Privacy theme against the four SeBIS themes with the privacy and policies theme showed reliability, consistency, and a good inter-item correlation mean. The only significant theme item were correlations between the ECQ Law theme with that of the SeBIS updating theme and the added theme of privacy to the ECQ with that of the proactive awareness theme in n the SeBIS.

4.3.4 *Factor Analysis Models*

Factor analysis was used to ascertain potential underlying factors or components to reduce the number of items on each scale to a more manageable number. The researcher used the sample of 234, providing ratios of over 10 cases per item, satisfying the minimum data size required. Principal component analysis (PCA) was used with a Varimax rotation to simplify the relationship among factors, reducing the data-set dimensionality through a covariance analysis. The reduced data sets enabled analysing, visualising, identifying and naming of factors to the constructs derived in the study, namely, online self-awareness, online privacy literacy, online organisational awareness, security behavioural intentions and OSN addiction and texting habits (Hair et al., 2014).

4.3.4.1 Factor Analysis of the Online Self-Awareness Scale (OSAS)

An exploratory factor analysis [R7](EFA) on the 20 self-reported items combining Rosenberg's 10-item self-esteem Scale (RSES) and the adapted 10-item online self-efficacy scale (OSES) was performed to identify potential underlying factors or components and to see if item reduction was possible. [R8]

All 20 items correlated a minimum of .3 with at least one of the other items signifying favourable factorability (Pallant, 2020). The Kaiser-Meyer-Olkin measure of sampling adequacy was shown to be .859, well above the accepted .6 (Mulaik, 2009). Bartlett's test of sphericity was significant (χ^2 (190) = 2944.81, p < .001) (Hair *et al.*, 2014). The commonalities of 18 items were all above .3, showing that each item shares a common variance with other items (Child, 2006; Samuels, 2016). The anti-image correlation matrix diagonals were over .5. The two items with a commonality below .3 were eliminated (Hair *et al.*, 2014). These were the two items 3.) "I do not believe anyone could crack my online passwords", and 4.) "I am confident that my personal information will not be misused by Online Social Networking companies", which were also intercorrelated with items regarding being able to stop malware or virus invasion and maintaining online privacy rights, respectively.

Principal Component Analysis was used as a linear dimension reduction method to reduce the items of the scales employed. The initial Eigenvalues accounted for 30.0%, 26.0% and 9.7% of the variance of the first three factors. For more consistency, a

Monte Carlo parallel analysis was carried out to confirm reducing the number of factors to three (Hair *et al.*, 2014; Pallant, 2020), as shown in Table 4.7 and Figure 4.7 Scree Plot of Monte Carlo Parallel Analysis (OSAS) (*n*=328)

The parallel analysis was done using software adapted for IBM SPSS, running simulations of 1000 randomly generated datasets using a 95 percentile for the distributions of the random data eigenvalues (O'Connor, 2000).

Table 4.7 Monte Carlo Parallel Analysis OSAS (*n*=328)

	Monte Carlo		**SPSS Varimax Initial Eigenvalues**		
Component	**Total**	**95%**	**Total**	**% of Variance**	**Cumulative %**
1	5.214	1.543	4.483	28.017	28.017
2	4.328	1.444	3.784	23.652	51.669
3	1.395	1.361	1.347	8.419	60.088

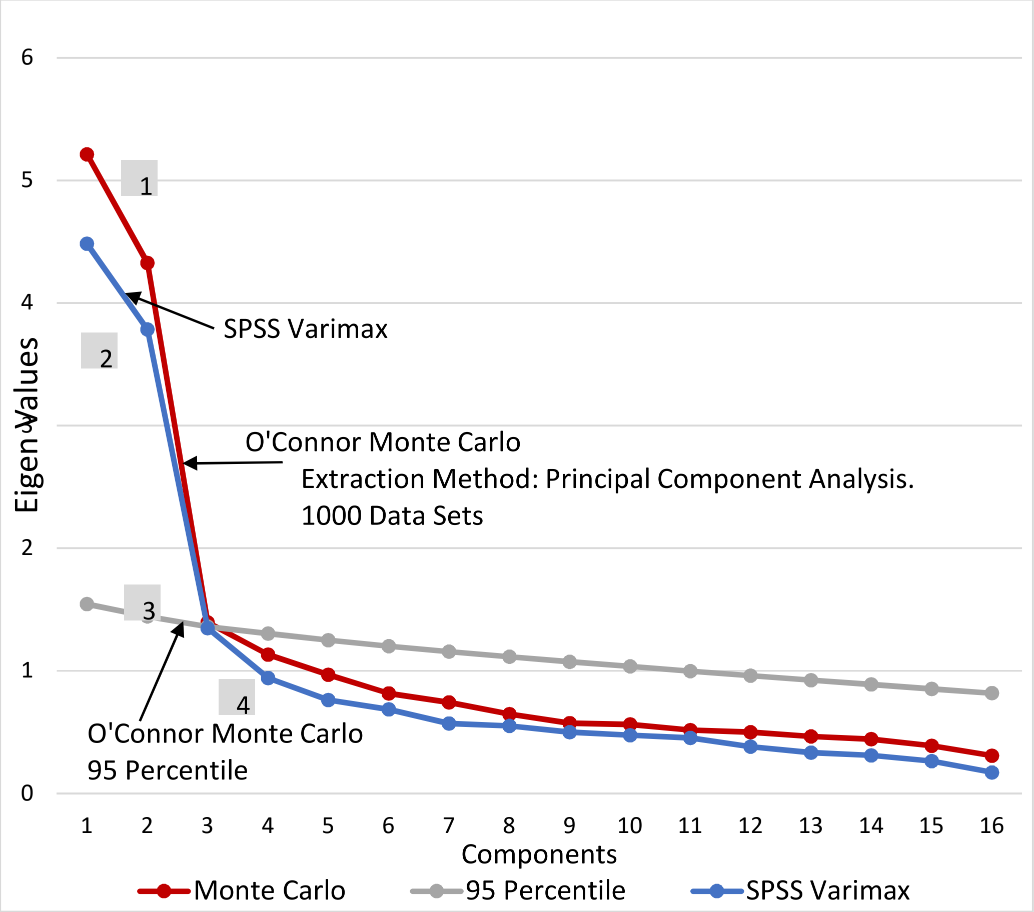


Figure 4.7 Scree Plot of Monte Carlo Parallel Analysis (OSAS) (*n*=328)

Seven items of the original 20 were eliminated, failing to meet a primary factor loading of .5 and above or a cross-loading of .2 and higher. From the self-efficacy factor, the process eliminated the two items relating to being able to protect one's self from cyber threats. These were 1.) "I am able to protect myself from cyber threats" and 2.) "Knowing how and protecting this organisation's private and client data from being tracked by outside sources is of prime importance for me." Both were highly inter-correlated to at least one corresponding item of *r* > .5 and covered by items relating to being able to find a solution if compromised by malware or a virus.

The RSES rotated into two self-esteem factors, Positive and Negative self-esteem, where three items were eliminated through the same process, failing to meet at least a .5 and .2 factor cross-loading. The items eliminated were 6.) "On the whole, I am satisfied with myself." 7.) "I feel I do not have much to be proud of", and 5.) "I take a positive attitude toward myself." Each was highly inter-correlated to at least one corresponding item of r > .5 of a similar question.

This resulted in 3 factors of a total of 16 items, see Table 4.8, namely, Online Self-Efficacy (8 items), Negative self-esteem (5 items) and positive self-esteem (3 items). It is important to note that the scale measuring self-esteem is now divided into two distinct factors measuring two different elements of self-esteem and not merely two equal, directly opposite related assessments, namely, Positive and Negative self-esteem. Instead, a poor or negative self-image does not mean a lack of the personal confidence of skills and knowledge to protect themselves from online security and privacy attacks or threats whilst engaging in OSNs, as illustrated by the positive response to question 4.) I am able to do things as well as most other people 7.) I feel that I'm a person of worth, at least on an equal plane with others which had significant correlations with self-efficacy in skill levels regarding the protection of online privacy and security.

Table 4.8 Final Rotated Component Matrix (OSAS)

Rotated Component Matrix[a] (OSAS)				***Communalities***
	Component			
Reduced Set of Variables	1	2	3	

9. If my online activity has been compromised by malware or a virus, I can stop the attack and prevent further invasion. (V88)	.814 [R9]			.693
8. If my online activity is under threat by a virus or is being maliciously traced, I know how to stop it and remove the threat. (V87)	.808			.682
6. If my online activity is compromised by unknown malware or a virus, I will be able to find a solution. (V85)	.806			.658
4. I know how to protect my private data from being tracked by outside sources. (V83)	.793			.640
3. I know and maintain my Online Privacy rights. (V82)	.727			.552
1. I am able to protect myself from cyber threats. (V80)	.684			.554
2. If my online privacy is compromised, I will be able to find a way to counter it within my legal privacy rights. (V81)	.656			.493
7. I am confident that Online Social Networking companies will not misuse my personal information. (V86)	.602			.371
6. I certainly feel useless at times. (V95)		.794		.671
9. All in all, I am inclined to feel that I am a failure(V98)		.780		.642
2. At times, I think I'm no good at all. (V91)		.752		.598
5. I feel I do not have much to be proud of.(V94)		.676		.466
8. I wish I could have more respect for myself. (V97)		.665		.470
4. I am able to do things as well as most other people. (V93)			.834	.741
3. I feel that I have a number of good qualities. (V92)			.808	.739
7. I feel that I'm a person of worth, at least on an equal plane with others. (V96)			.682	.643

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.
[a] *Rotation converged in 5 iterations. Factor loadings less than .40 have not been printed, and loadings have sorted variables on each factor*

The three factors were then assessed using a CFA using IBM AMOS (version 25), see Figure 4.8, resulting in each of the three extracted factors showing an average variance extracted (AVE) above the acceptable level of .5 and are all above the acceptable value .7 for the composite reliability (CR) (Hair *et al.*, 2014).

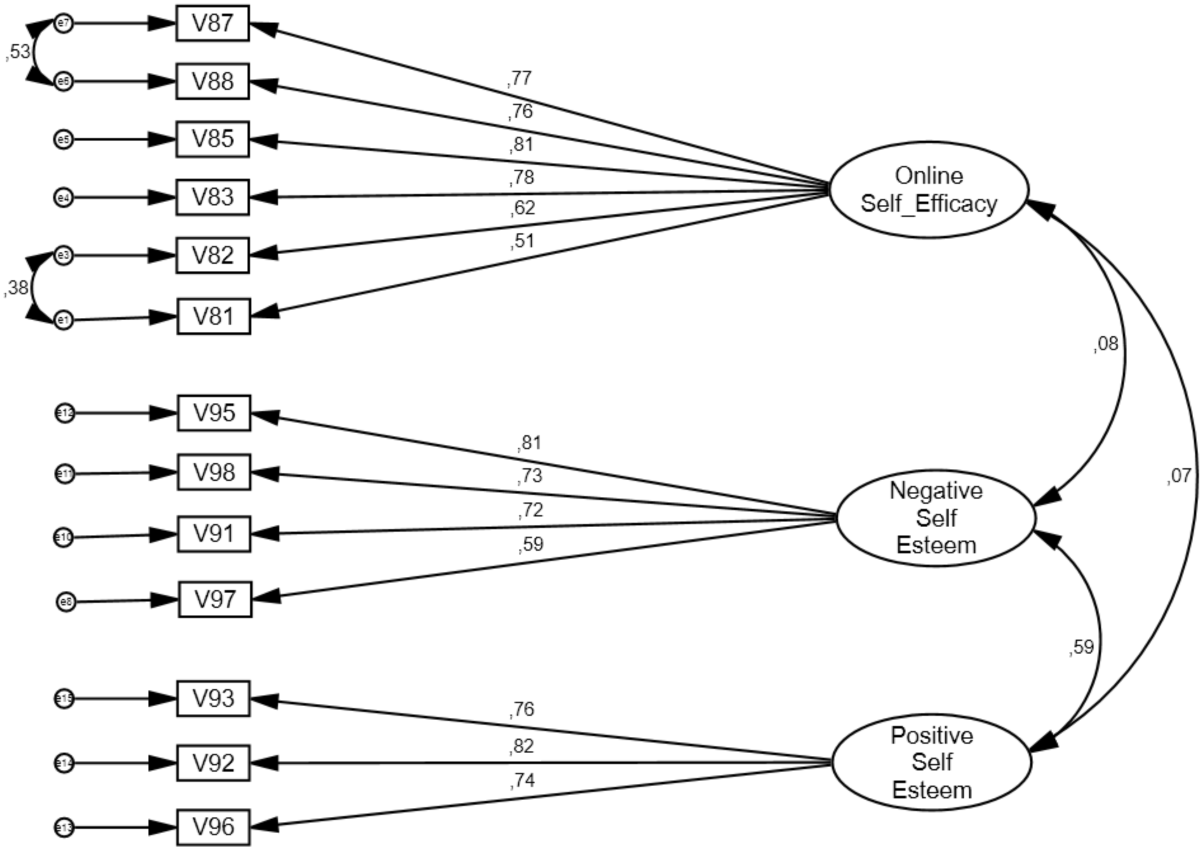


Figure 4.8 Confirmatory Factor Analysis Model (OSAS) (baseline).

4.3.4.1.1 Model Fit Summary

To evaluate a model, fit indices are used to compare the developed model to the fit of a baseline model, such as the independence model, where all relationships between the observed variables are assumed to be zero. Then, an assessment is made as to whether the fit of the developed model is an improvement of the independence model. Common practice would be to evaluate comparisons regarding the Goodness-of-Fit Index (GFI), the Normed Fit Index (NFI), the Comparative Fit Index (CFI), and the Adjusted Goodness-of-Fit Index (AGFI) (Schermelleh-Engel, Moosbrugger and Müller, 2003).

As seen in Table 4.9 Model Fit (OSAS)the model fit of the proposed exogenous variable online self-awareness meets accepted thresholds of all the commonly used comparison criteria as a good to acceptable fit (Schermelleh-Engel, Moosbrugger and Müller, 2003; Hooper, Coughlan and Mullen, 2008; Byrne, 2010).

Table 4.9 Model Fit (OSAS)

Measure	Value	Threshold
CMIN	145.765	
d*f*	60.000	
P	.00	>.05
CMIN/d*f*	2.429	Ratio between 2 (good) and 3 (acceptable)
GFI	.93	(0 no fit, 1 perfect fit); >.95 good; >.90 acceptable fit
NFI	.92	(0 no fit, 1 perfect fit); >.95 good; >.90 acceptable fit
CFI	.95	(0 no fit, 1 perfect fit); >.97 good; >.95 acceptable fit
AGFI	.90	(0 no fit, 1 perfect fit); >.90 good; >.85 acceptable fit
RMSEA	.06	.05 represents close approximate fit

Ratio Chi-square/degrees of freedom (CMIN/df), Comparative fit index (CFI), Goodness-of-fit index (GFI), Adjusted Goodness-of-Fit-Index (AGFI), Normed fit index (NFI), Roots mean squared error of approximation (RMSEA[R10]*)*

It is noted from the CFA in Figure 4.8 that there is a relatively large correlation between negative and positive self-esteem in comparison to almost no correlation to self-efficacy. This is in line with the formation of a cognitive view of attitudes, beliefs and value judgements a person understands about themselves manifested through thoughts, aptitude, capabilities, feelings and habits (Rodriguez and Loos-Sant’Ana, 2015), as discussed in the literature review. Simply stated, self-concept is how a person perceives their negative and positive aspects (Showers and Zeigler-hill, 2015). Furthermore, self-concept is related both to self-efficacy and self-esteem (Wehrle and Fasbender, 2018). A review of comparisons between self-concept and self-efficacy shows that as constructs self-efficacy may be a better measure than self-concept (Bong and Clark, 1999). Therefore, as an observed variable self-awareness or self-referenced beliefs can be stated to be a culmination of both negative and positive self-reflection in terms of self-concept and self-esteem surpassed by self-efficacy (Loos-Sant’Ana and Ferreira De Brito, 2017). This high correlation between negative and positive self-esteem with little correlation to self-efficacy could provide support for the relationship between online self-awareness as an observed variable within the context of the Cybersecurity Engagement Self-Efficacy Scale and the Self-Esteem Scale as an influencing factor toward responsible behaviour with OSN engagement.

4.3.4.2 Factor Analysis of Addiction and Habits

An EFA and CFA on the two six-item scales OSN addiction and texting habits exploring self-reporting habitual OSN engagement behaviours was performed to identify whether item-reduction was possible providing ratios of over 14 and 10 cases per variable respectively satisfying the minimum data size required.

All ten items correlated a minimum of .3 with at least one of any of the other items signifying favourable factorability (Pallant, 2020). The Kaiser-Meyer-Olkin measure of sampling adequacy was shown to be .782, well above the accepted .6 (Mulaik, 2009). Bartlett's test of sphericity was significant (χ2 (45) = 786.58, p < .001). The communalities were all above .3 showing each item shares a common variance with other items (Child, 2006; Samuels, 2016). The anti-image correlation matrix diagonals were over .5.

Principal component analysis was used as a linear dimension reduction method to reduce the items of the scales employed. The initial Eigen values accounted for 33.35%, 14.97% and 11.67% of the variance of the first three factors. A Monte Carlo parallel analysis was carried out to confirm reducing the number of factors to three see Table 4.10 and Figure 4.9.

Table 4.10 Monte Carlo Parallel Analysis (Addiction and Habits) (*n*=328)

	Monte Carlo		SPSS Varimax Initial Eigenvalues		
Factor	**Total**	**95%**	**Total**	**Percentage of Variance**	**Cumulative Percentage**
1	3.335	1.362	3.335	33.352	33.352
2	1.497	1.246	1.497	14.967	48.320
3	1.117	1.174	1.117	11.168	59.488

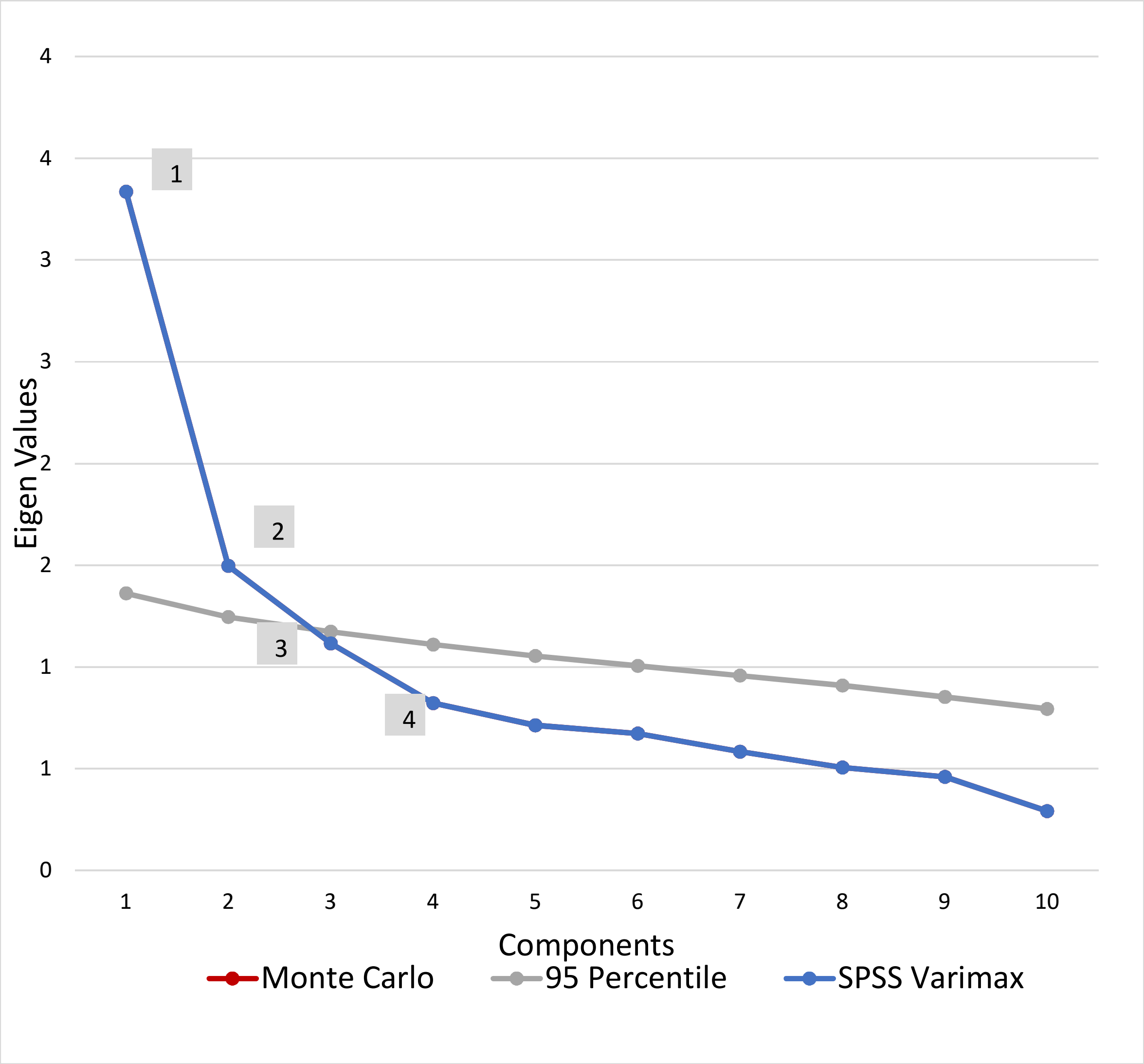


Figure 4.9 Scree Plot of Monte Carlo Parallel Analysis (Addiction and Habits) (n = 328)

Two items of the original ten were eliminated, failing to meet a primary factor loading of .5 and above or a cross-loading of .2 and above. The two items were 1.) “You have tried to cut down on the use of social media without success”, and 2.) “You use social media so much that it has had a negative impact on your job/studies”, which were inter-correlated to at least one corresponding item of *r* > .5, which resulted in the final rotated Varimax matric as seen in Table 4.11.

A CFA tested the fit between the data and the proposed three factor model for measuring soundness see Figure 4.10 however only the OSN Addiction factors reached the desired average variance extracted (AVE) above the acceptable level of .5 and are all above the acceptable value of .7 for the composite reliability (CR). The factor Bad Habits achieved an AVE above .5 and a CR of .63 and Good Habits an AVE of .37 and a CR of .54. When considering related nature and the inter-correlation of the Bad Habits *r* =.312, *p* < .001 and Good Habits *r* = .343, *p* < .001 items they were deemed suitable to be aggregated with the aggregated OSN Addiction factor as the variable addiction and habits.

Table 4.11 Rotated Component Matrix (Addiction and Habits)

Rotated Component Matrix[a] (Addiction and Habits)

	Component			**Communalities**
Reduced Set of Variables	1	2	3	
2. You feel an urge to use social media more and more? (V75)	.833			.713
1. You spend a lot of time thinking about social media or planning how to use it. (V74)	.752			.576
3. You use social media in order to forget about personal problems. (V76)	.731			.592
5. You become restless or troubled if you are prohibited from using social media. (V78)	.723			.533
4. You have tried to cut down on the use of social media without success. (V77)	.597			.365
6. You use social media so much that it has had a negative impact on your job/studies. (V79)	.542			.344
3. I check to see that I am sending to the correct recipient. (V70)		.872		.790
5. I think of the consequences of my message before sending it. (V72)		.777		.740
2. I text when I have been drinking. (V69)			.860	.739
6. I text whilst still angry. (V73)			.682	.556

Extraction Method: Principal Component Analysis.

Rotation Method: Varimax with Kaiser Normalization.

[a] *Rotation converged in 5 iterations. Factor loadings less than .40 have not been printed and variables have been sorted by loadings on each factor*

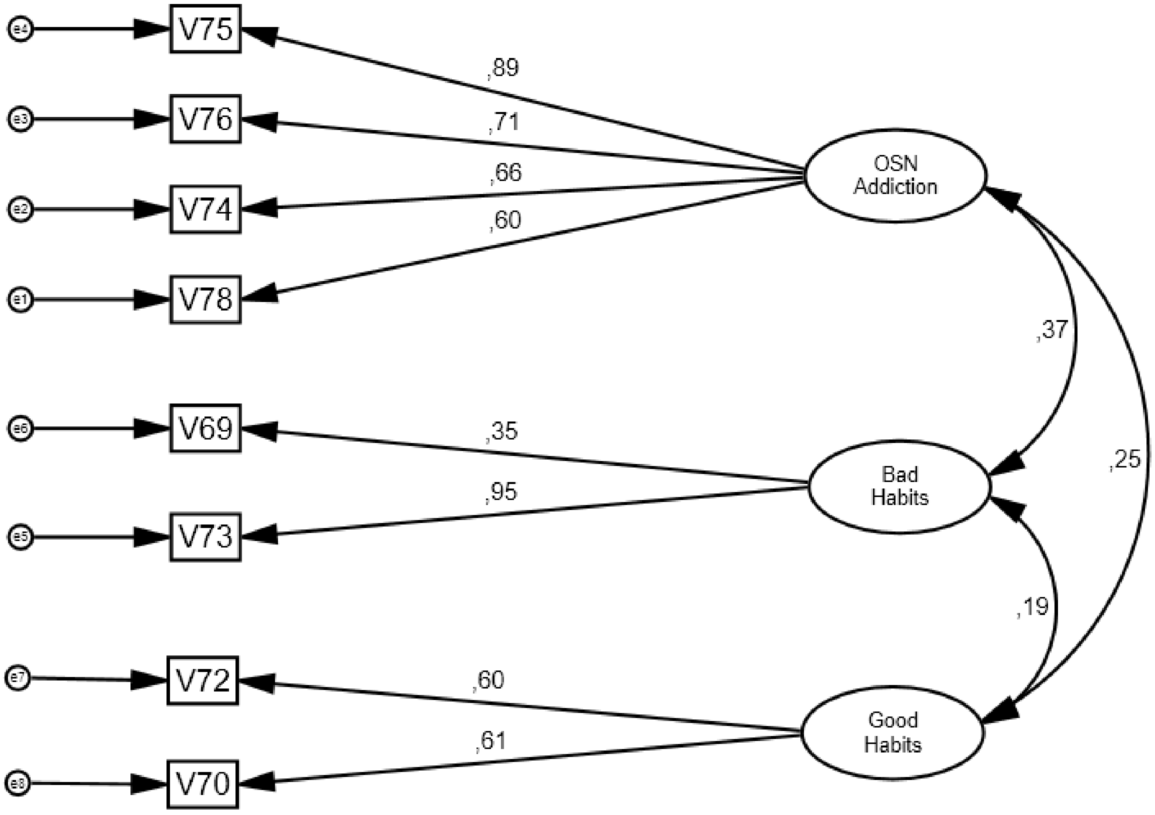


Figure 4.10 Confirmatory Factor Analysis Model (Addiction and Habits).

The relative larger correlation between OSN addiction and bad texting habits versus the lower correlation between OSN addiction and good texting habits is noted from the CFA in Figure 4.10, highlighting the dangerous effects of OSN addition supporting findings from studies using the Bergen social media addiction scale (BSMAS) (Andreassen, Pallesen and Grif, 2017). It should also be noted that there is still a relatively low correlation between OSN addiction and good texting habits, implying that those with vigilance in texting habits may still be vulnerable to OSN addiction. The low loading of “I text when I have been drinking” (V69) may be as a reluctance to respond honestly to an illegal texting bad habit as opposed to the legal but irrational emotionally charged dangerous habit of “I text whilst still angry” (V73).

4.3.4.2.1 Model Fit Summary

For the proposed addiction and habits model, fit comparison indices are used to compare the developed model to the fit of a baseline independence model where the relationships between the observed variables are assumed to be zero. In assessing whether they fit the addiction and habits, we see from Table 4.12 that there is an improvement over the independence model where the common practice comparisons Goodness-of-Fit Index (GFI), the Normed Fit Index (NFI), the Comparative Fit Index (CFI), and the Adjusted Goodness-of-Fit Index (AGFI) meet accepted thresholds of all the commonly used comparison criteria as a good to acceptable fit (Schermelleh-Engel, Moosbrugger and Müller, 2003; Hooper, Coughlan and Mullen, 2008; Byrne, 2010).

Table 4.12 Model Fit (Addiction and Habits)

Measure	Value	Threshold
CMIN	145.765	
df	60.00	
P	0.00	>.05
CMIN/*df*	2.429	Ratio between 2 (good) and 3 (acceptable)
GFI	0.94	(0 no fit, 1 perfect fit); >.95 good; >.9 acceptable fit
NFI	0.93	(0 no fit, 1 perfect fit); >.95 good; >.9 acceptable fit
CFI	0.96	(0 no fit, 1 perfect fit); >.97 good; >.95 acceptable fit
AGFI	0.91	(0 no fit, 1 perfect fit); >.90 good; >.85 acceptable fit
RMSEA	0.07	.05 represents close approximate fit

Ratio Chi-square/degrees of freedom (CMIN/df), Comparative fit index (CFI), Goodness-of-fit index (GFI), Adjusted Goodness-of-Fit-Index (AGFI), Normed fit index (NFI), Roots mean squared error of approximation (RMSEA)

This CFA and resulting model fit are sufficient for the researcher to aggregate the extracted items as an addiction and habits endogenous variable.

4.3.4.3 Factor Analysis of Online Security Intentions and Behaviour Scale (OSIBS)

A factor analysis of the 22 self-report items from OSIBS was performed to identify whether factor reduction was possible providing ratios of over 14 and 10 cases per variable, respectively, satisfying the minimum data size required.

All 22 items correlated a minimum of .3 with at least one of any of the other items signifying favourable factorability (Pallant, 2020). The Kaiser-Meyer-Olkin measure of sampling adequacy was shown to be .828, well above the accepted .6 (Mulaik, 2009). Bartlett's test of sphericity was significant (χ^2 (231) = 2824.96, p < .001). The commonalities were all above .3, showing that each item shares a common variance with other items (Child, 2006; Samuels, 2016). The anti-image correlation matrix diagonals were over .5.

Principal Axis Factor extraction was used to ascertain the factor structure. The initial Eigenvalues accounted for 31.40%, 12.88%, 9.00% and 6.95% of the variance of the first four factors. The fifth and sixth factors had eigenvalues just above one accounting for 6% and 5.3% of the variance. A Monte Carlo parallel analysis was carried out to confirm reducing the number of factors to four. The parallel analysis using principal axis factor extraction was done using software adapted for SPSS running simulations of 1000 randomly generated datasets using a 95 percentile for the distributions of the random data eigenvalues (O'Connor, 2000). This was compared to the results from the SPSS Varimax rotation conducted.

The results of the parallel analysis corresponded close to a 100% match where the 95% data set from the simulation intercept to the data set of both the SPSS Varimax and Monte Carlo simulation extraction was close enough to confirm a reduction to four factors four the online security behaviour scale (OSIBS) see Table 4.7 and Figure 4.11.

Nine items of the original 22 were eliminated, failing to meet a primary factor loading of .5 and above or a cross-loading of .2 and above. This process eliminated the four items relating to password security, which were all highly inter-correlated to at least one corresponding item of r > .5 and covered by items relating to passwords or PINs in device security. Two additional items were included in this elimination process. These items were 1) “My Device / Computer [Is set to lock when left for a while automatically.].” 2) “Regarding Social Network Apps Privacy Settings I... [accept the default settings]”, which were intercorrelated with similar items.

The EFA was followed with a CFA where a CFA tested the four factors using IBM AMOS (version 23), resulting in the elimination of three additional items from the now-defined factor OSN Policies and Settings to attain an acceptable model fit as depicted in Figure 4.12 namely “Regarding Social Network Apps Privacy Policies I... [agree to without reading them]”, “Regarding Social Network Apps Privacy Settings I... [don't care about them] and “Regarding Social Network Apps Privacy Settings I... [go with the flow as most people do]”. This resulted in each of the four extracted factors

Table 4.13 Monte Carlo Parallel Analysis of OSIBS (*n*=328)

	Monte Carlo		SPSS Varimax Initial Eigenvalues		
Factor	Total	95%	Total	Percentage of Variance	Cumulative Percentage
1	6.909	1.596	6.909	31.404	31.404
2	2.833	1.491	2.833	12.875	44.279
3	1.980	1.412	1.980	9.002	53.281
4	1.529	1.344	1.529	6.949	60.230

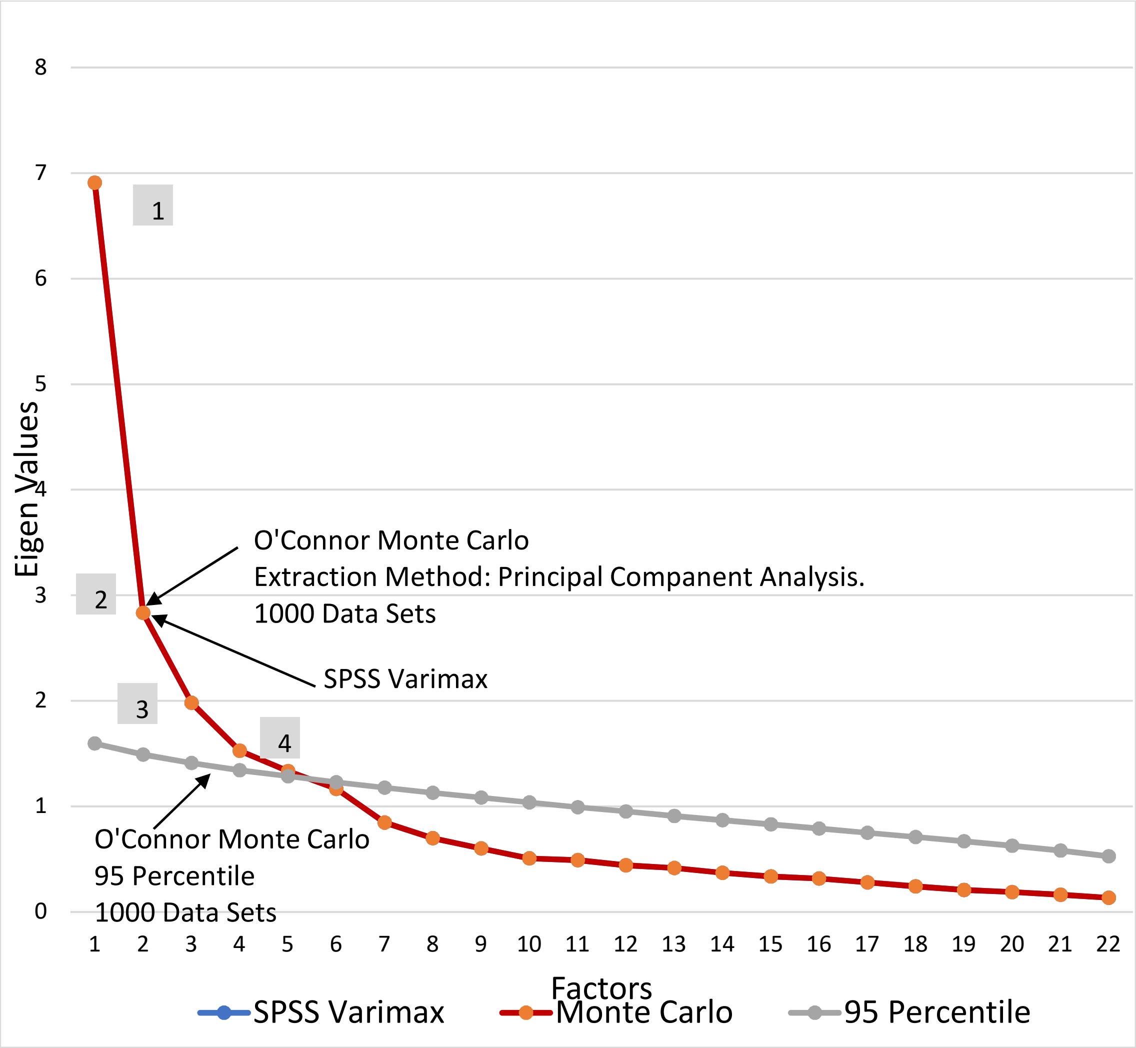


Figure 4.11 Monte Carlo Parallel Analysis (OSIBS) (*n*=328)

Table 4.14 Rotated Component Matrix (OSIBS)

Rotated Component Matrix[a] (OSIBS)					**Communalities**
	Component				
Reduced Set of Variables	1	2	3	4	
3. I will look at the URL of a website... [before I open a link someone has sent] (V54)	.861				.795
3. I will look at the URL of a website... [to check for https: or lock icon to submit data] V56)	.850				.764
3. I will look at the URL of a website... [even if I'm familiar with the website's look & feel] (V55)	.837				.762
3. I will look at the URL of a website... [by using a mouse over on links] (V57)	.769				.650
3. I will look at the URL of a website... [if I suspect a security problem] (V58)	.721				.621
1. My Passwords [Is longer than 6 characters] (V48)		.804			.657
1. My Passwords [Have special characters even if not required.] (V49)		.749			.610
2. My Device / Computer [Requires a PIN or passcode to be unlocked] (V53)		.725			.558
2. My Device / Computer [Is set to automatically lock when left for a while.] (V50)		.723			.608
4. When it comes to software updates I... [install the new update as soon as I'm notified] (V59)			.876		.788
4. When it comes to software updates I... [make sure programs are up-to-date] (V60)			.869		.836
4. When it comes to software updates I... [make sure my anti-virus updates itself] (V61)			.717		.628
5. Regarding Social Network Apps Privacy Policies I... [agree to without reading them] (V62)				.850	.729
5. Regarding Social Network Apps Privacy Policies I... [read thoroughly] (V63)				-.784	.647
6. Regarding Social Network Apps Privacy Settings I... [go with the flow like most people do] V64)				.707	.559

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.

[a] *Rotation converged in 5 iterations. Factor loadings less than .40 have not been printed and variables have been sorted by loadings on each factor*

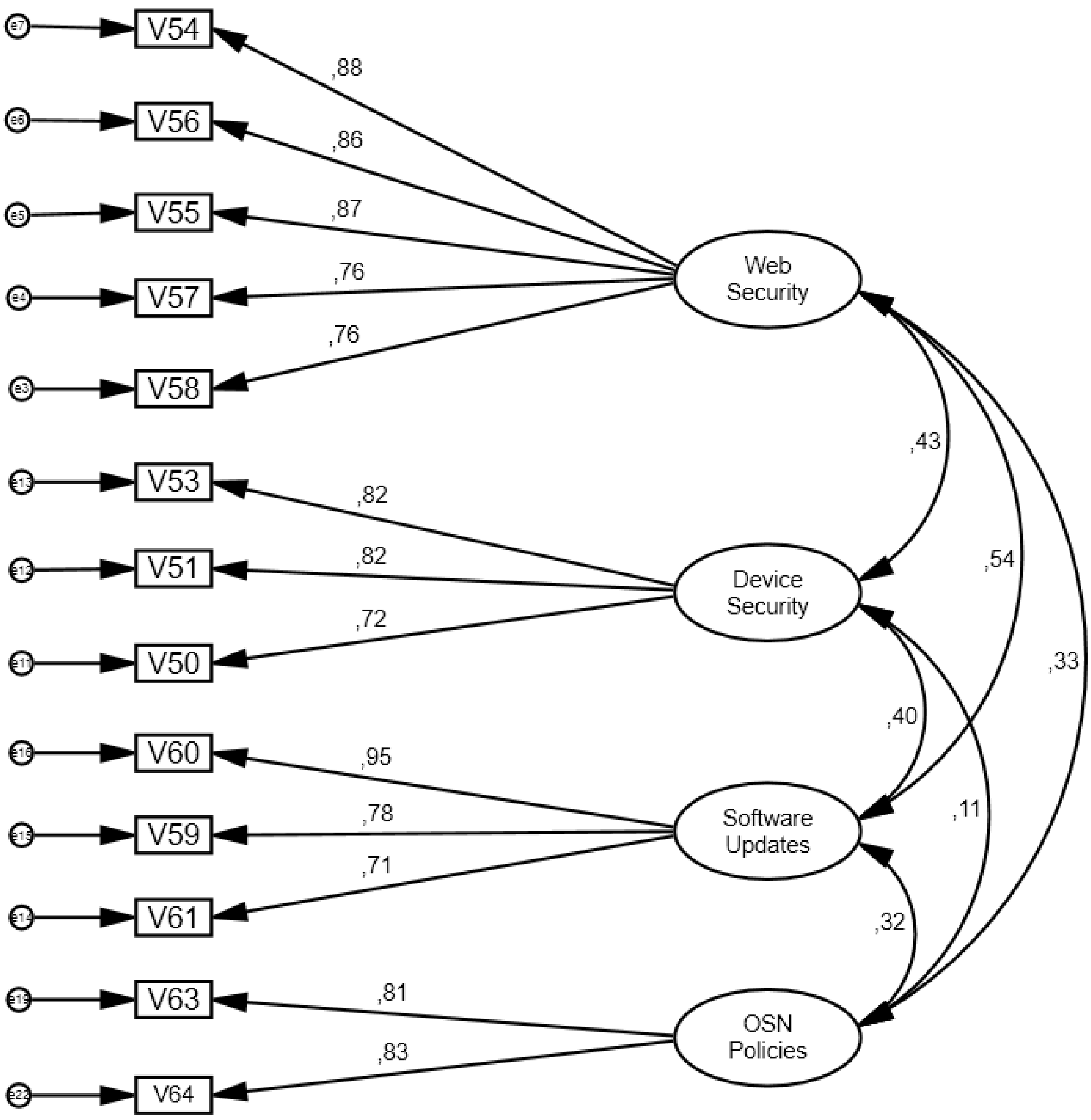


Figure 4.12 Confirmatory Factor Analysis Model (OSIBS)

showing an average variance extracted (AVE) above the acceptable level of .5 and all above the acceptable value of .7 for the composite reliability (CR).

Each of the aggregated four factors was aggregated to form the endogenous variable online security behaviour used to test the dependence of organisational awareness (objective six), online privacy literacy awareness (objective five) and online self-awareness (objective four) in the influence of responsible and abusive OSN engagement within organisations.

Noted from the CFA from Figure 4.12 is the slightly lower correlation to the proactive administrative formal behavioural intent toward security. Although both have a high loading, both V63 “Regarding Social Network Apps Privacy Policies I... [read thoroughly]” and V64 “Regarding Social Network Apps Privacy Settings I... [go with the flow like most people do]” both have a lower correlation toward more reactive vigilant behavioural intent of software updates, device security and web security.

4.3.4.3.1 Model Fit Summary

To assess the model fit for the proposed OSIBS, comparison indices are used to check the suggested model to fit a baseline independence model where the relationships between the observed variables are assumed to be zero. As seen in

Table 4.15, there is an improvement over the independence model where the common practice comparisons Goodness-of-Fit Index (GFI), the Normed Fit Index (NFI), the Comparative Fit Index (CFI), and the Adjusted Goodness-of-Fit Index (AGFI) meet accepted thresholds of all the commonly used comparison criteria as a good to acceptable fits (Hooper, Coughlan and Mullen, 2008; Byrne, 2010). The measured value of Ratio Chi-square to degrees of freedom (CMIN / *df*), 2.844, is a good model fit where the ratio is preferred to be smaller between the good and acceptable values of 2 and 3, respectively (Schermelleh-Engel, Moosbrugger and Müller, 2003).

The measure of approximate fit in the population is the Root Mean Square Error of Approximation (RMSEA), where a value < .05 is an approximate fit.

Table 4.15 reflects a value of .075, which according to Browne and Cudeck (1992), values between .05 and .08 reflect a reasonable fit (Browne and Cudeck, 1992) or further supported by others that anything less than .10 reflecting a reasonable fit between sample data and proposed model (Fan, Thompson and Wang, 1999).

This CFA and resulting model fit are sufficient for the researcher to aggregate the extracted items as an online security behaviour endogenous variable.

Table 4.15 Model Fit (OSIBS)

Measure	Value	Threshold
CMIN	170.631	
df	60.000	
P	.000	>.05
CMIN/*df*	2.844	Ratio between 2 (good) and 3 (acceptable)
GFI	.93	(0 no fit. 1 perfect fit); >.95 good; >.90 acceptable fit
NFI	.92	(0 no fit. 1 perfect fit); >.95 good; >.90 acceptable fit
CFI	.95	(0 no fit. 1 perfect fit); >.97 good; >.95 acceptable fit
AGFI	.90	(0 no fit. 1 perfect fit); >.90 good; >.85 acceptable fit
RMSEA	.08	.05 represents the close approximate fit

Ratio Chi-square/degrees of freedom (CMIN/df), Comparative fit index (CFI), Goodness-of-fit index (GFI), Adjusted Goodness-of-Fit-Index (AGFI), Normed fit index (NFI), Roots mean squared error of approximation (RMSEA)

4.3.4.4 Factor Analysis of Ethical Climate Questionnaire (ECQ)

IBM SPSS (Version 25) and IBM AMOS (Version 25) were used to fit the most suitable factors to build a reduced-item model of the ECQ. First, the ECQ data collected from the survey were analysed using EFA to obtain the appropriate factor model for assessing the ethical climate types. This was followed by confirmatory factor analyses CFA to compare the result from the EFA. Next, the reduced number of factors was determined using Kaiser Criterion based on Eigenvalues greater than or equal to 1. This was done in conjunction with an analysis of the scree plot to select the point at which the initial slope representing the Eigenvalues starts levelling out. Next, a Monte Carlo Principal Component Analysis for parallel analysis was conducted, confirming the reduced number of factors. The parallel analysis using Principal Component Analysis was done using software adapted for SPSS running simulations of 1000 randomly generated data sets using a 95 percentile for the distributions of the random data eigenvalues (O’Connor, 2000). This was compared to the results from the SPSS Varimax rotation conducted.

Principal Component Analysis was used as a linear dimension reduction method to reduce the items of the scales employed. The initial Eigenvalues accounted for 30.46%, 12.41%, 9.25% and 5.96% of the variance of the four factors. The results of the parallel analysis corresponded close to a 100% match where the 95% data set from the simulation intercept to the data set of both the SPSS Varimax and Monte Carlo simulation extraction was close enough to confirm a reduction to four factors four as per the flattening out in the scree plot and the intersection of the 95 percentile for the proposed reduction of components of the ECQ. See

Table 4.16 and Figure 4.13.

Of the 328 respondents, 234 did the ECQ of 29 items. The remaining 94 respondents were part of an organisation that opted not to do the ECQ. However, the number of respondents who completed the ECQ is sufficient for an EFA. All 29 items correlated a minimum of .3 with at least one of any of the other items signifying favourable factorability (Pallant, 2020). The Kaiser-Meyer-Olkin measure of sampling adequacy was shown to be .877, well above the accepted .6 (Mulaik, 2009). Bartlett’s test of sphericity was significant (χ2 (351) = 3355.81, p < .001). Twenty-eight of the twenty-nine commonalities were all above .3, showing each item shares a common variance with other items (Child, 2006; Samuels, 2016). The anti-image correlation matrix diagonals were over .5.

Twelve items of the original 29 were eliminated, failing to meet a primary factor loading of .5 and above or a cross-loading of .2 and above. This process eliminated five items relating to caring, which were all inter-correlated to at least one corresponding item of *r* >.4, namely, 1.) "What is best for everyone in the organisation is a major consideration here", 2.) "In this organisation, people look out for each other's good", 3.) "In this organisation, it is expected that you will always do what is right for the customer and public", 4.) "The most efficient way is always the right way in this organisation." 5) "Everyone is expected, above all, to work efficiently in this organisation." One item relating to rules, namely 6.) “People in this organisation strictly obey the organisation policies" and two questions relating to instrumental ethics, namely 7.) “In this organisation, people protect their own interests above all else", 8.) "The major responsibility of people in this organisation is to control costs". Two items from independence, namely, 9.) “In this organisation, people are expected to follow their own personal and moral beliefs", 10.) "Each person in this organisation decides what is right and wrong" and two from Privacy, namely, 11.) "In this organisation, colleagues respect each other's privacy and do not broadcast other's personal information" and 12.) "This organisation believes all private and personal information gathered about others is company property."

Table 4.16 Monte Carlo Parallel Analysis of the ECQ (*n*=328)

	Monte Carlo		SPSS Varimax Initial Eigenvalues		
Factor	Total	95%	Total	Percentage of Variance	Cumulative Percentage
1	8.269	1.804	8.224	30.459	30.459
2	3.740	1.671	3.351	12.411	42.870
3	2.237	1.578	2.496	9.245	52.115
4	1.604	1.499	1.608	5.956	58.071
5	1.205	1.435	1.240	4.592	62.663
6	1.040	1.371	1.070	3.962	66.625

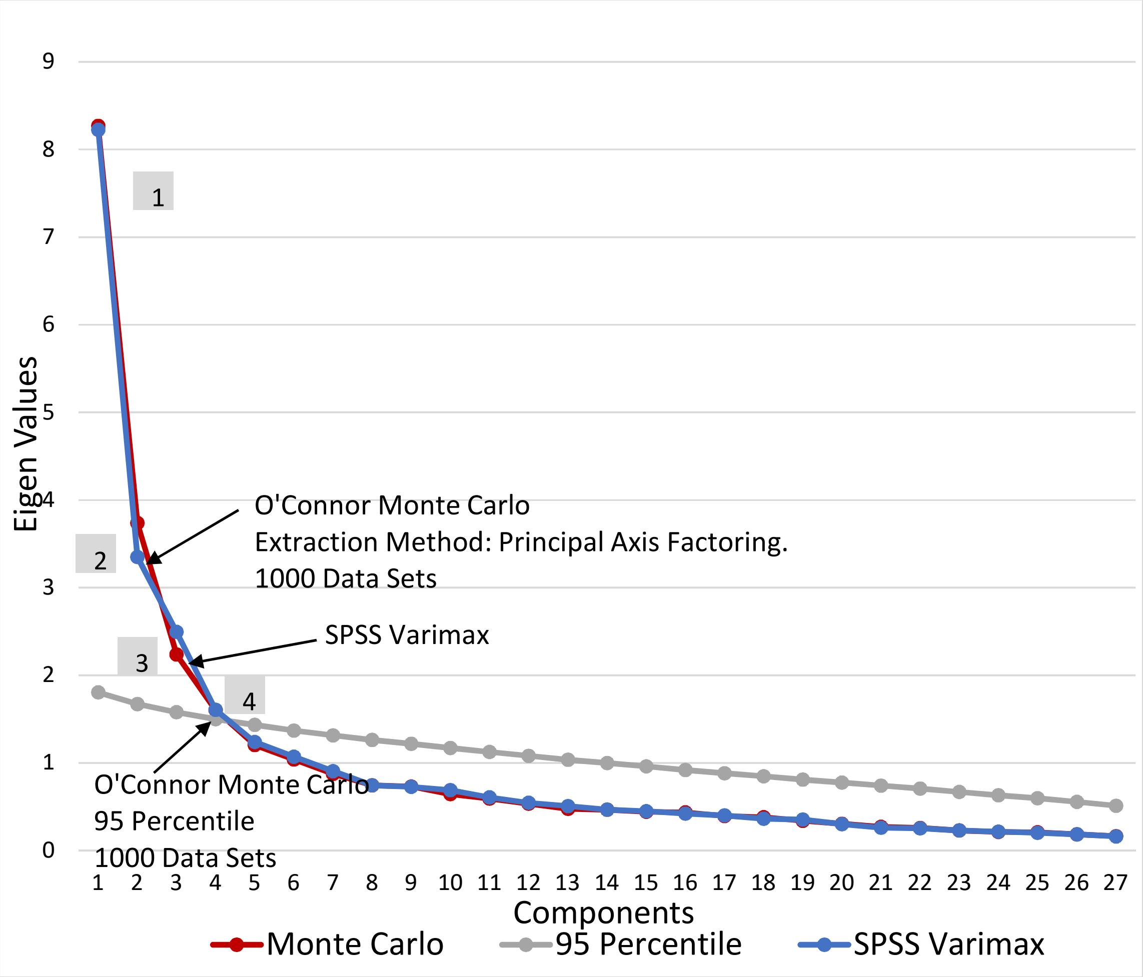


Figure 4.13. Monte Carlo Parallel Analysis (ECQ) (*n*=234).

This was followed with a CFA where a CFA then tested the four factors using IBM AMOS (version 23), resulting in the elimination of three further items in the questions about Instrumental Ethics, namely, 13.)"People are expected to do anything to further the organisation's interests, regardless of the consequences", 14.) "People here are concerned with the organisation's interests to the exclusion of all else", 15.) "Work is considered substandard only when it hurts the organisation's interests." to attain an acceptable model fit as depicted in

Figure **4.14**.

This resulted in each of the four extracted factors showing an average variance extracted (AVE) above the acceptable level of .5 and all above the acceptable value of .7 for the composite reliability (CR).

Each of the aggregated four factors was aggregated to form the endogenous variable organisational awareness used to test the dependence of ethical climate on responsible OSN engagement in meeting objective six.

4.3.4.4.1 The Reduction of the ECQ to a Four Factor 14 Item Variable

Using an EFA through SPSS in conjunction with a Monte Carlo PCA for parallel analysis, the ECQ was reduced to four factors defined as:

1. Ethical Work Environment
   (7 Items)
2. Instrumental Ethics or Self Interest
   (2 Items)
3. Independence or Personal Morality
   (3 Items)
4. Institutionalised Ethics
   (2 Items)

The results of the CFA in

Figure **4.14** yield a four ethical climate type typology, being 1.) ethics in the work environment, 2.) instrumental ethics or self-interest, 3.) independence or personal morals and 4.) organisational ethics. Noted from the CFA from

Figure **4.14** is the lower correlation between self-interest and personal morals to general ethics and organisational ethics. This may indicate that self-values and company values are not always aligned and that for the individual employee at times personal morals self and self-interest take preference over ethics in the work environment and organisational ethics or vice versa. As a medium for both personal and business communication, the employee is bound to be caught in the dichotomy of either promoting self-interest or the interests of the organisation while engaging with OSN platforms. This begs the question of whether the employees' perceptions an ethical climate is based on self-interest and individualism, suggesting either a negative leading to a moral disengagement from the organization or a positive influence identification with the organization and leading to moral engagement with the organisation, as found in the study and discussed in the literature review of Italian SMEs measuring ethical organisational climate of self-interest (Pagliaro *et al.*, 2018). In assessing the findings from the ECQ, this may imply that the importance of behavioural intentions when engaging with OSNs within an ethical climate of the organization is vital.

4.3.4.4.2 Model Fit Summary

To assess the model fit for the component reduced ECQ, comparison indices are used to check the suggested reduced ECQ model to the fit of a baseline independence model where the relationships between the observed variables are assumed to be zero. In assessing whether the fit the ECQ, we see from Table 4.18 that there is an improvement over the independence model where the common practice comparisons Goodness-of-Fit Index (GFI), the Normed Fit Index (NFI), the Comparative Fit Index (CFI), and the Adjusted Goodness-of-Fit Index (AGFI) meet accepted thresholds of all the commonly used comparison criteria as a good to acceptable fit (Byrne, 2010; Hooper et al., 2008; Schermelleh-Engel et al., 2003).

The measured value of Ratio Chi-square to degrees of freedom (CMIN / df), 2.425, is a good model fit where the ratio is preferred to be smaller between the good and acceptable values of 2 and 3, respectively (Schermelleh-Engel et al., 2003).

The measure of approximate fit in the population, the Root Mean Square Error of Approximation (RMSEA), reflects a value of .079, which, according to Browne and Cudeck, is subjective (1992). Values between .05 and .08 reflect a reasonable fit (Browne and Cudeck, 1992), anything less than .05 is a strong fit, and less than .10 is a reasonable fit (Fan, Thompson, and Wang, 1999).

This CFA and resulting model fit are sufficient for the researcher to aggregate the extracted items as an addiction and habits endogenous variable.

Table 4.17 Rotated Component Matrix (ECQ)

Rotated Component Matrix[a] (ECQ)

	Component				***Communalities***
Reduced Set of Variables	1	2	3	4	
13. Everyone is expected to stick by organisation rules and procedures. (V112)	.838				.737
9. In this organisation, the law or ethical code of their profession is the major consideration. (V108)	.784				.691
11. In this organisation, the first consideration is whether a decision violates any law. (V110)	.768				.629
12. It is very important to follow the organisation's rules and procedures here. (V111)	.767				.601
10. In this organisation, people are expected to strictly follow legal or professional standards. (V109)	.751				.581
15. People in this organisation strictly obey the organisation policies. (V114)	.724				.568
14. Successful people in this organisation go by the book. (V113)	.714				.582
8. People are expected to comply with the law and professional standards over and above other considerations. (V107)	.694				.583
17. In this organisation, people are mostly out for themselves. (V116)		.806			.708
19. People are expected to do anything to further the organisation's interests, regardless of the consequences. (V118)		.797			.652
16. In this organisation, people protect their own interests above all else. (V115)		.778			.631
20. People here are concerned with the organisation's interests â€” to the exclusion of all else. (V119)		.717			.575
18. There is no room for one's own personal morals or ethics in this organisation. (V117)		.702			.601
2. The most important concern is the good of all the people in the organisation as a whole. (V101)			.841		.782
1. What is best for everyone in the organisation is the major consideration here. (V100)			.816		.782

Rotated Component Matrix[a] (ECQ Cont.)

Reduced Set of Variables	*Component* 1	2	3	4	*Communalities*
3. Our major concern is always what is best for the other person. (V102)			.753		.651
24. Each person in this organisation decides for themselves what is right and wrong. (V123)				.832	.701
25. The most important concern in this organisation is each person's own sense of right and wrong. (V124)				.816	.682
26. In this organisation, people are guided by their own personal ethics. (V125)				.798	.659

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.

[a] *Rotation converged in 5 iterations. Factor loadings less than .40 have not been printed and variables have been sorted by loadings on each factor*

Table 4.18 Model Fit (ECQ)

Measure	Value	Threshold
CMIN	172.167	
df	71.000	
P	.000	<.05
CMIN/*df*	2.425	Ratio between 2 (good) and 3 (acceptable)
GFI	.91	(0 no fit. 1 perfect fit); >.95 good; >.90 acceptable fit
NFI	.90	(0 no fit. 1 perfect fit); >.95 good; >.90 acceptable fit
CFI	.94	(0 no fit. 1 perfect fit); >.97 good; >.95 acceptable fit
AGFI	.86	(0 no fit. 1 perfect fit); >.90 good; >.85 acceptable fit
RMSEA	.08	.05 represents close approximate fit

Ratio Chi-square/degrees of freedom (CMIN/df), Comparative fit index (CFI), Goodness-of-fit index (GFI), Adjusted Goodness-of-Fit-Index (AGFI), Normed fit index (NFI), Roots mean squared error of approximation (RMSEA)

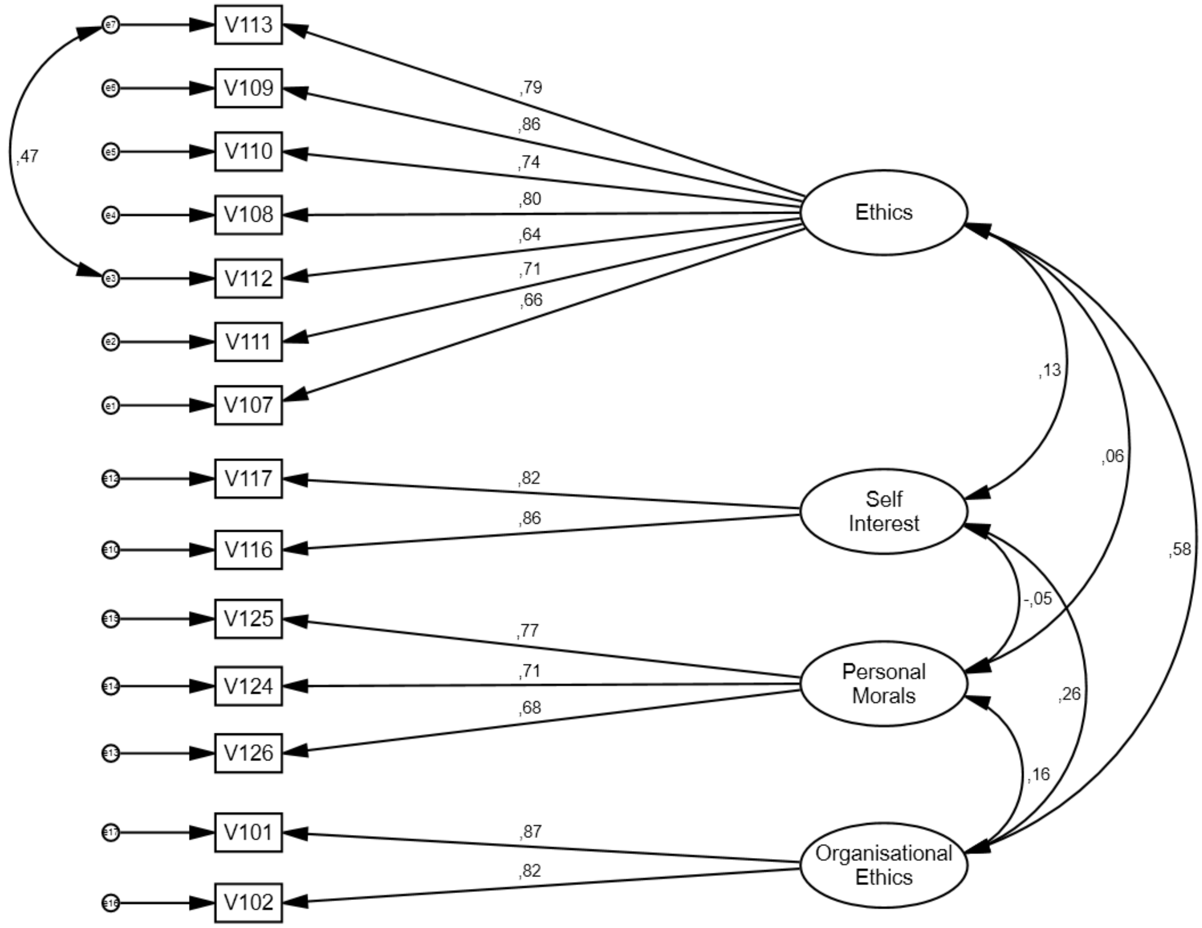


Figure 4.14 Confirmatory Factor Analysis Model (ECQ).

4.3.4.5 Factor Analysis of Classification of OSN Platforms

A key finding from the qualitative study was to group the OSN platform apps into four categories: Business type OSNs, Social type OSNs, Dual Purpose type OSNs and the little-used Niche Social type OSNs.

Table 4.19 Rotated Component Matrix of Frequency Usage of OSNs

Rotated Component Matrix[a]

	Component		
	1	2	3
Facebook	.820		
Facebook Messenger	.761		
Instagram	.607		
WhatsApp	.482		
YouTube	.314		

Rotated Component Matrix[a]

	Component		
	1	2	3
Viber		.707	
Tinder		.571	
Tumblr		.544	
WeChat		.532	
Snap Chat		.443	
Email			.670
Skype			.645
LinkedIn			.622
Twitter			.522
Pinterest			.297

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.
[a] Rotation converged in 5 iterations.

Using SPSS, an initial Exploratory Factor Analysis was conducted using Principal Axis Factoring as the Extraction Method and Varimax as the Rotation method to explore the underlying theoretical structure of the data to see if the reduced data identifies the OSN categories from the qualitative study. OSN usage revealed three-factor extractions in line with the classification, as seen in Table 4.19. This identification of OSN categories was used to match the case for gauging the responsible use of OSN platforms discussed in section 2.12 of the literature review. This classification, except for Pinterest, was corroborated through the qualitative research where the interviewees classified OSNs as those that were a positive impact on the day-to-day operations of the organisation, those that were predominantly social in nature with a limited positive impact on the organisation and those used by a limited number of employees who were purely social and had no positive impact to the business at all. The nature of the OSN Pinterest as a virtual pin board predominantly used as a bookmarking app did not fit into the business or social OSNs. So, it was decided to omit Pinterest from the business apps moving it to the niche app as the survey revealed a daily usage below 10% of the Pinterest OSN, limiting its influence as an OSN on the organisation.

As with the previous EFA analyses, a Monte Carlo PCA for parallel analysis was conducted, confirming the reduced number of factors.

It was decided to do a second Exploratory Factor Analysis using Principal Axis Factoring as the Extraction Method and Varimax as the Rotation method using the top ten OSNs in terms of frequency usage. Therefore, Pinterest was removed from the list, leaving the top nine frequency usage OSN applications, which resulted in extraction, as seen in Table 4.20

The second extraction helps further categorise the social and business OSN apps and simultaneously reveals a third factor which could be categorised as a crossover between the OSN app classifications. As with the first extraction, lower factor loadings included some OSN Apps, such as Twitter, in more than one of the three categories. The help of classification in the qualitative research findings yields the category of a dual app.

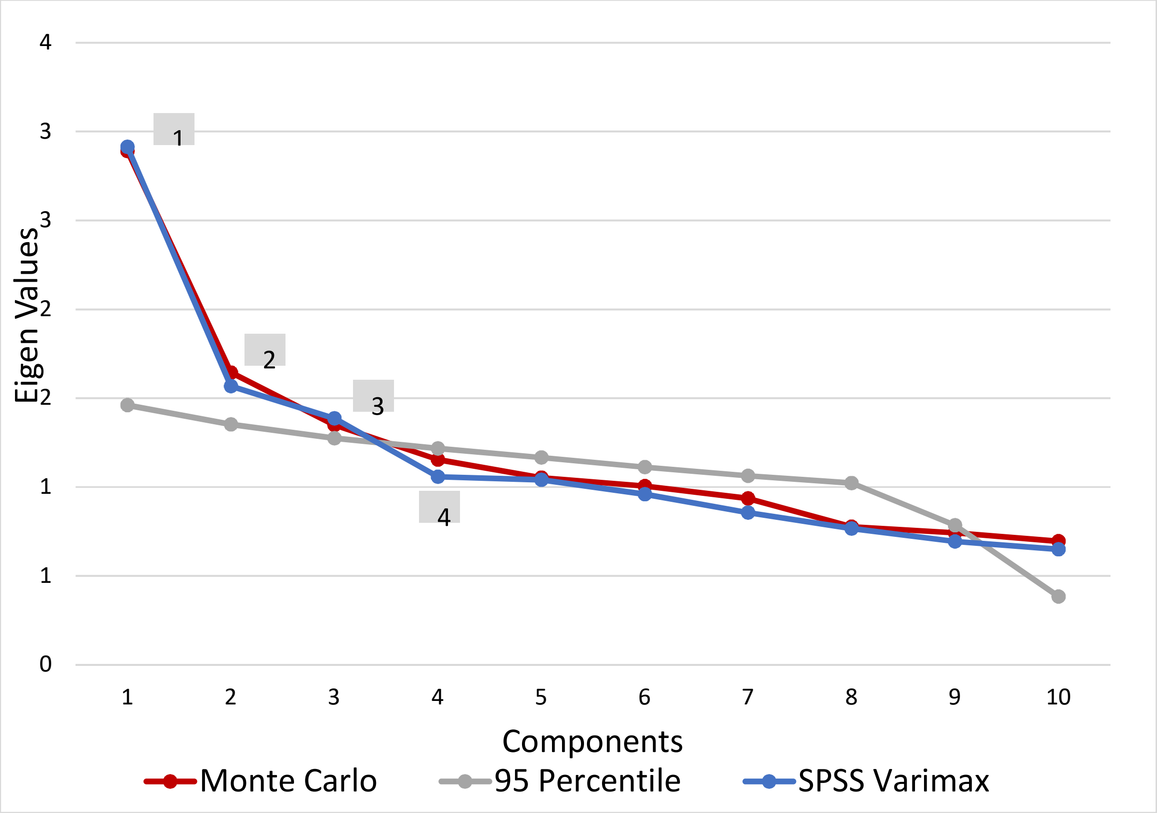


Figure 4.15 Monte Carlo Parallel Analysis (Classification of OSNs) (n = 328)

.

Table 4.20 Rotated Component Matrix of Top Nine OSNs

Rotated Component Matrix[a]

	Component		
	Social	Business	Dual Purpose
Facebook	.820		
Facebook Messenger	.806		
Instagram	.665		
LinkedIn		.787	
Skype		.723	
Twitter		.506	
WhatsApp			.850
Email		.456	.584
YouTube			.450

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.
[a] Rotation converged in 5 iterations.

4.3.5 *OSN Categorisation*

For this research, the final categorisation regarding the frequency usage of OSN apps follows:

4.3.5.1 Business Apps

4.3.5.1.1 Specific Apps identified in the research

Twitter, YouTube, LinkedIn, Skype, WhatsApp and Email

4.3.5.1.2 Key Purposes

Business communications, exchanging officially conversational text recorded open, private, and confidential correspondence. Exchange of documentation as electronic files that may be in the form of documents and images. The formation of management groups for group communication. These groups have now become crucial to effective management within most organisations.

Broadcast and content provided through video-sharing promoting relevant business concepts, products and services, often without having to advertise its products or services directly. Effective and popular medium for education, reviews, instructional and troubleshooting of products such as consumer goods and software. Business communication enables the spread of knowledge to a large captive audience (Cetto *et al.*, 2018).

4.3.5.1.3 Characteristics

- Messaging within groups. Accepted as formal business correspondence.
- Many organisations now accept signed photographed contracts sent via WhatsApp or email.
- Email or WhatsApp confirmation has become equivalent to physically signed confirmation.
- Broadcast and content

4.3.5.2 Social apps

4.3.5.2.1 Specific Apps identified in the research

Facebook, Facebook Messenger, Instagram, WhatsApp, Twitter, YouTube

4.3.5.2.2 Key Purposes

Making connections with friends, family, colleagues and people of personal interest for the purposes of social interaction, maintaining contact and keeping abreast of key events in the lives of connections.

4.3.5.2.3 Characteristics

- Creating Public Events
- Profile
  - Personal Information, Favourite movies, music, etc.
  - Status Update Relationships, etc.
  - Timelines highlight posts or images, add new life events
- Post and share photos, videos, news
- Geo-Tagging
- Reaction Buttons Likes and Reactions
- Comments
- Messenger Messages and inbox

- Notifications
- Groups
- News Feed

4.3.5.3 Dual apps

4.3.5.3.1 Specific Apps identified in the research.

Twitter, YouTube and WhatsApp

4.3.5.3.2 Key Purposes

Apps are used for social and business interaction, broadcast and personal entertainment and instruction, and content providing and promotion.

4.3.5.3.3 Characteristics

- Broadcast and content
- Messaging within groups. Accepted as formal business correspondence.

4.3.5.4 Niche apps

4.3.5.4.1 Specific Apps identified in the research

Viber, Tumbler, WeChat, Snap Chat Tinder, Pinterest*

4.3.5.4.2 Key Purposes

For this research, these OSNs were classified as Niche. They are, however, in their own right part of mainstream OSN functions that may be key business drivers in organisations, industries or populations groups not used for this research, typically used for blogs, forums, microblogs, social bookmarking and online dating, to name a few.

4.3.5.4.3 Characteristics

- Dating, forums, blogs, etc.

4.3.5.5 Previous Categorisation of OSNs

The classifications derived in this study have similar traits to those derived in two recent studies classifying OSNs. The resultant classification of first study published in 2016, was the 5Cs, namely Communicating, Connecting, (Business apps and Social apps) Collaborating, Combining (Business apps and Dual Purpose apps) and Completing, (Niche apps and Dual Purpose apps) (Vuori and Jussila, 2016). The classification of the second study published in 2020, was social, entertainment and profiling networks (Koukaras, Tjortjis and Rousidis, 2020). It must be noted at the time each of the studies categorised OSN platforms into groups in terms of similar functions based on the designed purpose. The classification resulting from this study however has been derived and named from perceived usage and factor analysis from actual self-reported frequency of use. In addition, it is noted that only the top ten OSN apps where used for the classification process.

4.3.6 *Regression analysis and testing for mediation*

The next phase of the analysis focussed on determining the statistical relationship between levels of (i) online privacy literacy, (ii) online self-awareness and online organisational awareness as exogenous variables (predictors) as defined from the constructs in the literature review under section *2.7 A Case for Online Self-Awareness as an Influencing Factor*, section *2.9 A Case for Online Privacy Literacy as an Influencing Factor* and section *2.11 A Case for Online Privacy Literacy as an Influencing Factor*, respectively, and levels of the frequency usage of the endogenous variables, business apps, (iii) social apps, (iv) dual apps, (v) top 10 apps, and (vi) niche apps as defined under The Levels of Responsible OSN Engagement within the organisation, in assessing the levels of responsible OSN engagement.

In addition, the analysis also focussed on determining the mediating roles of online security behaviour and addiction and habits between the exogenous and endogenous variables.

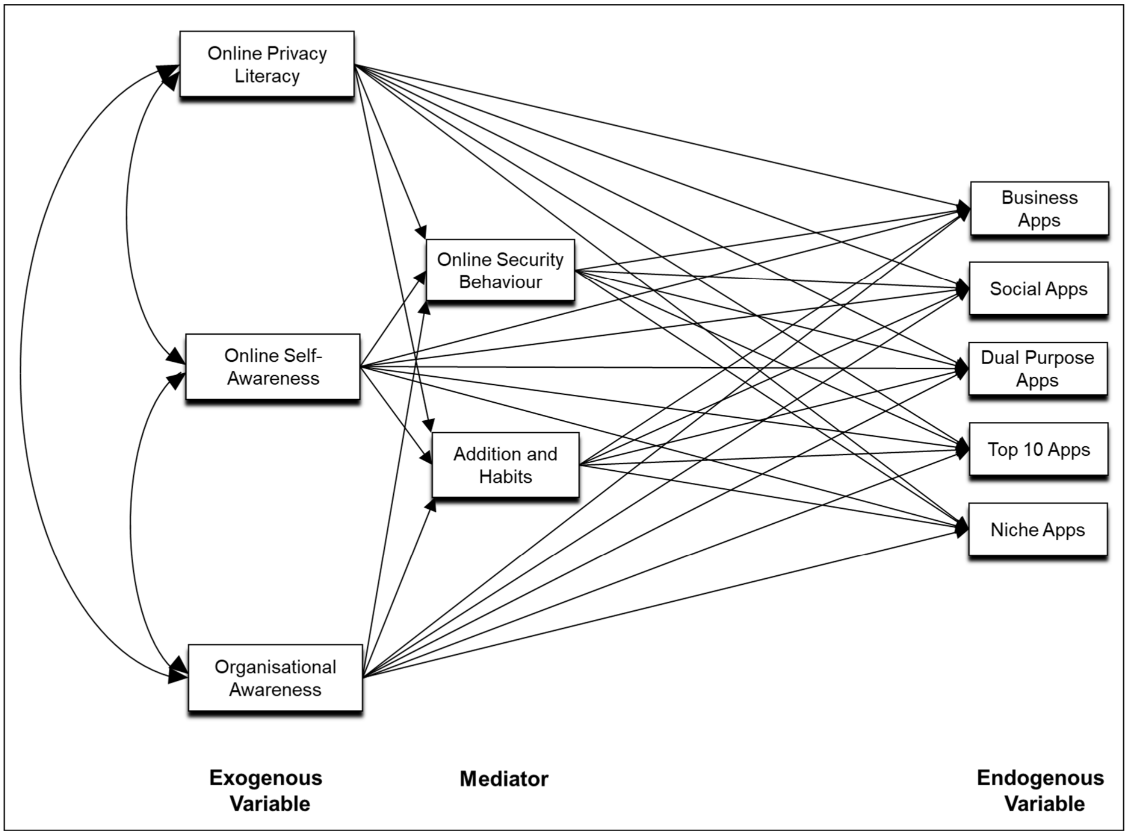


Figure 4.16 Conceptual measurement model

Figure 4.16 provides a graphical presentation of the proposed conceptual measurement model being tested.

A stepwise regression analysis using Hayes's PROCESS macro on IBM SPSS (version 25) was employed to test the various linear paths.

As a first step, the statistical relationships between the exogenous and endogenous variables in the absence of the mediators were determined, as shown in

Table 4.21. In mediation analyses, these are referred to as the total effects models.

Table 4.21 Regression model outcomes of the relationship between the exogenous and endogenous variables (Total Effects Model).

Endogenous Variable	Exogenous	Model Statistics	Std Beta (p-value)
Business Apps	Online Privacy Literacy	R^2=0.244; Adj R^2=0.234	0.464 (<.001)
	Online Self-Awareness	F(3,230)=24.733, p<.001	0.062 (0.297)
	Organisational Awareness		0.151 (0.012)
Social Apps	Online Privacy Literacy	R^2=0.015; Adj R^2=0.002	0.123 (0.064)
	Online Self-Awareness	F(3,230)=1.177, p=0.319	-0.011 (0.868)
	Organisational Awareness		0.026 (0.701)
Dual Apps	Online Privacy Literacy	R^2=0.103; Adj R^2=0.091	0.303 (<.001)
	Online Self-Awareness	F(3,230)=8.774, p<.001	-0.001 (0.989)
	Organisational Awareness		0.125 (0.055)
Top 10 Apps	Online Privacy Literacy	R^2=0.079; Adj R^2=0.067	0.015 (<.001)
	Online Self-Awareness	F(3,230)=6.551, p<.001	0.066 (0.639)
	Organisational Awareness		0.041 (0.334)
Niche Apps	Online Privacy Literacy	R^2=0.014; Adj R^2=0.002	0.010 (0.699)
	Online Self-Awareness	F(3,230)=1.117, p=0.343	0.043 (0.810)
	Organisational Awareness		0.027 (0.083)

The following significant paths are reported in

Table 4.21:

- Online privacy literacy on business apps (Std Beta = 0.464; p<0.001). Higher values of online privacy literacy have a positive linear relationship with higher levels of business apps.
- Online organisational awareness on business apps (Std Beta = 0.151; p<0.05). Higher values of online organisational awareness have a positive linear relationship with levels of business apps.
- Online privacy literacy on dual apps (Std Beta = 0.303; p<0.001). Higher values of online privacy literacy have a positive linear relationship with levels of dual

apps.

- Online privacy literacy on top 10 apps (Std Beta = 0.067; p<0.001). Higher values of online privacy literacy have a positive linear relationship with levels of top 10 apps.

As a second step, the statistical relationships between the exogenous and the mediating variables were determined. The results are presented in Table 4.22.

Table 4.22 Regression model outcomes of the relationship between the mediating and exogenous variables

Mediating variable **(dependent)**	**Exogenous variable**	**Model statistics**	**Std Beta** **(p-value)**
Online Security Behaviour	Online Privacy Literacy	R^2=0.214; Adj R^2=0.203	0.021 (<.001)
	Online Self-Awareness	F(3,230)=20.834, p<.001	0.090 (<.001)
	Organisational Awareness		0.056 (0.027)
Addiction and Habits	Online Privacy Literacy	R^2=0.056; Adj R^2=0.043	0.022 (0.035)
	Online Self-Awareness	F(3,230)=4.527, p=0.004	0.095 (0.027)
	Organisational Awareness		0.059 (0.226)

The following significant paths are reported in Table 4.22:

4.3.6.1 Online Security Behaviour

- A positive linear relationship between online privacy literacy and online security behaviour (r=0.021, p<.001)
- The relationship between online self-awareness and online security behaviour (r=0.090, p<.001)
- The relationship between online self-awareness and online security behaviour (r=0.056, p<.05)

4.3.6.2 Addiction and habits

- The relationship between online privacy literacy and addiction and habits (r=0.022, p<.05)
- The relationship between online self-awareness and addiction and habits (r=0.095, p<.05)

The third step was to estimate path coefficients between the exogenous and endogenous variables in the presence of the mediators, as shown in Table 4.23. In mediation analyses, these are referred to as the direct effects models.

The following significant paths are reported in Table 4.23. The relationship between online privacy literacy and business apps (r=0.464, p<.001).

- The relationship between online organisational awareness and business apps (r=0.151, p<.05).
- The relationship between online privacy literacy and dual apps (r=0.303, p<.001).

- The relationship between online privacy literacy and top 10 apps (r=0.015, p<.001).

The last step involved assessing the indirect effects of the mediators on the statistical relationship between the exogenous and endogenous variables. Again, Hayes's PROCESS macro was used, and the indirect effect was tested using a bootstrap estimation approach with 5 000 samples. The results are reported in Table 4.23.

Introducing both mediators running in parallel show similar-sized significant effects but with different sign (one positive and one negative) resulting in insignificant total indirect where the total indirect effect is calculated as the sum of the direct effect of X and the mediated indirect effects, namely online security behaviour and addiction and habits. As in the case of this study, where the bootstrap confidence intervals were calculated based on 5 000 random samples estimating the significance of the effects, where the effect is considered significant if the upper to the lower confidence intervals do not cross through zero (Hayes, 2013). In the case of this study, the mediators, on the one hand, show a positive intention to engage responsibly toward online security while simultaneously showing a negative tendency towards the susceptibly of OSN addiction and lousy texting habits. This invariably results in the confidence levels of the total indirect effect crossing through zero.

However, an insignificant total indirect effect may, as suggested by Hayes and Rockwood and several subsequent recent publications, not necessarily negate significant effects from the mediators in the parallel mediation model (Hayes and Rockwood, 2016; Meule, 2019; Miranda *et al.*, 2019)). As shown in Table 4.23, both online privacy literacy and addiction and habits can be significant and should be analysed as such.

The following significant mediating indirect paths are reported in Table 4.23.

Business apps

- The relationship between online privacy literacy and business apps is mediated by online security behaviour (Std *b*= 0.046, 95% CI= 0.013; 0.087) while at the same time mediated by addiction and habits (Std b= -0.027, 95% CI= -0.062; -0.003).
- The relationship between online self-awareness and business apps is mediated by online security behaviour (Std *b*= 0.055, 95% CI= 0.016; 0.104) while at the same time mediated by addiction and habits (Std b= -0.029, 95% CI= -0.071; -0.001).
- The relationship between online organisational awareness and business apps is mediated by online security behaviour (Std *b*= 0.024, 95% CI= 0.001; 0.051).

4.3.6.3 Social apps

- The relationship between online privacy literacy and social apps is mediated by online security behaviour (Std b= 0.064, 95% CI= 0.024; 0.118) while at the same time mediated by addiction and habits (Std b= -0.057, 95% CI= -0.113;-0.007).
- The relationship between online self-awareness and social apps is mediated by online security behaviour (Std *b*= 0.078, 95% CI= 0.031; 0.134) while at the same time mediated by addiction and habits (Std b= -0.062, 95% CI= -0.131; -0.003).
- The relationship between online organisational awareness and social apps is mediated by online security behaviour (Std b= 0.034, 95% CI= 0.004; 0.071).

4.3.6.4 Dual apps

- The relationship between online privacy literacy and dual apps is mediated by online security behaviour (Std b= 0.048, 95% CI= 0.018; 0.109) while at the same time mediated by addiction and habits (Std b= -0.040, 95% CI= -0.085; -0.005).

- The relationship between online self-awareness and dual apps is mediated by online security behaviour (Std b= 0.058, 95% CI= -0.071; -0.001) while at the same time mediated by addiction and habits (Std b= -0.043, 95% CI= -0.095; -0.002).
- The relationship between online organisational awareness and dual apps is mediated by online security behaviour (Std b= 0.025, 95% CI= 0.001; 0.051).

4.3.6.5 Top 10 apps

- The relationship between online privacy literacy and top 10 apps is mediated by online security behaviour (Std b= 0.062, 95% CI= 0.024; 0.113) while at the same time mediated by addiction and habits (Std b= -0.048, 95% CI= -0.098; -0.006).
- The relationship between online self-awareness and top 10 apps is mediated by online security behaviour (Std b= 0.076, 95% CI= 0.029; 0.134) while at the same time mediated by addiction and habits (Std b= -0.052, 95% CI= -0.113; -0.001).
- The relationship between online organisational awareness and the top 10 apps is mediated by online security behaviour (Std b= 0.033, 95% CI= 0.003; 0.066) while at the same time mediated by addiction and habits.

4.3.6.6 Niche apps

- The relationship between online privacy literacy and social apps is mediated by addiction and habits (Std b= -0.043, 95% CI= -0.091;-0.005).
- The relationship between online organisational awareness and social apps is mediated by addiction and habits (Std b= -0.046, 95% CI= -0.105; -0.001).

Table 4.23 Online Security Behaviour and Addiction and Habits as mediators

	Exogenous Variable								
Endogenous Mediator Variable	**Online Privacy Literacy**			**Online Self-Awareneass**			**Organisational Awareness**		
Business Apps									
Total effects	0.464 *(p<.001)*			0.062 *(p=0.297)*			0.151 *(p=0.012)*		
Direct Effect	0.446 *(p<.001)*			0.036 *(p=0.554)*			0.143 *(p=0.015)*		
		95% CI			***95% CI***			***95% CI***	
		Lower	***Upper***		***Lower***	***Upper***		***Lower***	***Upper***
Total Indirect Effect	0.019	-0.029	0.066	0.026	-0.028	0.082	0.008	-0.031	0.042
Online Security Behaviour	0.046	0.013	0.087	0.055	0.016	0.104	0.024	0.001	0.051
Addiction and Habits	-0.027	-0.062	-0.003	-0.029	-0.071	-0.001	-0.016	-0.049	0.008
Social Apps									
Total effects	0.123 *(p=0.064)*			-0.011 *(p=0.868)*			0.026 *(p=0.701)*		
Direct Effect	0.116 *(p=0.064)*			-0.027 *(p=0.676)*			0.026 *(p=0.674)*		
		95% CI			***95% CI***			***95% CI***	
		Lower	***Upper***		***Lower***	***Upper***		***Lower***	***Upper***
Total Indirect Effect	0.007	-0.063	0.079	0.016	-0.070	0.100	0.000	-0.062	0.059
Online Security Behaviour	0.064	0.024	0.118	0.078	0.031	0.134	0.034	0.004	0.071
Addiction and Habits	-0.057	-0.113	-0.007	-0.062	-0.131	-0.003	-0.034	-0.088	0.018
Dual Pupose Apps									
Total effects	0.303 *(p<.001)*			-0.001 *(p=0.989)*			0.125 *(p=0.055)*		
Direct Effect	0.295 *(p<.001)*			-0.015 *(p=-0.816)*			0.124 *(p=0.048)*		
		95% CI			***95% CI***			***95% CI***	
		Lower	***Upper***		***Lower***	***Upper***		***Lower***	***Upper***
Total Indirect Effect	0.008	-0.048	0.063	0.014	-0.051	0.079	0.001	-0.047	0.044
Online Security Behaviour	0.048	0.014	0.094	0.058	0.018	0.109	0.025	0.002	0.054
Addiction and Habits	-0.040	-0.085	-0.005	-0.043	-0.095	-0.002	-0.024	-0.066	0.013
Top 10 Apps									
Total effects	0.272 *(p<.001)*			0.026 *(p=0.693)*			0.064 *(p=0.334)*		
Direct Effect	0.257 *(p<.001)*			0.002 *(p=0.972)*			0.059 *(p=0.335)*		
		95% CI			***95% CI***			***95% CI***	
		Lower	***Upper***		***Lower***	***Upper***		***Lower***	***Upper***
Total Indirect Effect	0.015	-0.049	0.080	0.024	-0.054	0.098	0.005	-0.052	0.055
Online Security Behaviour	0.062	0.024	0.113	0.076	0.029	0.134	0.033	0.003	0.066
Addiction and Habits	-0.048	-0.098	-0.006	-0.052	-0.113	-0.001	-0.028	-0.075	0.015
Niche Apps									
Total effects	0.026 *(p=0.699)*			0.016 *(p=0.810)*			-0.119 *(p=0.083)*		
Direct Effect	0.048 *(p=0.464)*			0.039 *(p=0.577)*			-0.104 *(p=0.117)*		
		95% CI			***95% CI***			***95% CI***	
		Lower	***Upper***		***Lower***	***Upper***		***Lower***	***Upper***
Total Indirect Effect	-0.023	-0.087	0.043	-0.022	-0.100	0.055	-0.015	-0.065	0.034
Online Security Behaviour	0.020	-0.015	0.067	0.024	-0.020	0.077	0.010	-0.007	0.041
Addiction and Habits	-0.043	-0.091	-0.005	-0.046	-0.105	-0.001	-0.025	-0.071	0.012

4.3.7 *Further Quantitative Analysis of Moderation Variables*

The primary focus of this research in meeting objectives four, five and six was to gauge the dependence of the three factors identified in the literature review that influence responsible and abusive OSN engagement within organisations namely; Online Self-Awareness (objective four), online privacy literacy (objective five) and Organisational awareness (objective six).

The moderating factors namely OSN frequency usage by industry, gender, generation and qualification levels were considered in light of these objectives however, the research sample was made of several organisations in two different industries that have a varied and different mix of gender, generation and qualification levels dependent on the type of industry and size of an organisation.

The possible moderating effects concerning gauging the objectives specific to industry and generation were explored with findings reported from the qualitative analysis. The initial statistical findings provided further insight and findings reported the possible moderating effects of in a particular generation.

A further breaking down of sample sizes within each industry or organisation for accurate moderation analysis not only deviates from the primary focus key objectives but would be beyond the scope of this study.

CHAPTER 5 : DISCUSSION, CONCLUSION AND RECOMMENDATIONS

5.1 INTRODUCTION

Chapter 5 concludes this research. A summary of the research with the findings from both the quantitative and qualitative results are discussed and interpreted. The conclusions drawn from the results were based on the purpose, research objectives and questions of the study. The interpretations and implications from the results of the quantitative and qualitative findings lead to the development and presentation of an OSN governance framework. Further recommendations based on the conclusions and purpose of the study are presented.

5.2 QUALITATIVE FINDINGS DISCUSSION

5.2.1 *Personal Online Behaviour*

The invariable response of the interviewees reflected the academic literature that controlling the impulsive human nature to voice one’s convictions and disseminate information on an OSN platform can indeed be challenging. Those from senior management who are part of the digital immigrants felt that there was a definite sense that the consequence of information disclosure's intent depends on the generation. Coming from an era where communication was not instant, the digital immigrant was more cautious regarding information disclosure. Communication of the digital immigrant is more deliberate, whereas, for the younger generations who are seen to be ‘surgically’ bonded to their mobile devices, communication is like background noise, communication is less deliberate, and they often do not think about the consequences of what is being disclosed, it's just part of a stream of continuous communication.

The consequence of the intent of information disclosure was further deemed by the employee to be dependent on the types of OSN app being used, whether it be a business-oriented, social or dual-purpose OSN app. However, the concern from management was that no matter the purpose of the OSN app, information disclosure may still be open to the general public and that frivolous careless open messaging may have grave consequences for the employee representing the organisation. The personal awareness of the employee of the consequence of who, what, and the potential reach of the type of OSN app being used when messaging or posting, whether for personal or business reasons, is of paramount importance.

Concerns about compulsive social behaviour were evident from almost all the interviewees. However, social factors that have been proven to contribute to compulsive social behaviour, such as a lack of self-esteem, were not noticed or recognised by management, making the susceptibility to social media addiction more of an unknown factor. The general response to the compulsive behaviour was the need to consistently stay connected to the organisation, continually checking messages or email for any incoming communication. There was a concern that the organisation is open to the fragility of compulsive behaviour-driven emotional needs and insecurities, as mentioned earlier by a medical practitioner

> *"…I'd see possibly reason for concern, so alarm bells like whether they need emotional support."*

When questioned about the effects of a lack of self-esteem on OSN usage, the discussion invariably moved towards cyberbullying or OSN abuse. However, a few respondents viewed a lack of self-esteem as more likely to manifest itself through high levels of anxiety and low levels of impulse control that could be subject to corporate cyberbullying. A repeated example discussed was the anxiety raised by WhatsApp's blue ticks that indicate to the sender that the recipient has read the sent message and not responding immediately.

From the observations and the analysis of the interviews in the qualitative study, an online self-awareness regarding responsible OSN engagement is about the employee being self-aware of their behavioural intent regarding information disclosure when engaging on OSNs. This meets objective four where responsible engagement of OSNs within the organisation is dependent on the employee's personal online behaviour as derived from the literature review as online self-awareness. From a management perspective, online self-awareness should be a key element in a governance framework to empower the employee with confidence as a representative of the organisation to manage the challenge of compulsive social communication when disseminating information on an OSN platform.

5.2.2 *Personal Online Privacy*

In general, most interviewees felt challenged by their own level of online privacy literacy and had a limited view of the level of the average employee. However, there was an underlying theme that the average employee who fell into the millennial generation was far more *au fait* with mobile device security settings and online privacy literacy. Some actually saw their staff as a resource to improve their own literacy, as mentioned by one of the managers in the healthcare sector, who stated:

> *"I think my staff is quite clued up with that, hey. Cos if I battle with my cell phone, I ask one of the staff, and they can sort it out. So they are well informed."*

There was comfort all the interviewees said that, when it came to their desktop workstation, that online privacy and security settings were well handled by the IT department but only to the degree that it was acknowledged that, when it came to mobile phones and other devices, the levels of online privacy literacy and security settings was of prime concern. As a result, all saw the urgency for ongoing training and awareness. Some interviewees went as far as to suggest a company IT helpline dedicated to assisting employees with the privacy settings of a new OSN or mobile device.

From the qualitative research, responsible engagement of OSNs within the organisation depends on the employee's online privacy literacy and is an area that requires ongoing training and education, meets objective five. Concern was expressed with OSN apps like WhatsApp, which often contained patient information, company gossip, and complaints about management, which go to company values. There was a view that a complete lack of online privacy awareness resulting in a breach of an online privacy protocol is best controlled through a decisive action such as potential dismissal. However, many of the interviewees thought this scenario would be somewhat extreme.

There is a unanimous consensus that online privacy literacy competency levels require ongoing training and education and should be included as a module in organisation induction and part of the governance framework as a continuing education aspect or in refresher programmes.

5.2.3 *Organisational Awareness*

The consensus was that the complexities in the responsible business usage of an OSN often lie in that the OSN landscape OSN apps are used for both business and social communication and are challenging and difficult to enforce merely through documented organisational procedures and policies. There was an overwhelming consensus that responsible OSN usage should be driven and promoted through an awareness of the organisation’s values and culture, which should be spelt out to employees from the outset of their tenure. The employees' personal perspective comes back to their moral values regarding what they communicate, provided it complies with the organisation’s policies. This would be in keeping with the professional values such as client confidentiality historically embedded in both the financial services and healthcare industries. In understanding, embracing, and subscribing to the organisation’s values and culture, employees will do what is best for the organisation, themselves, and others. The hope is that employees will live up to the organisation's values so when there's a decision to send an email or post something on Facebook, they exercise the behaviours they live up to. Employees must maintain the professionalism of their vocation and industry, aware that they are engaging on a public platform as ‘ambassadors’ for the organisation. In the case of transparency, the employee must rely on the company's values. In other words, what are the do's and the don’ts expected of them?

However, during the discussion with senior management, there was a distinct apprehension that there should be reliance on organisational culture and values. In the discussion around driving the organisational values and culture to address notions found in the literature, such as the “Loss of Control” concerning responsible OSN engagement, three tangible factors emerged, namely 1.) Defining clear documented governance and policies, 2.) Training and awareness in the use of OSNs, and 3.) Decisive action should there be a compliance breach in the organisation’s governance, policies, and procedures. Addressing the notion of “Loss of control” is about not controlling the human impulse to engage without premeditated thought resulting in possible careless, though it may be unintentional, irresponsible messaging. Most interviewees had an underlying theme, particularly senior management, that there is clearly a need for ongoing training with an awareness of the dangers of impulsive, reactive OSN engagement to the organisation and the communicator. Specific awareness of values within the digital world is needed. One must spell out the consequences of not managing their digital world directly. One cannot simply rely on values, and the employee should sign an acknowledgement that they understand the organisation's policy concerning OSN engagement. Any breach of organisational OSN engagement cannot be tolerated and must be met with decisive action, whether based on company policy or legal aspects.

It was also noted that embedded in organisational values and culture is a personal code of ethics guiding the individual employee, and this derives, among other things, from one's education, upbringing and religion.

Interviewees mentioned that OSN communication within the organisation is effectively governed by employees themselves, particularly in group communication. For example, a WhatsApp management or team group employee will immediately reprimand any group member stepping out of line with an inappropriate OSN media post or comment. The more senior interviewees expressed caution regarding today's younger generation of employees who subscribe less to loyalty and their contribution to the organisation but tend to be more motivated by monetary rewards. This means that an eagerness to subscribe to the organisation's culture and values should not be assumed. This could be ascribed to an emerging work culture as seen in the notion of the South African "the job-hopping millennial" (Vittee and Makhubele, 2016) and in recent studies on job satisfaction of young versus older employees (Kollmann et al., 2020) and or as noted earlier by an interviewee, who stated:

> *"I can't say that, under the current economic climate, I don't think a lot of people out there working for the sake of a job, not necessarily because they want to help care for people necessarily."*

The executive and senior management respondents were in unison that organisational awareness driven by the employee's professionalism and that the organisation's culture and value system go a long way in mitigating the reputational risk of being vulnerable to the fragility of the human impulse when engaging in OSNs. This addresses objective six where the organisation's responsible engagement of OSNs is influenced by the employee's organisational awareness and is echoed in a medical practitioner's comment regarding an unprofessional post

> *"…it was explained in no uncertain terms that her online behaviour reflected on the company."*

5.2.4 *Behavioural Intent Awareness*

As a core theme emanating from the qualitative study, behavioural intent awareness can be defined as an awareness of the factors influencing and motivating the employee's willingness to perform a behaviour. As defined in this study, the notion of radical transparency cautions against a reactive and impulsive nature when communicating face-to-face or over the telephone. The dangers of radical transparency should to be managed with personal and organisational awareness as part of one's responsible behavioural intent when engaging with OSNs.

The theory of planned behaviour (Ajzen, 1991) suggests that behaviours are determined by behavioural intentions, which are determined by a combination of three factors: attitude toward the behaviour, subjective norms, and perceived behavioural control. Being aware of the personal influences of one's own online behaviour can be viewed as one's attitude to behaviour. Being aware of and identifying with the online culture and values of the organisation can be viewed as abiding to the subjective norms of the organisation. Maintaining a high competency in online literacy can be viewed as a form of perceived behavioural control. Therefore, one might associate behavioural intent awareness as discussed in this study to the Fishbein-Ajzen theory of planned behaviour model (Fishbein and Ajzen, 1975; Christian *et al.*, 2019). However, from the analysis of the qualitative study, it may difficult to distinguish between personal attitude towards the consequences of behaviour and the normative values of organisational culture (Miniard and Cohen, 1981).

This study's key objectives were to analyse and assess critical factors influencing OSN responsible engagement leading to a governance framework for the organisation. Further analysis of the merits of formally relating behavioural intention awareness in responsible OSN engagement to the Fishbein-Ajzen Theory of Planned Behaviour possible leading to the theory of planned behaviour is beyond the scope of this study and, thus, a limitation. Nevertheless, the developed themes of personal online behaviour, personal online privacy, and organisational behaviour lead to the core theme of behavioural intent awareness contributing toward responsible use OSN platforms. The themes from the qualitative analysis of the interviews conducted meet objective two of this study. This objective leads to objective seven in developing a conceptual governance framework for responsible engagement on OSNs.

5.3 QUANTITATIVE FINDINGS DISCUSSION

The classification of frequency usage of OSN platforms emanated through the measurement of the frequency of specific OSN platforms. Responsible use of the gauge responsible OSN usage from the plethora of OSN platforms accessible to the average employee revealed a grouping and taxonomy of OSN platforms regarding factor rotation of frequency usage from the selected organisations within financial services and healthcare industries. After an EFA analysis of the frequency usage of OSNs selected in this research was performed together with the help of OSN classifications in the qualitative research findings yields the following classification of frequency usage of OSN platforms:

1. **Business apps** (*Twitter, YouTube, LinkedIn, Skype, WhatsApp and Email*).
2. **Social apps** *(Facebook, Facebook Messenger, Instagram, WhatsApp, Twitter, YouTube).*
3. **Dual apps** *(Twitter, YouTube and WhatsApp).*
4. **Niche apps** *(Viber, Tumbler, WeChat, Snap Chat Tinder, Pinterest).*

The classification of frequency usage of OSN platforms is key in gauging the levels of responsible OSN engagement as ascertained from the literature review, where the levels of responsible OSN engagement within the organisation can be gauged by the usage frequency levels of business platforms relative to social-based platforms. The category of top 10 apps was added as a comparative baseline. Gauging the frequency usage of each group of OSN apps and endogenous variables through the regression analysis enabled gauging the influence the three defined constructs, namely, online self-awareness, online privacy literacy and organisational awareness, have on responsible OSN engagement. As defined in 2.13.1. in the literature review, the higher self-reported levels of frequency usage engagement with business platforms to that of social platforms are observed as an indicator of higher levels of responsible usage.

5.3.1 *Online Self-Awareness*

There is no significant direct effect of online self-awareness in any defined categories of OSN Apps. This is corroborated from the qualitative findings where self-esteem was not perceived or recognised by management, making the susceptibility to social media addiction more of an unknown factor. This may appear to be contrary to the findings from the literature review, where the more positive the employee’s self-esteem and self-efficacy, the more vigilant and aware the employee is toward their online security behaviour and OSN addiction. However, regression analysis revealed significant mediation by introducing the two self-reported variables ‘online security behaviour’ and ‘addiction and texting habits’ as parallel mediators run in parallel. The regression analysis reveals a small effect through online security behaviour between online self-awareness and the frequency usage of social apps, dual apps, top 10 apps and business apps. Simultaneously, they reveal a small effect through the mediator variable addiction and habits from online self-awareness to the frequency usage of social apps, top 10 apps, niche apps, and a lesser effect toward dual purpose and business apps.

The results indicate the need to promote behavioural intent toward online security behaviour and behavioural vigilance against addiction and texting habits as a fundamental principle to responsible OSN engagement. Developing online self-esteem and online self-efficacy regarding personal online self-awareness should go on to encourage and empower the employee with the confidence to follow through with online security behaviour to actively pursue online privacy and security while guarding against OSN addiction and lazy texting habits. This meets objective four whereby responsible engagement of OSNs within the organisation depends on the employee’s online self-awareness. Company programmes and processes within its governance framework should include developing the employee’s online self-esteem and online self-efficacy.

5.3.2 *Online Privacy Literacy*

A medium to high direct effect reveals the association that the higher the competency of online privacy literacy is, the higher the level associated of frequency usage toward business apps, top 10 apps and dual apps in order of direct effect. The associated direct effect of online privacy on social apps and niche apps is insignificant

The two self-reported variables ‘online security behaviour’ and ‘addiction and texting habits’ as parallel mediators using regression analysis revealed significant mediation by online security behaviour between online privacy literacy and the business apps, dual apps, top 10 apps, including social apps. Simultaneously, the mediator variable addiction and habits revealed a significant effect between online privacy literacy and the OSN categories of social apps, top 10 apps, niche apps, dual apps and, to a lesser extent business apps.

From an organisational perspective, the higher the competency of the employee's online privacy literacy, the higher the association of frequent usage of business-friendly apps. However, irrespective, of high levels of online privacy literacy, the findings show positive behavioural intent toward online security promotes responsible OSN engagement. Simultaneously, vigilance against OSN addiction and bad texting habits will support responsible engagement with OSNs. As a mediator, both online security behaviour and addiction and habits show the highest effect on the frequency of use of social apps, followed by top 10 apps, dual apps, and then to a lesser extent, business apps.

As with the consensus from qualitative findings, that online privacy literacy competency levels require ongoing training and education, the results indicate the importance of training and awareness within the organisation's governance framework in developing the employee's online privacy literacy regarding security and privacy settings. Training and awareness with regards to online privacy literacy will enhance the positive behavioural intent when engaging with OSN platforms and meets objective five where responsible engagement of OSNs within the organisation depends on the employee's online privacy literacy. Furthermore, it is imperative to monitor and consistently remind and encourage the employee to actively maintain and apply security vigilance while guarding against OSN addiction and bad texting habits especially when using socially orientated OSN platforms.

5.3.3 *Organisational Awareness*

Better organisational ethics regarding the construct of online organisational awareness shows a small significant direct effect associated with more frequent use of business apps and dual apps. From an organisational perspective, a richer ethical climate in the organisation, is associated with more frequent use of business-friendly apps. Furthermore, introducing the mediating variables 'online security behaviour' and 'addiction and habits' in parallel using regression analysis, shows a small indirect effect from online organisational awareness through online security behaviour to the social apps, dual apps, top 10 apps and business apps. Simultaneously, there is no indirect effect through the mediator addiction and habits from online organisational awareness to any of the defined categories of OSN Apps.

The regression analysis reveals that irrespective of the levels of positive reinforcement of online organisational awareness regarding ethical reasoning through adhering to the online culture, standards, or rules for decision-making within the organisation, there is still a tendency toward a positive intent in exercising online security when engaging with OSNs. In the case of organisational awareness, online security behaviour shows the highest mediating effect toward the frequency of use of social apps. This is followed by top 10 apps, dual apps, and business apps.

These findings may be in contrast to the perceptions and views from the findings of the qualitative study. On the surface, perceptions of management from the qualitative study felt that organisational awareness driven by the employee’s professionalism and the organisation’s culture and value system goes a long way in mitigating irresponsible use of OSN platforms. From the qualitative analysis however, these perceptions lean towards the core theme of behavioural intent awareness similar to the intention toward online security behaviour in the quantitative findings.

This may be due to blurring the online boundary between management and employee. A co-worker who is part of the management structure of the organisation may be included as part of social chat group by an employee on an OSN platform. This may confuse the boundaries between both work and non-work time and social politics in the workplace. In addition, the profile of on the OSN may disclose personal information beyond that required for business interaction. The blur between social and work interaction may result in organisational awareness being a less effective driver toward responsible OSN behaviour. This may account for the contrast in perception gathered from the qualitative study where executive management feel that organisational culture should be a driver for responsible OSN engagement in contrast to that of the actual behaviour from gathered from the employee in the quantitative study.

As echoed from the findings of the qualitative study, driving and developing a strong company ethos and culture through an awareness to promote intent toward online security behaviour which in turn promotes responsible use of OSN platforms, cannot be underestimated which address objective six.

5.3.4 *Behavioural Intent Awareness*

The quantitative study gauges how the employees' self-reported experience levels of the defined constructs, online self-awareness, online privacy literacy and organisational awareness influence responsible OSN engagement. The literature review revealed extensive research on psychological and behavioural elements associated with the derived constructs, such as OSN addiction, engagement habits and the intention to adhere to security and privacy when engaging with OSNs. Using existing and adapted scales enables not only gauging the constructs but possible relation to the self-reported effects of psychological and behavioural elements acting as mediators to the resultant levels of responsible OSN engagement in the workplace.

Self-reported self-awareness regarding levels of self-esteem and online and cyber self-efficacy is mediated by behavioural intention towards online security and caution toward addiction, and bad habits can be associated with the employees' attitude to responsible engagement.

The higher the self-reported levels of online privacy literature, the higher the association of frequency of usage of business-orientated OSN platforms. This is further reinforced through the mediation of behavioural intention towards online security and caution toward addiction and bad habits and can be likened to the behaviour of perceived control of excising secured and safe OSN engagement.

Self-reported levels of organisational awareness reinforced through the mediation of behavioural intention towards online security can be likened to being aware and understanding the subjective norm towards engaging in OSNs within the organisation’s values and culture.

The nature of communication within the industries used in this study, namely, the financial services and health sector, does not likely lend itself to formal communication through social apps. It should also be noted that users with a higher tendency to use social apps are predisposed to suffer from OSN addiction and bad texting habits (Kircaburun and Griffiths, 2018; D’Arienzo, Boursier and Griffiths, 2019). These results imply that as a parallel mediating effect when employees engage with OSNs socially, there is a positive tendency of higher behavioural intent toward online security while simultaneously greater vigilance against OSN addiction and bad texting habits leading to more responsible OSN engagement. The mediation process is defined as an intervention between the endogenous and exogenous variables and results in the initial exogenous variables no longer necessarily affecting the outcome of responsible OSN engagement. This emphasises that notwithstanding the self-reported levels of online privacy literacy, online self-awareness and organisational awareness, the need for positive behavioural intent in exercising high levels of online security and behavioural vigilance against addiction and texting habits as fundamental to responsible OSN engagement.

As discussed in the qualitative findings, one could associate behavioural intent awareness to the Fishbein-Ajzen theory of planned behaviour ((Fishbein and Ajzen, 1975; Christian *et al.*, 2019)). However, this would require a research study specifically geared to the theory of planned behaviour.

Quantifying the constructs derived in this study, towards responsible use of OSN platforms satisfy objective four, five and six leading towards objective seven of the development a conceptual governance framework for responsible engagement on OSNs.

5.4 A GOVERNANCE FRAMEWORK FOR RESPONSIBLE OSN ENGAGEMENT

OSNs, if not already, are becoming a standard in business, business-to-consumer and consumer-to-consumer communications. From the study, it is clear that the assumption that the notion of “Loss or Lack of Control” makes OSN engagement impossible to control is no longer a satisfactory attitude in any of today’s organisations. OSN governance framework, or the Social Media governance framework, is a toolbox of policies, procedures and practices that are key to the arsenal protecting the organisation’s assets, mitigating and minimizing risks and maintaining compliance. It is essential that this governance continually evolves and has room to evolve organically from within the OSN ecosystem that connects all organisation stakeholders.

The ongoing development of a solid OSN engagement governance framework requires a risk management plan that addresses the prevention and mitigation of irresponsible OSN engagement, which should guide the behavioural intent of employees when engaging on OSN platforms. In addition, the governance framework must have clear set boundaries based on the organisation’s values and culture, cultural norms, gender equality, human rights violations and industry standards that, if breached, can be dealt with promptly and definitively.

Like with all governance frameworks, success is defined not only through an endorsed mandate from the organisation’s board and executive management but an ongoing buy-in and commitment by all employees and other stakeholders.

5.4.1 *Scope of the governance framework*

Social media governance frameworks within the modern-day organisation encompass governance and compliance that covers the web and social media presence regarding the organisation’s promotion and marketing, sales strategy and customer feedback process. However, the scope of this research study is concerned and focuses on employee OSN engagement. Thus, it is prudent to restrict the governance framework to the responsible use of OSN engagement by executive management, employees and other stakeholders bound to the organisation’s governance and compliance policies. The governance framework will apply using OSN in both a personal capacity and in representing the organisation.

An OSN governance consists of the organisation's policies, procedures and tools to mitigate risks and ensure that compliance is maintained. An OSN governance framework should provide a structure for aligning digital media strategy with the organisation's business strategy.

The nature of OSN platforms has given rise to an evolution of an organic non-centralized way OSN platforms are used and controlled. For governance to be effective, it needs to be developed as an enterprise-wide framework to maintain the organisation’s web and mobile-based employees, customers and other stakeholders. In addition, the governance framework needs timeous scheduled reviews and updates to account for the fast-evolving nature of OSN platforms.

Some organisations may have a shared governance framework across internal and external employees and stakeholders.

The governance framework should stipulate the approved processes to engage on OSNs. Rules regarding the approval of official OSN profiles and official chat groups for internal and external employees and other stakeholders must be laid out. The responsibilities of group administrators should be stipulated and acknowledged by the administrators.

A governance framework must include how OSN accounts that are fully or partly representative of the organisation clearly state the intention, purpose, target audience, and security and privacy settings. In addition, a continuity strategy should be implemented to transfer an account to a new owner. This will ensure that any popular OSN account on platforms such as Twitter, YouTube, Facebook, LinkedIn or Instagram will not be compromised or locked out should the person representing the organisation through such an account left.

A formal framework ensures the organisation provides guidance of regulated behaviour that reflects and is endorsed by its corporate culture. Such a formal programme aims to protect and take every stakeholder's interests into account, considering the needs of an employee with the processes for responsible, ethical and profitable engagement they should follow. In today's organisation, OSN governance is integral to both internal and external communication culture and forms part of the governance in the overall way of doing business. This includes social discussion groups and forums from outside organisations, clubs, committees, and social groups the employee as a company representative may be involved in their private capacity.

In contrast to the organisation trying to police its employees, placing the appropriate resources in training and awareness of company values, together with branding guidelines embedded in a well-balanced robust governance framework, will instead empower employees to not only engage responsibly on OSN platforms but will successfully promote the organisation's brand and ethos.

Adherence to this governance framework through training and corporate culture will ensure that each employee or stakeholder of the organisation will understand the risks of negligent and irresponsible behaviour as a point-of-presence representing the organisation as a stakeholder and in their private capacity when engaging with OSN platforms. This will maintain the organisation's corporate reputation promoting the corporate brand while mitigating reputational damage. It will also promote accountability, effectiveness and efficiency levels and encourage positive behaviour ensuring internal control.

Specifically, and most importantly, it is likely to improve the performance of the origination while reducing the risks, particularly the notion of radical transparency.

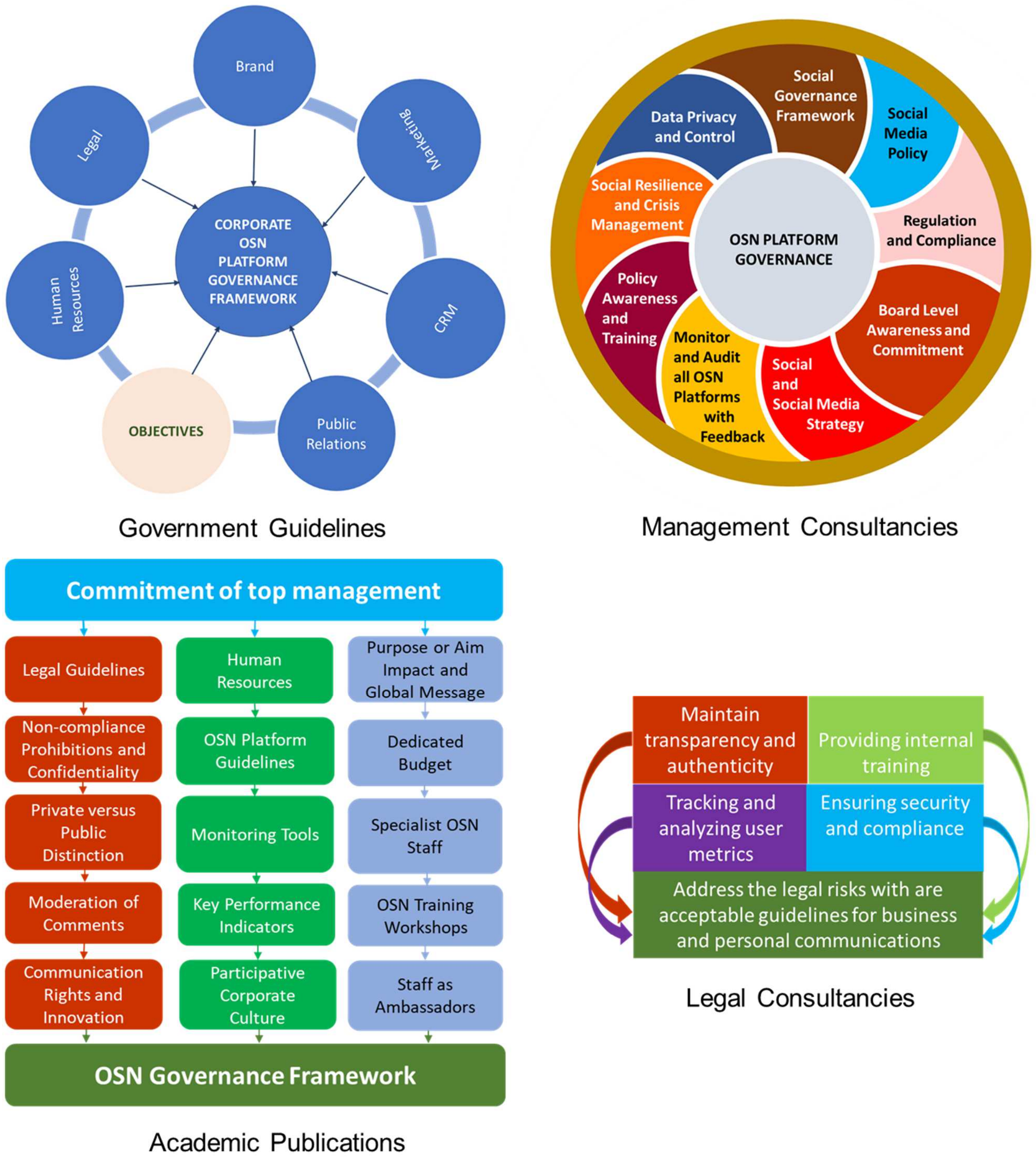
5.4.1.1 Current Recommended Governance Frameworks

Limited academic publications on OSN or social media governance frameworks led the researcher to supplement recommended frameworks by legal or management consultancies and government guidelines (Schmitz, Boothroyd and Garland, 2012; Linke and Zerfass, 2013b; Mennie and Smith, 2013; Strachan, 2015; Whitler, 2017; Athianos and Kydros, 2018; Anant *et al.*, 2020; Martinez, 2020; Paliwal, 2022).

Common Consideration in Recommended Governance Frameworks

An analysis of recommended governance frameworks from academic publications from 2013 to 2022, legal consultancies, management consultancies and government guidelines revealed the following components as part of an OSN governance framework:

1. Internal training and awareness
2. Governance policy and guidelines
3. Monitoring and assessing
4. Customer engagement guidelines
5. Brand awareness and guidelines
6. Marketing and sales channels
7. Transparency
8. Crisis management
9. Data privacy regulation
10. Security regulation and compliance


Brand
Marketing
CRM
Public Relations
OBJECTIVES
Human Resources
Legal
CORPORATE OSN PLATFORM GOVERNANCE FRAMEWORK
Social Governance Framework
Social Media Policy
Regulation and Compliance
Board Level Awareness and Commitment
Social and Social Media Strategy
Monitor and Audit all OSN Platforms with Feedback
Policy Awareness and Training
Social Resilience and Crisis Management
Data Privacy and Control
OSN PLATFORM GOVERNANCE
Commitment of top management
Legal Guidelines
Non-compliance Prohibitions and Confidentiality
Private versus Public Distinction
Moderation of Comments
Communication Rights and Innovation
Human Resources
OSN Platform Guidelines
Monitoring Tools
Key Performance Indicators
Participative Corporate Culture
Purpose or Aim Impact and Global Message
Dedicated Budget
Specialist OSN Staff
OSN Training Workshops
Staff as Ambassadors
OSN Governance Framework
Maintain transparency and authenticity
Providing internal training
Tracking and analyzing user metrics
Ensuring security and compliance
Address the legal risks with are acceptable guidelines for business and personal communications

Government Guidelines

Management Consultancies

Academic Publications

Legal Consultancies

Figure 5.1 Current Frameworks based on academic publications, legal consultancies, management consultancies and government guidelines.

5.4.1.2 Introducing Responsible Behavioural Intent

The results of this research study introduce the notion of behavioural intent when engaging with OSN platforms. This behavioural intent is moderated through online self-awareness, online privacy and security and an online ethos and culture. This behavioural intent further considers the risk mitigation toward an awareness of OSN addiction and texting habits.

5.4.2 *Governance Framework Foundation*

A formal governance framework should address the influencing factors explored and defined in the literature review that were investigated, observed and analysed in quantitative and qualitative findings to lay a foundation toward responsible behavioural intent, mitigating reputational risk promoting responsible OSN engagement, namely:

- Online self-awareness.
- Online privacy and security.
- Online ethos and culture.

More importantly, however, a key finding from the quantitative and qualitative findings stresses that a governance framework must first and simultaneously promote a conscientious behavioural intent toward online security while guarding against OSN addiction and lousy texting habits.

Common to the three factors is the need for training and awareness toward elements highlighted in the findings specific to each to promote responsible behavioural intent toward online security limiting while mitigating reputational risk or damage for both the employee and the organisation. In addition, as part of a governance framework, disciplinary consequences must be put in place for any violations of policies.

5.4.2.1 Personal Online Self-Awareness Behaviour

OSN platforms are a key part of the digital and fourth industrial revolution making it critical to adequately train employees about the risks and consequences of OSN engagement. Employees should feel empowered to engage within the organisation’s guidelines.

OSN engagement comes down to the behavioural intent of the individual pressing the send button when messaging or posting—it is knowing that the content is appropriate within the context of the subject matter, and its recipients depend on the employee’s confidence in their online self-awareness. Pausing for a conscious risk assessment before executing the send button depends on the employee’s self-empowered intention. Risk mitigation is thus dependent on the employee’s belief that the content of the message or post is responsible, appropriate and representative of the organisation and will not lead to reputational damage.

The fine and often blurred line between private and social interdependence makes it infeasible to mitigate risk through complete prohibition by postulating clearly defined policies.

Responsible behavioural intent when engaging with OSNs is critical in mitigating risk. A robust governance framework that empowers employees through well-supported resources, training and awareness will not need policing but rather enforce a company culture of responsible behavioural intent engaging with OSNs. Furthermore, the ubiquitous nature of communicating through OSN platforms enables employees with well-supported guidelines to act as brand ambassadors in both business and private engagement.

5.4.2.2 Online Privacy and Security Settings

Smart mobile devices are personal, and, as discussed in the literature review, the findings can be regarded as an extension of our persona regarding communication and information exchange with others. Understanding the dangers of breaches through weak privacy and security settings, ignorant or careless behaviour and a lack of vigilance cannot be over-emphasised. The findings, in particular from the quantitative study, show the importance of a vigilant behavioural attitude toward online security and privacy and an awareness of the dangers of OSN addiction and careless behaviour more than the need for detailed expertise in the privacy and security settings of any specific OSN platform. It should be noted that encouraging competent online privacy and security literacy and alerting employees to signs and specific indicators of addiction and lousy texting habits lays a foundation for promoting vigilant behaviour and awareness and should form a vital part of any OSN governance framework. This means there should be a policy of training and awareness in the organisations’ induction programmes. This should be followed up with regular workshops revising privacy and security settings while highlighting new security trends and concerns.

A governance framework requires well-defined online security and privacy policies that include but are not limited to strong passwords, regularly changing or varying passwords and an awareness of possible information disclosure. There should be strict and well-defined rules when administrating and governing chat groups. Awareness of the need for antivirus, firewall and related software is critical. A policy of regular communication as a reminder of privacy and security vigilance in the form of emails will significantly benefit. The availability of assisted support from the IT and social media departments is critical. Outsourcing online security and privacy to a specialist consultancy should not be underestimated.

It must be noted that a well-defined set of policies and processes will go a long way in mitigating security and privacy risks; however, it is not infallible. A set of processes should be put in place should there be a security and privacy breach to limit further and mitigate reputational or legal damage.

5.4.2.3 Online Ethos and Culture

The nuances of conversation and information exchange are personal in nature. Again, the employee's behavioural intent is key to maintaining the organisation's ethos and culture when communicating through OSN platforms. Employees should always be careful when posting on OSN platforms. Having reasonable guidelines about what employees should or should not post is an essential part of the governance framework; however, the intent of the employee to mimic the organisation's ethos and culture when engaging on OSN platforms rather than specific guidelines should be encouraged. Whilst the organisation cannot restrict what may be posted, employees are expected to adhere to the organisation's confidentiality policies at all times. Employees should be encouraged to avoid engaging in conversation on subjects they have little expertise in.

As part of compliance and regulation, formal rules of conduct when engaging with OSNs must be defined and adhered to. These should include the rule that no defamatory or derogatory exchanges directed towards other employees or stakeholders should be permitted at all times. As a policy, all employees should note and acknowledge that all OSN communication is recorded and thus can be used to incriminate both the employee and/or the organisation. As a policy, an organisational culture of courteous, respectful conversation should be encouraged at all times. Any form of hate speech or discriminatory comments, even in jest, cannot be tolerated. Fake news or misrepresentative, confusing and ambiguous content should be corrected and removed immediately.

Strict guidelines separating public, company and private account profiles should be defined. In addition, the scope and responsibilities for all official OSN profiles should be defined. When using a private personal profile, it may be necessary to use a disclaimer stating that your personal opinions and content are your own and may not be aligned with the company. This will avoid confusion or misunderstanding.

As part of the company culture, there should be an awareness of timeous responses to customers and other stakeholders. Employees should be constantly aware that prompt acknowledgement and dialogue are expected from customers. Employees must be aware that turning a blind eye to comments or blocking customers without reason may cause reputational harm to the employee and the organisation.

A policy for the control and handover of corporate assets and branding when business relationships change or are terminated. Such a policy must cater for a change in the association of account profiles when employees resign or when new stakeholders such as suppliers or outsourced agents are appointed.

5.4.2.4 Disciplinary Consequences

An OSN governance framework is of no value if there are no consequences when not followed. Should employees not follow policy guidelines, disciplinary action must be taken. This may result in and including dismissal. Examples of possible violations are:

- Sending or including company information to inappropriate recipients.
- Disclosing both private and organisational confidential information through personal or corporate accounts profiles.
- Posting violent, vulgar or sexually explicit media or comments in the organisation’s online community.
- Offensive and/or inappropriate media or comments directed towards other employees or stakeholders of the organisation’s online community.

Violating any governance framework policy inadvertently should result in reprimand. Repeated violations should lead to further disciplinary action that may result in organisational dismissal.

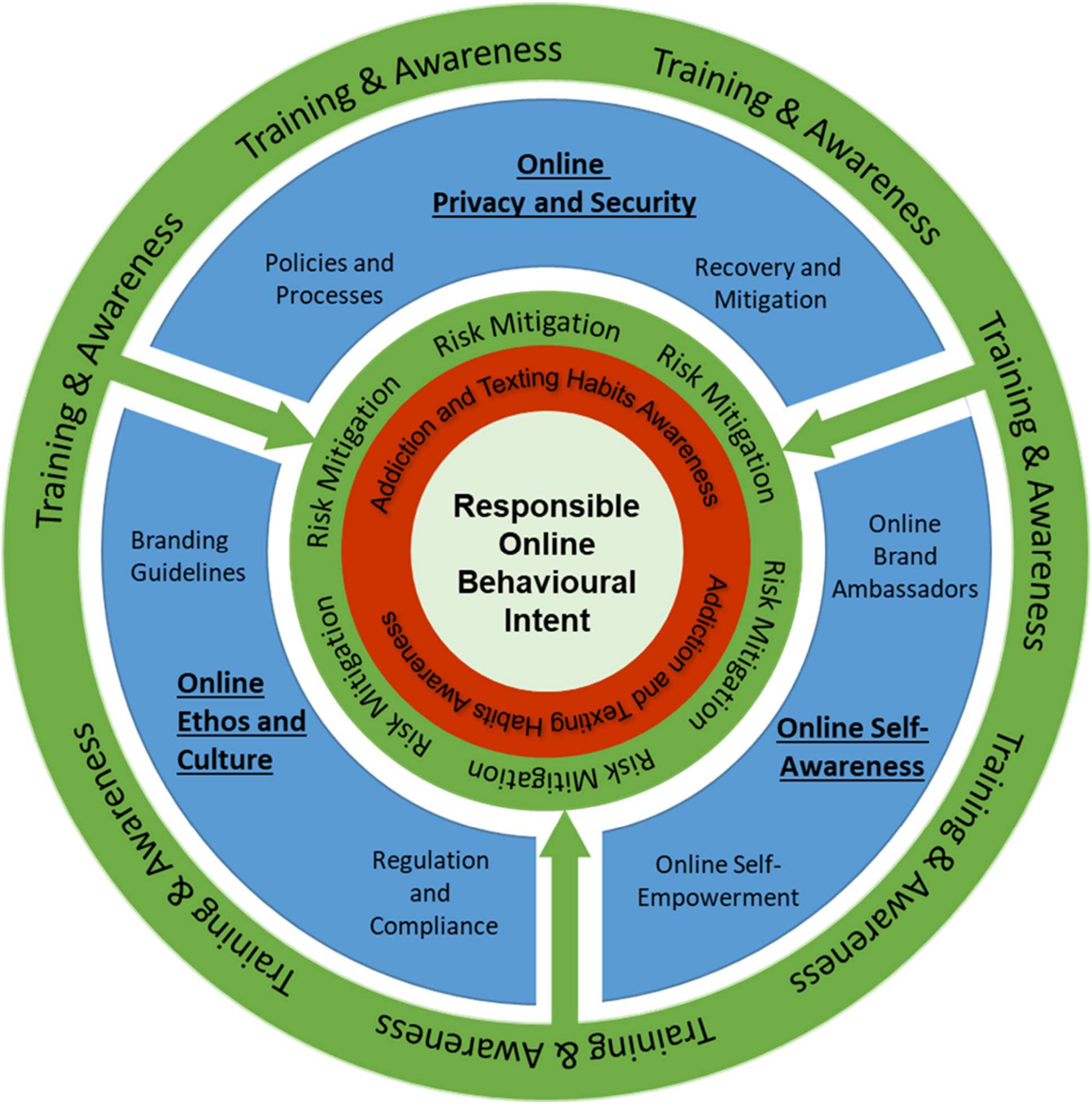


Figure 5.1. A typical governance framework for OSN engagement.

5.4.2.5 A Typical Governance Framework

Figure 5.1 represents the themes from the findings discussed that should form part of an OSN governance framework. As depicted, training and awareness form the outer shell of the framework. As discussed, a fundamental part of training and awareness behaviour toward risk mitigation is promoting conscientious behavioural intent toward online security while guarding against OSN addiction and bad texting habits, which form the framework's centre and heart. The key influencing factors that form the foundation of this study with their associated policies and aims are embodied by continuous training and awareness. Observing clearly defined policies will promote an organisational culture of maintaining strict security and privacy settings and behaviour, adherence to organisational regulation and compliance, and branding guidelines promoting an online ethos and culture that will empower the employee to engage online, representing the organisation with responsible behavioural intent mitigating reputational risk.

5.5 CONCLUSION

Reviewing the literature to identify factors influencing responsible OSN engagement meets objective one. Assessing the levels of influence of the identified factors, namely, online privacy literacy, online self-awareness and online organisational awareness towards responsible OSN engagement meets objectives four, five and six respectively.

In meeting the objectives, the research findings from the organisations investigated show that, despite the perceptions of loss or lack of control identified in the academic literature, positive levels and attitudes towards the identified influencing factors are associated with positive responsible behavioural intention when engaging with OSNs. The qualitative and quantitative findings from the selected industries show that OSNs are used primarily as a business tool with limited social use.

From the discussions in the qualitative findings, senior management and executives emphasise an awareness of the employee’s professionalism and that of the organisation’s culture and values when promoting responsible OSN engagement. The key theme from the perceptions of senior management and executives is that responsible OSN engagement is driven by the positive behavioural intent of the employee. The conclusions from the analysis of the opinions and perceptions from senior management are supported by the quantitative findings in that the contributing factor associated with responsible OSN engagement, that being positive behavioural intent to exercise online security and privacy and to be vigilant about the perils of OSN addiction. This is irrespective of the association of positive levels from the observable variables of online self-awareness, online privacy literacy and online organisational awareness to responsible engagement that were identified in the literature. This is a key contribution from this study to the body of knowledge.

From the governance frameworks researched, none approach risk mitigation with the full consideration of the influencing factors identified in this study that are associated responsible behaviour. The framework promotes training and awareness of the employee's self-concept tied to the online ethos and culture of the organisation. Part of the purpose of this study was to develop a governance framework further contributes to the body of knowledge. purposeful convenience

In addition, the quantitative research revealed that there are competent levels of online privacy, positive levels of online security behavioural intentions, and low OSN addiction and dangerous texting habits. Nevertheless, the qualitative findings warn of the exposure to organisational reputational risk arising from deliberate or accidental irresponsible behaviour when engaging on OSN platforms that may be subject to:

1. Asymmetrical information on the dangers of OSN usage is being nudged by OSN platform providers through adverse selection using the human instinct to seize instant gratification and social acceptance to gain marketing and strategic information.
2. Impulsive, unintended, inattentive or negligent behaviour and habits.
3. Decontextualised misinformation through a reduction in social cues

The problem of organisational reputational risk of susceptibility to misdirected behaviour is by no means new; however, this problem may be exacerbated by the adverse effects of radical transparency arising from the proliferation of OSN platforms. In meeting objective seven, this study draws both the qualitative and quantitative findings of factors promoting behavioural intent towards responsible OSN engagement through developing a governance framework to mitigate the reputational risk and damage of this vulnerability.

5.6 RECOMMENDATIONS

5.6.1 *Theoretical Implications*

Employee self-efficacy and self-esteem are not widely addressed in today’s business environment. Although the likelihood of grave reputational damage through irresponsible negligent engagement is low, there have been enough incidents in the recent past to illicit concern. The research shows that an employee's low online self-awareness may leave the organisation vulnerable to irresponsible OSN usage through elements such as OSN addiction and negligent texting habits. Furthermore, the nature of radical transparency going awry renders the susceptibility of low levels of online self-awareness regarding self-efficacy and self-esteem a problem that, before the advent of OSN platforms, was not apparent in the business environment. As a recommendation to the future organisation, it is suggested that corporate initiatives to identify and help address low self-esteem may reduce the risk of irresponsible OSN engagement through increased self-confidence, which may help negate unintended negligence.

Even though a high level of online privacy literacy competency is desirable in all organisations, employees generally are expected to develop a level of online privacy literacy competency through self-education. This may be attributed to OSN usage's fast-moving landscape and the associated skills and knowledge required to protect employees from compromising their personal and organisational data. However, this is an area where malicious intent by a third party can prey on a lack of awareness and the misguided trust or false sense of security of personal and organisational data in the personal profile of a user’s OSN profile. The knowledge and trust of who has access to and owns the data residing and shared from within a personal OSN profile have become not only a controversial but a serious issue in recent years. This is typified by Facebook's expecting to pay up $5 (US) billion in fines to the Federal Trade Commission in the US for violating the privacy consent decree in 2011. This is one example, as the infamous Cambridge Analytica data breach scandal exposed 50 million users' personal information (Isaak and Hanna, 2018; Isaac and Kang, 2019).

5.6.2 *Practitioner Implications*

The research shows that a positive behavioural intent toward online privacy in security goes a long way toward responsible OSN engagement. However, there are times when the user's misguided trust and a false sense of security in OSN platforms when sharing confidential information can lead to unwanted data breaches and possible severe reputational damage. The research shows that the higher levels of an employee's online privacy literacy and awareness may be crucial in averting privacy and security breaches during OSN engagement. As a recommendation to the future organisation, corporate initiatives to identify and consistently promote awareness while skilling up on online privacy levels about OSN engagement may reduce the unintended risk of having personal and organisational data compromised. Promoting positive intent toward online security behaviour is key to high levels of online privacy literacy competency

5.6.3 *Policy Implications*

Developing a governance framework that drives a strong company ethos and culture to promote positive intent toward online security behaviour will promote the responsible use of OSN platforms. The typical governance framework for OSN engagement presented in section 5.4.2.5, page 303 can be used as a basis for future frameworks.

There was a unanimous call from all interviewees for more organisational awareness regarding training and education on the appropriate safe use of OSN platforms. They emphatically suggested a module in the induction programme for new employees and for continuing education programmes for existing employees. Reoccurring key themes from an organisational perspective that need to be addressed are:

1. Revising and enforcing the ever-evolving do's and don'ts of OSN engagement.
2. Promote organisational values and conduct.
3. Understand that freedom of expression as a right comes with responsibilities.
4. The notion of "What happens in Vegas stays in Vegas" no longer applies in today's world of OSNs.

From an organisational awareness perspective instilling company values through leadership and training, it is believed, will go a long way in promoting responsible OSN engagement. It is imperative, however, for the employee to be fully aware of the consequence of not abiding by the organisation's OSN engagement values, culture, governance, policies and procedures.

5.7 FUTURE RESEARCH

Developing online self-awareness as a construct by combining the used scales, online self-efficacy and self-esteem for measuring responsible OSN engagement require further research and validation.

The Online Self-Efficacy (OSES) adapted based on the Scales for the General Self-Efficacy Scale (GSE) (Schwarzer and Jerusalem, 2013) and the unpublished Cybersecurity Engagement and Self-Efficacy Scale (CESES) (Amo, L., Zhuo, Wilde, Murray, Cleary, Upadhyaya, 2016). OSES as a scale showed a Cronbach α =.870 for reliability and consistency with an inter-item correlation mean of .405. However, this scale needs to be further validated and can be used to test the self-efficacy of online security regarding data privacy protection and against any unknown malware or a virus.

The online privacy literacy construct used in this research was adapted for the South African POPI act and adjusted for the evolving data privacy technologies from the online privacy literacy scale (OPLIS) (Trepte *et al.*, 2015). However, the researcher believes there is scope for further validation and improvement of the South African version of the scale.

A further recommendation is to explore the relationship between online privacy awareness and online behaviour regarding security intent, habits and addiction. In the engagement of OSNs, habits and addiction influence attitudes and behaviour toward online security.

In determining the ethical climate of an organisation, Victor and Cullen's ECQ (Victor and Cullen, 1988) remains a landmark instrument. With the advent of OSN platforms, both an individual's and an organisation's rights to privacy are of paramount ethical importance. To this end, the researcher introduced three additional questions to the 26-item ECQ. From a research perspective, the ethical awareness of data privacy needs to be further validated and explored.

To explore the findings in both the qualitative and quantitative study of behavioural intention awareness in responsible OSN engagement to the Fishbein-Ajzen behavioural intentions model and the theory of planned behaviour (Fishbein and Ajzen, 1975; Christian et al., 2019).

Influencing factors in the responsible engagement of OSNs such as, ease of use, accessibility to OSN platforms, the perceived need to engage and the attitude toward the use of OSNs, should be considered when conducting future research.

The effect the dynamic rapidly evolving landscape of OSNs toward responsible engagement is suggested for future research.

Further recommendations for future research is to consider using a similar research approach in industries outside of the financial and health services sectors.

The governance framework proposed in this research could be evaluated using a case study within a few organisations. Furthermore, comparisons of the effectiveness of the framework in different industries may be considered.

The use of OSNs in organisations is an evolving and constantly changing process. This prompts research on the effect the covid-19 pandemic may have on the use and behaviour engaging with OSN platforms.

5.8 LIMITATIONS OF THIS RESEARCH

This research is subject to the following key limitations.

5.8.1 *Influencing Factors*

In order to investigate the behaviour of OSNs platform usage and its impact, not all factors were included in the study. In a broader context, there may be other antecedents and impact factors such as ease of use, accessibility, perceived need to engage and attitude toward use. Therefore, the inclusion of only the factors in the considered in the study may be a limitation.

5.8.2 *The Selection of OSN platforms*

The concentration on only the top social media and OSN platforms can also be considered a limitation, although the results from web statistics and the literature review show that the top 10 platforms are the most relevant to a behaviour analysis in OSN platform engagement.

5.8.3 *The Rapidly Evolving Landscape of OSN platforms*

The dynamic of OSNs are rapidly and consistently evolving and changing. OSN platforms are acquired and relaunched with new functionality. This study is concerned in responsible engagement on OSNs regardless of the OSN platform however the evolving dynamic of the OSN platform industry may be a limitation to the data gathered at the time this study was conducted.

5.8.4 *Sample Bias*

Although sufficient data regarding respondents for meaningful analysis was collected, the researcher is cognizant that the data may not have some bias for the following reason.

The study delves into the stealth invasion of personal data privacy through a lack of online privacy literacy and the behaviour whilst engaging OSNs. Asking potential survey respondents to answer questions related to the competency of their online privacy literacy and behaviour engaging with OSNs may leave them with the suspicion that their organisation may be spying on them even though all attempts were made to assure them that their responses remain anonymous. This possible suspicion or distrust is directly related to the recent exposure of some of the major organisation's OSNs that have given the registered user an impression of a false sense of comfort that their personal data are secured through default privacy settings in the terms and conditions when registering with the OSN.

5.8.5 *Self-report method Social Desirability Bias*

Additionally, in the quantitative study using the self-report method through the online survey may limit the validity of the data because of social desirability bias. This may be particularly relevant on self-report for accuracy in time and effort reading security policies and procedures for various services. Time and effort spent reading these policies may be inflated by the social desirability to indicate higher security and governance vigilance.

5.8.6 *Limited Participation from Industry*

There has been recent activity and hype of the wave of online data leaks and security breaches in an attempt to bring large organisations into disrepute, initiated by organisations such as WikiLeaks. In addition, local incidents of the politically incorrect faux pas threatening reputational damage to associated organisations from OSN posts have cautioned many organisations against any external online activity. This was apparent when having gone through a rigorous process to obtain ethical clearance for research participation from a large financial organisation which was endorsed by the Chief Operating Officer of the organisation. However, it was immediately vetoed by the human resources department, deemed “too dangerous.”

The convenience sample represents participants for the qualitative and quantitative study recruited only from the selected organizations willing to participate in the study. The representativeness of the sample is limited.

5.8.7 *Limitation of Industry Sectors Selected*

The study restricted the selection of organisations from sectors that adhere to the benchmark of professional standards and norms concerning business transparency, privacy and confidentiality. The study is not concerned with the disparate business functions of these sectors and it is believed that the stringent benchmark in privacy and confidentiality can carry through to other sectors.

5.8.8 *Qualitative Research*

5.8.8.1 Access Bias

The qualitative research was extensive 29 interviews comprising 25 hours of used recordings. Although it was felt that the research topic was well-saturated, it must be noted that the researcher had limited influence on the selection of demographic representation and was restricted to senior management willing to afford the time for an interview.

As senior management in the financial services and healthcare industry, 22 of the 29 interviewees fell into the X-Generation category, 4 were Millennials, and 3 were Baby Boomers. From a gender perspective, 9 out of the 29 interviewees were female, and 14 out of the 29 were classified as white males. Although the sample is representative of the current senior management from the two industries researched, the researcher would have liked to have had access to a slightly more balanced representation regarding generation, gender and race.

5.8.8.2 Time Constraints

After an exhaustive analysis of the interviews, the researcher would have liked to have had the time to do some follow-up interviews. However, this and the extensive quantitative research would have extended the study beyond its scope regarding time. In addition, a request for a second interview with most interviewees would likely be unsuccessful.

5.8.8.3 Geographical sample representation

From a budget perspective regarding cost and time, the qualitative sample was restricted to the Gauteng and KwaZulu-Natal regions of South Africa. The Free Sate, North, Eastern and Western Cape provinces were not considered, thus possibly limiting general South African representation.

5.9 DELIMITATIONS AND ASSUMPTIONS OF THIS RESEARCH

The delimitations and assumptions related to this study are discussed in the following sections.

The following are the study's delimitations concerning the theory context, constructs

1. The evolving nature of the subject matter, namely, the responsible usage of OSNs and business transparency, is in a state of rapid technological and social evolution. Therefore, the literature review is limited to current information within the last three years from data collection of the qualitative and quantitative findings. The literature from related topics like the effect of social capital from OSN usage, behavioural science, and the health effects of OSN usage was only reviewed and discussed in passing.
2. All participation in the quantitative research was voluntary and may have been subject the distribution at the discretion of the management of the organisation.
3. Various statistical methods and techniques can be considered to develop and

derive underlying factors or components within the constructs proposed. For example, the researcher used Principal Component Analysis and Varimax extraction.

4. Very little was found for a standard measurement for responsible OSN usage.
5. Data was gathered using an online questionnaire to determine constructs as a measure of responsible OSN usage. However, the researcher acknowledges that other questions or methods may not be considered a measure of responsible OSN usage.
6. Whilst data gathered on the moderating factors, industry, gender, generation and qualification were explored in the literature review, they did the part of primary focus in evaluating the study's proposed objectives. They were thus not fully statistically gauged as moderators.

5.9.1 *Assumptions*

Assumptions of the research study are:

- The frequency usage of OSN engagement can measure responsible OSN engagement.
- Participants in the online survey engage in the use of OSNs.

REFERENCES

A Big Brother Watch report (2015) *Careless Whispers: How speech is policed by outdated communications legislation*.

Abadiga, M. *et al.* (2019) ‘Relationship between nurses’ perception of ethical climates and job satisfaction in Jimma University Specialized Hospital, Oromia region, south west Ethiopia’, *BMC Nursing*, 18(1), pp. 1–10. Available at: https://doi.org/10.1186/s12912-019-0365-8.

Abdul Talib, Y.Y. and Mat Saat, R. (2017) ‘Social proof in social media shopping: An experimental design research’, *SHS Web of Conferences*, 34, p. 02005. Available at: https://doi.org/10.1051/shsconf/20173402005.

Acohido, B. (2010) *An invitation to crime : How a friendly click can compromise a company*, *USA Today*. Available at: http://phys.org/news/2010-03-crime-friendly-click-compromise-company.html (Accessed: 12 October 2016).

Acohido, B. and Swartz, J. (2008) ‘Botnet scams are exploding.pdf’, *USA TODAY*, 16 March, pp. 1B-2B. Available at: usatoday30.usatoday.com/money/industries/.../2008-03-16-computer-botnets_N.htm.

Agha, S. *et al.* (2019) ‘Use of the Fogg Behavior Model to Assess the Impact of a Social Marketing Campaign on Condom Use in Pakistan’, *Journal of Health Communication*, 24(3), pp. 284–292. Available at: https://doi.org/10.1080/10810730.2019.1597952.

Ahani, A. and Nilashi, M. (2020) ‘Coronavirus Outbreak and its Impacts on Global Economy : The Role of Social Network Sites’, *Journal of Soft Computing and Decision Support Systems*, 7(2), pp. 19–22.

Alemanno, A. (2012) ‘Nudging smokers: The behavioural turn of tobacco risk regulation’, *European Journal of Risk Regulation*, 3(1), pp. 32–42. Available at: https://doi.org/10.1017/S1867299X00001781.

Ali, S. *et al.* (2018) ‘Privacy and Security Issues in Online Social Networks’, *Future Internet*, 10(114), pp. 1–12. Available at: https://doi.org/10.3390/fi10120114.

AlKalbani, A., Deng, H. and Kam, B. (2015) ‘Organisational security culture and information security compliance for e-government development: The moderating effect of social pressure', *Pacific Asia Conference on Information Systems, PACIS 2015 - Proceedings* [Preprint].

Alkire, L., Pohlmann, J. and Barnett, W. (2019) 'Triggers and motivators of privacy protection behavior on Facebook', *Journal of Services Marketing*, 33(1), pp. 57–72. Available at: https://doi.org/10.1108/JSM-10-2018-0287.

Allodi, L. *et al.* (2020) 'The Need for New Antiphishing Measures against Spear-Phishing Attacks', *IEEE Security and Privacy*, 18(2), pp. 23–34. Available at: https://doi.org/10.1109/MSEC.2019.2940952.

Amo, L., Zhuo, Wilde, Murray, Cleary, Upadhyaya, and R. (2016) *Cybersecurity Engagement and Self-Efficacy Scale*.

Amo, L. (2016) 'Addressing Gender Gaps in Teens' Cybersecurity Engagement and Self-Efficacy', *IEEE Security & Privacy*, 14(1), pp. 72–75.

Anant, V. *et al.* (2020) *The consumer-data opportunity and the privacy imperative*, *McKinsey & Company*.

Anaraky, m R.G., Knijnenburg, B.P. and Risius, M. (2020) 'Exacerbating Mindless Compliance: The Danger of Justifications during Privacy Decision Making in the Context of Facebook Applications', *AIS Transactions on Human-Computer Interaction*, 12(2), pp. 70–95. Available at: https://doi.org/10.17705/1thci.00129.

Andersson, H. (2018) *Social media apps are 'deliberately' addictive to users*, *BBC News*. Available at: https://www.bbc.com/news/technology-44640959 (Accessed: 25 August 2020).

Andreassen, C.S. *et al.* (2013) 'The relationships between behavioral addictions and the five-factor model of personality', *Journal of Behavioral Addictions*, 2(2), pp. 90–99. Available at: https://doi.org/10.1556/jba.2.2013.003.

Andreassen, C.S. (2015) 'Online Social Network Site Addiction : A Comprehensive Review', *Curr Addict Rep*, pp. 175–184. Available at: https://doi.org/10.1007/s40429-015-0056-9.

Andreassen, C.S., Pallesen, S. and Grif, M.D. (2017) 'The relationship between addictive use of social media , narcissism , and self-esteem : Findings from a large national survey', *Addictive Behaviors*, 64, pp. 287–293. Available at: https://doi.org/10.1016/j.addbeh.2016.03.006.

Andreassen, C.S., Pallesen, S. and Griffiths, M.D. (2017) 'The relationship between addictive use of social media, narcissism, and self-esteem: Findings from a large national survey', *Addictive Behaviors*, 64(December), pp. 287–293. Available at: https://doi.org/10.1016/j.addbeh.2016.03.006.

Angelopoulos, S. *et al.* (2020) 'Stewardship of personal data on social networking sites', *International Journal of Information Management*, 56(July 2020), p. 102208. Available at: https://doi.org/10.1016/j.ijinfomgt.2020.102208.

Anstey Watkins, J.O.T. *et al.* (2018) 'Mobile phone use among patients and health workers to enhance primary healthcare: A qualitative study in rural South Africa', *Social Science and Medicine*, 198(January), pp. 139–147. Available at: https://doi.org/10.1016/j.socscimed.2018.01.011.

Aruguete, N. and Calvo, E. (2018) 'Time to #protest: Selective exposure, cascading activation, and framing in social media', *Journal of Communication*, 68(3), pp. 480–502. Available at: https://doi.org/10.1093/joc/jqy007.

Asongu, S.A. and Odhiambo, N.M. (2019) 'Governance and social media in African countries: An empirical investigation', *Telecommunications Policy*, 43(5), pp. 411–425. Available at: https://doi.org/10.1016/j.telpol.2018.10.004.

Athianos, S. and Kydros, D. (2018) 'Corporate governance and social networks: The relationship between the board of directors and earnings management', *Corporate Ownership and Control*, 15(3), pp. 80–91. Available at: https://doi.org/10.22495/cocv15i3art7.

Atroszko, P.A. *et al.* (2018) 'Facebook addiction among Polish undergraduate students: Validity of measurement and relationship with personality and well-being', *Computers in Human Behavior*, 85, pp. 329–338. Available at: https://doi.org/10.1016/j.chb.2018.04.001.

Attrill, A. (2016) 'The Role Of Culture In Online Behavi', in Attrill A and F. C (eds) *Applied Cyberpsychology*. London: Palgrave Macmillan UK, pp. 39–57. Available at: 10.1057/9781137517036_3.

Babbie, E., Wagner III, W.E. and Zaino, J. (2015) *Adventures in Social Research: Data Analysis Using IBM SPSS Statistics*. 9th edn. SAGE Publictions.

Babbie, E.R. (2014) *The Basics of Social Research, Sixth Edition*. Sixth. Wadsworth.

Bada, M., Sasse, A. and Nurse, J.R.C. (2019) 'Cyber Security Awareness Campaigns: Why They Fail to Change Behavior', (January), p. 38. Available at: http://discovery.ucl.ac.uk/1468954/1/Awareness CampaignsDraftWorkingPaper.pdf.

Bandsuch, M., Pate, L. and Thies, J. (2008) 'Rebuilding Stakeholder Trust in Business: An Examination of Principle-Centered Leadership and Organizational Transparency in Corporate Governance', *Business and Society Review*, 113(1), pp. 99–127.

Bandura, A. (1998) 'Self-efficacy', *Encyclopedia of human behavior*, 4(1994), pp. 1–65. Available at: https://doi.org/10.1002/9780470479216.corpsy0836.

Bányai, F. *et al.* (2017) 'Problematic social media use: Results from a large-scale nationally representative adolescent sample', *PLoS ONE*, 12(1), pp. 10–14. Available at: https://doi.org/10.1371/journal.pone.0169839.

Baraibar, D.E. (2013) *contextualization of transparency in integrating elements of corporate communications*, *Transparencia*.

Barry, A.E. *et al.* (2011) 'So you want to develop a survey: practical recommendations for scale development.', *American Journal of Health Studies*, 26(2), p. 359.

Barth, S. *et al.* (2019) 'Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources', *Telematics and Informatics*, 41(March 2019), pp. 55–69. Available at: https://doi.org/10.1016/j.tele.2019.03.003.

Barth, S. and de Jong, M.D.T. (2017) 'The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review', *Telematics and Informatics*, 34(7), pp. 1038–1058. Available at: https://doi.org/10.1016/j.tele.2017.04.013.

Bartsch, M. and Dienlin, T. (2016) 'Control your Facebook: An analysis of online privacy literacy', *Computers in Human Behavior*, 56, pp. 147–154. Available at: https://doi.org/10.1016/j.chb.2015.11.022.

Baumgartner, R. (2013) ‘Survey Design and Implementation Cross-Cutting Protocols for Estimating Gross Savings’, *National Renewable Energy Laboratory* [Preprint], (April).

BBC (2018) ‘India lynchings: WhatsApp sets new rules after mob killings - BBC News’, *BBC*, p. 1. Available at: https://www.bbc.com/news/world-asia-india-44897714.

Belgrave, L.L. and Seide, K. (2019) ‘Grounded theory methodology: Principles and practices’, *Handbook of Research Methods in Health Social Sciences*, pp. 299–316. Available at: https://doi.org/10.1007/978-981-10-5251-4_84.

Berezan, O. *et al.* (2018) ‘The pursuit of virtual happiness: Exploring the social media experience across generations’, *Journal of Business Research*, 89(June), pp. 455–461. Available at: https://doi.org/10.1016/j.jbusres.2017.11.038.

van den Berg, A. and Struwig, M. (2020) ‘Social Media Policies Within the Financial Sector in South Africa’, *SAGE Open*, 10(4). Available at: https://doi.org/10.1177/2158244020975030.

Berto, J. (2019) ‘Social Media, Open Platforms, and Democracy: Transparency Enabler, Slayer of Democracy, Both?’, *Proceedings of the 52nd Hawaii International Conference on System Sciences* [Preprint]. Available at: https://doi.org/10.24251/hicss.2019.942.

Bhattacharyya, S. and Bose, I. (2020) ‘S-commerce: Influence of Facebook likes on purchases and recommendations on a linked e-commerce site’, *Decision Support Systems*, 138(August), p. 113383. Available at: https://doi.org/10.1016/j.dss.2020.113383.

Birchall, C. (2014) ‘Radical Transparency?’, *Cultural Studies ↔ Critical Methodologies*, 14(1), pp. 77–88. Available at: https://doi.org/10.1177/1532708613517442.

Birkett, A. (2015) *Online Manipulation: All The Ways You’re Currently Being Deceived*, *conversionxl*. Available at: https://conversionxl.com/online-manipulation-all-the-ways-youre-currently-being-deceived/ (Accessed: 10 June 2017).

Bitter, S., Grabner-Kräuter, S. and Breitenecker, R.J. (2014) ‘Customer engagement behaviour in online social networks - The Facebook perspective’, *International Journal* *of Networking and Virtual Organisations*, 14(1–2), pp. 197–220. Available at: https://doi.org/10.1504/IJNVO.2014.065088.

Błachnio, A., Przepiorka, A. and Pantic, I. (2016) 'Association between Facebook addiction, self-esteem and life satisfaction: A cross-sectional study', *Computers in Human Behavior*, 55, pp. 701–705. Available at: https://doi.org/10.1016/j.chb.2015.10.026.

Blackwell, D. *et al.* (2017) 'Extraversion, neuroticism, attachment style and fear of missing out as predictors of social media use and addiction', *Personality and Individual Differences*, 116, pp. 69–72. Available at: https://doi.org/10.1016/j.paid.2017.04.039.

Blascovich, J. and Tomaka, J. (1991) *Measures of Self-Esteem*. Third Revi, *Measures of Personality and Social Psychological Attitudes*. Third Revi. Academic Press, Inc. Available at: https://doi.org/10.1016/b978-0-12-590241-0.50008-3.

Blome, C. and Paulraj, A. (2013) 'Ethical Climate and Purchasing Social Responsibility: A Benevolence Focus', *Journal of Business Ethics*, 116(3), pp. 567–585. Available at: https://doi.org/10.1007/s10551-012-1481-5.

Bolton, R.N. *et al.* (2013) 'Understanding Generation Y and their use of social media: a review and research Understanding Generation Y and their use of social media: a review and research agenda', *Journal of Service Management*, 24(3), pp. 245–267. Available at: https://doi.org/10.1108/09564231311326987.

Bolton, R.N., Parasuraman, A. and Hoefnagels, A. (2013) 'Understanding Generation Y and their use of social media : a review and research agenda This item was submitted to Loughborough ' s Institutional Repository (https://dspace.lboro.ac.uk/) by the author and is made available under', *Loughborough University Institutional Repository*, 24(3), pp. 245–267. Available at: https://dspace.lboro.ac.uk/dspace-jspui/bitstream/2134/13896/3/Understanding Generation Y and Their Use of Social Media_A Review and Research Agenda.pdf.

Boren, A. (2015) 'A Rhetorical Analysis of Black Mirror: Entertaining Reflections of Digital Technology's Darker Effects', *URJ-UCCS: Undergraduate Research Journal at UCCS*, 8(1), pp. 15–24. Available at: http://ojs.uccs.edu/index.php/urj/article/view/181.

Borrello, A. (2016) *The Shocking Truth About Tinder; It's More Than Just a Hook-Up*

App!, *The Huffington Post*. Available at: http://www.huffingtonpost.com/antonio-borrello-phd/the-shocking-truth-about-_7_b_8011462.html (Accessed: 4 June 2017).

Bosker, B. (2016) *The Binge Breaker*, *The Atlantic*. Available at: https://www.theatlantic.com/magazine/archive/2016/11/the-binge-breaker/501122/ (Accessed: 10 June 2017).

Bouadjenek, M.R., Hacid, H. and Bouzeghoub, M. (2016) ‘Social networks and information retrieval, how are they converging? A survey, a taxonomy and an analysis of social information retrieval approaches and platforms’, *Information Systems*, 56, pp. 1–18. Available at: https://doi.org/10.1016/j.is.2015.07.008.

Bouter, C., Venter, B. and Etheredge, H. (2020) ‘Guidelines for the use of WhatsApp groups in clinical settings in South Africa’, *South African Medical Journal*, 110(5), pp. 364–368. Available at: https://doi.org/10.7196/SAMJ.2020.v110i5.14558.

Boyd, D. (2015) ‘Social Media: A Phenomenon to be Analyzed’, *Social Media and Society*, 1(1). Available at: https://doi.org/10.1177/2056305115580148.

Boyd, D.M. and Ellison, N.B. (2007) ‘Social network sites: Definition, history, and scholarship’, *Journal of Computer-Mediated Communication*, 13(1), pp. 210–230.

Brady, W.J. *et al.* (2017) ‘Emotion shapes the diffusion of moralized content in social networks’, *Proceedings of the National Academy of Sciences of the United States of America*, 114(28), pp. 7313–7318. Available at: https://doi.org/10.1073/pnas.1618923114.

Bressler, M. and Bergen, C.W. Von (2023) ‘Sweat the Small Stuff, How Small Incidents of Negative Workplace Behavior Lead to Larger Misconduct’, *Journal of Organizational Psychology*, 23(1). Available at: https://doi.org/10.33423/jop.v23i1.5850.

Brewer, G. and Kerslake, J. (2015) ‘Cyberbullying, self-esteem, empathy and loneliness’, *Computers in Human Behavior*, 48, pp. 255–260. Available at: https://doi.org/10.1016/j.chb.2015.01.073.

Brown, B., Chui, M. and Manyika, J. (2011) ‘Are you ready for the era of “big data”? | McKinsey &amp; Company’, *McKinsey Quarterly*, 4, pp. 24–35. Available at: https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/are-you-ready-for-the-era-of-big-data.

Brown, E. *et al.* (2013) ‘Reciprocity: Understanding online social relations’, *First Monday*, pp. 1–13. Available at: https://doi.org/10.5210/fm.v17i10.3324.

Brown, I. and Marsden, C.T. (2023) *Regulating code: Good governance and better regulation in the information age.* MIT Press.

Browne, M.W. and Cudeck, R. (1992) ‘Alternative Ways of Assessing Model Fit’, *Sociological Methods & Research*, 21(2), pp. 230–258. Available at: https://doi.org/10.1177/0049124192021002005.

Browse Media (2017) *Messaging Apps vs. Social Media*, *Browse Media*. Available at: http://www.browsermedia.co.uk/2017/03/10/messaging-apps-vs-social-media/ (Accessed: 20 July 2017).

Bryant, A. and Charmaz, K. (2012) ‘Grounded theory and psychological research’, in *APA handbook of research methods in psychology*, pp. 39–56. Available at: https://doi.org/https://doi.org/10.1037/13620-003.

Burrow, A.L. and Rainone, N. (2017) ‘How many likes did I get?: Purpose moderates links between positive social media feedback and self-esteem.’, *Journal of Experimental Social Psychology*, 69, pp. 232–236. Available at: https://doi.org/10.1016/j.jesp.2016.09.005.

Busalim, A.H., Che Hussin, A.R. and Iahad, N.A. (2019) ‘Factors Influencing Customer Engagement in Social Commerce Websites: A Systematic Literature Review’, *Journal of theoretical and applied electronic commerce research*, 14(2), pp. 0–0. Available at: https://doi.org/10.4067/s0718-18762019000200102.

Business Insider (2016) *Messaging apps are now bigger than social networks*, *Business Insider*. Available at: http://www.businessinsider.com/the-messaging-app-report-2015-11 (Accessed: 20 July 2017).

Business Insider SA (2021) *South Africans are downloading Telegram like crazy – and Signal isn’t far behind*, *businessinsider.co.za*. Available at: https://www.businessinsider.co.za/telegram-is-topping-signal-as-a-whatsapp-replacement-in-sa-downloads-so-far-2021-1.

BusinessTech (2016) *Chris Hart reveals why he quit Standard Bank*, *BusinessTech*. Available at: https://businesstech.co.za/news/business/116910/why-christ-hart-quit-standard-bank/ (Accessed: 14 July 2017).

Byrne, B.M. (2010) *Multivariate applications series. Structural equation modeling with AMOS: Basic concepts, applications, and programming*. 2nd edn. New York: Routledge/Taylor & Francis Group.

Callard, F. (2015) *Psychological coercion and manipulation is now a daily part of claiming benefits*. Available at: https://www.dur.ac.uk/research/news/thoughtleadership/?itemno=24998 (Accessed: 5 June 2017).

Calvo-Porral, C. and Pesqueira-Sanchez, R. (2019) ‘Generational differences in technology behaviour: comparing millennials and Generation X’, *Kybernetes*, 49(11), pp. 2755–2772. Available at: https://doi.org/10.1108/K-09-2019-0598.

Cambridge (2019) *Indirect advertising*, *Cambridge dictionary*. Available at: https://dictionary.cambridge.org/dictionary/english/indirect-advertising (Accessed: 13 March 2019).

Capriotti, P., Zeler, I. and Camilleri, M.A. (2021) ‘Corporate Communication Through Social Networks: The Identification of the Key Dimensions for Dialogic Communication’, in M.A. Camilleri (ed.) *Strategic Corporate Communication in the Digital Age*. Emerald Publishing Limited. Available at: https://doi.org/https://doi.org/10.1108/978-1-80071-264-520211003.

Capurro, R. (2013) ‘Ethical issues of online social networks in Africa.’, *Innovation (10258892)*, (47), pp. 161–175. Available at: http://libaccess.sjlibrary.org/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=lls&AN=101170549&site=ehost-live&scope=site.

Carabantes, M. (2021) ‘The Coronavirus as a Revenge Effect: The Pandemic from the Perspective of Philosophy of Technique’, *Science, Technology, & Human Values*, p. 016224392110085. Available at: https://doi.org/10.1177/01622439211008595.

Caredda, S. (2020) *Organisational Awareness: a critical capability for the business*, *Sergio Caredda*. Available at: https://sergiocaredda.eu/organisation/organisational-awareness-a-critical-capability-for-the-business/amp/ (Accessed: 12 February 2021).

Carlsson, U. (2019) *Understanding Media and Information Literacy (MIL) in the Digital*

Age, *Understanding Media Literacy in the Digital Age. A question of democracy*. Available at: https://en.unesco.org/sites/default/files/gmw2019_understanding_mil_ulla_carlsson.pdf.

Carnegie Mellon University (2016) *Personalised Privacy Assistant Project*. Available at: http://www.privacyassistant.org/ (Accessed: 13 October 2016).

Carpenter, C.J. and McEwan, B. (2016) *Dating apps on smartphones have brought speed dating on the Internet to a new level*, *First Monday*. Available at: Christopher J. Carpenter and Bree McEwan (Accessed: 4 June 2017).

Carroll, A.B. (2014) '" Societies for Business Ethics " , Wiley Encyclopedia of Management ,' (January).

Carroll, A.B., Brown, J. and Buchholtz, A.K. (2018) *Business & Society: Ethics, Sustainability & Stakeholder Management*. Tenth. Boston: Cengage Learning.

Carroll, A.B. and Buchholtz, A.K. (2015) *Business and Society: Ethics, Sustainability, and Stakeholder Management 9th Edition*. 9th edn. Cengage Learning.

Cetto, A. *et al.* (2018) '"Thanks for sharing"—Identifying users' roles based on knowledge contribution in Enterprise Social Networks', *Computer Networks*, 135, pp. 275–288. Available at: https://doi.org/10.1016/j.comnet.2018.02.012.

Charmaz, K. (2008) 'Reconstructing Grounded Theory', in *The SAGE Handbook of Social Research Methods*, pp. 463–478.

Chawla, A. *et al.* (2019) 'Computer Vision Syndrome: Darkness Under the Shadow of Light', *Canadian Association of Radiologists Journal*, 70(1), pp. 5–9. Available at: https://doi.org/10.1016/j.carj.2018.10.005.

Child, D. (2006) *The Essentials of Factor Analysis*. 3rd edn. London: Continuum.

Chin, C.P.Y., Evans, N. and Choo, K.K.R. (2015) 'Exploring Factors Influencing the Use of Enterprise Social Networks in Multinational Professional Service Firms', *Journal of Organizational Computing and Electronic Commerce*, 25(3), pp. 289–315. Available at: https://doi.org/10.1080/10919392.2015.1058118.

Choe, E.K. *et al.* (2013) 'Nudging people away from privacy-invasive mobile apps through visual framing', *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 8119 LNCS(PART 3), pp. 74–91. Available at: https://doi.org/10.1007/978-3-642-40477-1_5.

Choi, Y. (2018) 'Narcissism and Social Media Addiction in Workplace', *The Journal of Asian Finance, Economics and Business*, pp. 95–104. Available at: https://doi.org/10.13106/jafeb.2018.vol5.no2.95.

Chouaib, A. and Zaddem, F. (2013) 'The Ethical Climate at Work: Promoting Trust in Organizations', *RIMHE : Revue Interdisciplinaire Management, Homme & Entreprise*, n° 9(5), pp. 15–30. Available at: https://doi.org/10.3917/rimhe.009.0015.

Christian, J.S. and Ellis, A.P.J. (2014) 'The Crucial Role of Turnover Intentions in Transforming Moral Disengagement Into Deviant Behavior at Work', *Journal of Business Ethics*, 119(2), pp. 193–208. Available at: https://doi.org/10.1007/s10551-013-1631-4.

Christian, L. *et al.* (2019) 'Enhancing the Theory of Planned Behaviour by Incorporating Social Marketing Behavioural Enhancers: A First VS Second Order Confirmatory Factor Analysis Approach', *Journal of Economics and Behavioral Studies*, 11(1), pp. 139–151.

Cipolletta, S., Malighetti, C. and Cenedese, C. (2020) 'How Can Adolescents Benefit from the Use of Social Networks ? The iGeneration on Instagram', *International Journal of Environmental Research and Public Health*, 17.

Clark, D. (2012) 'Transparency is the new leadership imperative', *Harvard Business Review* [Preprint]. Available at: http://blogs.hbr.org/cs/2012/04/transparency_is_the_new_leader.html?cm_mmc=email-_-newsletter-_-leadership-_-leadership050212&referral=00206&utm_source=newsletter_leadership&utm_medium=email&utm_campaign=leadership050212.

Clement, J. (2017) *Most famous social network sites worldwide as of April 2017, ranked by number of active users (in millions)*, *Statista*. Available at: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ (Accessed: 28 June 2017).

Clement, J. (2019a) *Mobile messenger apps - Statistics & Facts | Statista*, *Statista*. Available at: https://www.zipwhip.com/blog/heres-how-each-generation-prefers-to-text-with-your-business/ (Accessed: 24 October 2019).

Clement, J. (2019b) *Most famous social network sites worldwide as of July 2019, ranked by number of active users (in millions)*, *Statista*. Available at: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ (Accessed: 2 November 2019).

Clement, J. (2019c) *Most popular global mobile messenger apps as of July 2019, based on number of monthly active users (in millions)*, *Statista*. Available at: https://www.statista.com/statistics/961736/crude-oil-reserves-bolivia/.

Clement, J. (2020) *Most popular global mobile messenger apps as of October 2020, based on number of monthly active users*, *Statista*. Available at: https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/ (Accessed: 2 November 2020).

Constantinou, C.S., Georgiou, M. and Perdikogianni, M. (2017) ‘A comparative method for themes saturation (CoMeTS) in qualitative interviews’, *Qualitative Research*, 17(5), pp. 571–588. Available at: https://doi.org/10.1177/1468794116686650.

Cooper, A. (2017) ‘What is "brain hacking? Tech insiders on why you should care’, *CBS News* [Preprint]. Available at: http://www.cbsnews.com/news/brain-hacking-tech-insiders-60-minutes/ (Accessed: 30 May 2017).

Corbin, J.M. and Strauss, A. (1990) ‘Grounded theory research: Procedures, canons, and evaluative criteria’, *Qualitative Sociology*, 13(1), pp. 3–21. Available at: https://doi.org/10.1007/BF00988593.

Correia, J. and Compeau, D. (2017) ‘Information Privacy Awareness (IPA): A Review of the Use , Definition and Measurement of IPA’, *50th Hawaii International Conference on System Sciences*, pp. 4021–4030.

Cosenza, V., Alexa and Similarweb.com (2019) *WORLD MAP OF SOCIAL*, *Vincos.it*. Available at: https://vincos.it/world-map-of-social-networks/ (Accessed: 19 September 2019).

Cox, T. (2019) *How Different Generations Use Social Media Social Media*, *The Manifest*. Available at: https://themanifest.com/social-media/how-different-generations-use-social-media (Accessed: 18 October 2019).

Creswell, J.W. *et al.* (2007) 'Qualitative Research Designs: Selection and Implementation', *The Counseling Psychologist*, 35(2), pp. 236–264. Available at: https://doi.org/10.1177/0011000006287390.

Creswell, J.W. (2013) *Research Design_ Qualitative, Quantitative, and Mixed Methods Approaches-SAGE Publications, Inc (2013)*. Sage Publications. Available at: https://doi.org/10.1007/s13398-014-0173-7.2.

Creswell, J.W. and Creswell, J.D. (2018) *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. Fifth. Sage Publications, Inc.

Crosby, J. (2015) *Phone skills a major work hang-up for Millennials*, *Star Tribune*. Available at: http://www.startribune.com/phone-skills-a-major-work-hang-up-for-millennials/282793031/ (Accessed: 22 June 2017).

Crossler, R.E. and Bélanger, F. (2019) 'Why would I use location-protective settings on my smartphone? Motivating protective behaviors and the existence of the privacy knowledge–belief gap', *Information Systems Research*, 30(3), pp. 995–1006. Available at: https://doi.org/10.1287/isre.2019.0846.

Crowell, A. and Ramakrishna, A. (2020) 'Risk and Demographics ' Influence on Security Behavior Intentions', *The Journal of the Southern Association for Information Systems Volume*, 7(1). Available at: https://aisel.aisnet.org/jsais/vol7/iss1/2.

Cullity, G. (2018) 'Moral judgement', *Routledge Encyclopedia of Philosophy*, pp. 1–2. Available at: https://doi.org/10.4324/9780415249126-l053-2.

Curtis, M. (2014) 'Discussion of "Ethical Climate, Social Responsibility and Earnings Management"', *Journal of Business Ethics*, pp. 61–63. Available at: https://doi.org/10.1007/s10551-013-2036-0.

D'Arienzo, M.C., Boursier, V. and Griffiths, M.D. (2019) 'Addiction to Social Media and Attachment Styles: A Systematic Literature Review', *International Journal of Mental Health and Addiction*, 17(4), pp. 1094–1118. Available at: https://doi.org/10.1007/s11469-019-00082-5.

Dahlberg, K. (2006) ‘The essence of essences - The search for meaning structures in phenomenological analysis of lifeworld phenomena’, *International Journal of Qualitative Studies on Health and Well-being*, 1(1), pp. 11–19. Available at: https://doi.org/10.1080/17482620500478405.

Daniels, G. (2016) *Digital activism in the social media era: Critical reflections on emerging trends in sub-Saharan Africa*, *Digital Activism in the Social Media Era: Critical Reflections on Emerging Trends in Sub-Saharan Africa*. Edited by B. Mutsvairo. Palgrave Macmillan. Available at: https://doi.org/10.1007/978-3-319-40949-8.

Davenport, S.W. *et al.* (2014) ‘Twitter versus Facebook: Exploring the role of narcissism in the motives and usage of different social media platforms’, *Computers in Human Behavior*, 32, pp. 212–220. Available at: https://doi.org/10.1016/j.chb.2013.12.011.

Davies, B. and Badal, K. (2016) *#Yourefired: Dismissals Of Employees Due To Social Media Usage*, *Go Legal*. Available at: http://www.golegal.co.za/yourefired-dismissals-of-employees-due-to-social-media-usage/ (Accessed: 29 September 2016).

Davis, N. (2011) *F**k, It’s Hard To Keep Profanity Off Your Facebook Wall*, *Business Insider*. Available at: http://www.businessinsider.com/facebook-swearing-profanity-reppler-2011-5 (Accessed: 19 June 2017).

Debatin, B. *et al.* (2009) ‘Facebook and online privacy: Attitudes, behaviors, and unintended consequences’, *Journal of Computer-Mediated Communication*, 15(1), pp. 83–108. Available at: https://doi.org/10.1111/j.1083-6101.2009.01494.x.

Debatin, B. (2011) ‘Ethics, Privacy, and Self-Restraint in Social Networking’, in *In Privacy online*. Springer Berlin Heidelberg, pp. 47–60. Available at: https://doi.org/10.1007/978-3-642-21521-6.

Desai, R., Patel, D. and Mohit, M. (2019) ‘Correlation of anxiety, depression, and socioeconomic status with phantom vibration syndrome in healthy individuals’, *National Journal of Physiology, Pharmacy and Pharmacology*, 9(0), p. 1. Available at: https://doi.org/10.5455/njppp.2019.9.0415316052019.

Deterding, N.M. and Waters, M.C. (2021) ‘Flexible Coding of In-depth Interviews: A

Twenty-first-century Approach', *Sociological Methods and Research*, 50(2), pp. 708–739. Available at: https://doi.org/10.1177/0049124118799377.

DeTienne, K.B. *et al.* (2019) 'Moral Development in Business Ethics: An Examination and Critique', *Journal of Business Ethics*, 170(3), pp. 429–448. Available at: https://doi.org/10.1007/s10551-019-04351-0.

Deutsch, A.L. (2018) *WhatsApp: The Best Facebook Purchase Ever? | Investopedia*, *Investopedia*. Available at: https://www.investopedia.com/articles/investing/032515/whatsapp-best-facebook-purchase-ever.asp.

Devellis, R.F. (2017) *Scale Development: Theory and Applications (Applied Social Research Methods)*. Fourth. SAGE Publications.

DeWane, M., Waldman, R. and Waldman, S. (2019) 'Cell phone etiquette in the clinical arena: A professionalism imperative for healthcare', *Current Problems in Pediatric and Adolescent Health Care*, 49(4), pp. 79–83. Available at: https://doi.org/10.1016/j.cppeds.2019.03.005.

Dhir, A. *et al.* (2018) 'Online social media fatigue and psychological wellbeing—A study of compulsive use, fear of missing out, fatigue, anxiety and depression', *International Journal of Information Management*, 40(January), pp. 141–152. Available at: https://doi.org/10.1016/j.ijinfomgt.2018.01.012.

Díaz-prieto, C. and Canedo-garcía, A. (2019) 'Impact of Life Experiences and Use of Web 2 . 0 Tools in Adults and Older Adults', *Frontiers in Psychology*, 10(September), pp. 1–11. Available at: https://doi.org/10.3389/fpsyg.2019.02158.

Dienlin, T. and Trepte, S. (2015) 'Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors', *European Journal of Social Psychology*, 45(3), pp. 285–297. Available at: https://doi.org/10.1002/ejsp.2049.

Dijck, J. van and Poell, T. (2013) 'Understanding social media logic', *Media and Communication*, 1(1), pp. 2–14. Available at: https://doi.org/10.1177/1745691612459060.

DLA PIPER (2020) *Data Protection Laws of the World South Africa*, *Data Protection Laws of the World Handbook*. Available at:

http://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw/functions/export.pdf?country=all.

Doffman, Z. (2020) ‘Ashley Madison Hack Returns To “ Haunt ” Its Victims : 32 Million Users Now Watch And’, *Forbes.com*, pp. 1–5. Available at: https://www.forbes.com/sites/zakdoffman/2020/02/01/ashley-madison-hack-returns-to-haunt-its-victims-32-million-users-now-have-to-watch-and-wait/?sh=48aba5355677.

Dogra, M. (2017) *Messaging Apps Are The Next Big Thing In Social Media*, *Mambo*. Available at: https://www.mambomedia.com/blog/messaging-apps-are-the-next-big-thing-in-social-media/ (Accessed: 20 July 2017).

Dolan, R. *et al.* (2019) ‘Social media engagement behavior: A framework for engaging customers through social media content’, *European Journal of Marketing*, 53(10), pp. 2213–2243. Available at: https://doi.org/10.1108/EJM-03-2017-0182.

Donnellan, M.B., Ackerman, R.A. and Brecheen, C. (2015) ‘Extending Structural Analyses of the Rosenberg Self- Esteem Scale to Consider Criterion-Related Validity : Can Composite Self-Esteem Scores Be Good Enough ? Extending Structural Analyses of the Rosenberg Self-Esteem Scale to Consider Criterion-Related Val’, *Journal ofPersonality Assessment* [Preprint], (September). Available at: https://doi.org/10.1080/00223891.2015.1058268.

Dworkin, G. (1983) ‘Paternalism: some second thoughts’, *Paternalism*, p. 105.

Edwards, K. (2016) ‘There Is No Such Thing as Medium Rare.’, in *Hello! And Every Little thing That Matters*. New York: Palgrave Macmillan, New York, pp. 67–78. Available at: https://doi.org/https://doi.org/10.1057/9781137489715_6.

Egelman, S., Harbach, M. and Peer, E. (2016) ‘Behavior Ever Follows Intention?: A Validation of the Security Behavior Intentions Scale (SeBIS)’, *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pp. 5257–5261. Available at: https://doi.org/10.1145/2858036.2858265.

Egelman, S. and Peer, E. (2015) ‘Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS)’, *Proceedings of the ACM CHI’15 Conference on Human Factors in Computing Systems*, 1, pp. 2873–2882. Available at:

https://doi.org/10.1145/2702123.2702249.

Elhai, J.D. *et al.* (2016) ‘Fear of missing out, need for touch, anxiety and depression are related to problematic smartphone use’, *Computers in Human Behavior*, 63, pp. 509–516. Available at: https://doi.org/10.1016/j.chb.2016.05.079.

Emiliussen, J. *et al.* (2021) ‘We are all in it!: Phenomenological Qualitative Research and Embeddedness’, *International Journal of Qualitative Methods*, 20, pp. 1–6. Available at: https://doi.org/10.1177/1609406921995304.

Eslambolchilar, P. *et al.* (2011) ‘PINC : Persuasion , Influence , Nudge and Coercion Through Mobile Devices’, *In CHI’11 Extended Abstracts on Human Factors in Computing Systems (pp. 13-16). ACM.*, pp. 13–16.

Evans, J.S.B.T. (2008) ‘Dual-Processing Accounts of Reasoning, Judgment, and Social Cognition’, *Annual Review of Psychology*, 59(1), pp. 255–278. Available at: https://doi.org/10.1146/annurev.psych.59.103006.093629.

Evans, J.S.B.T. and Stanovich, K.E. (2013) ‘Dual-Process Theories of Higher Cognition’, *Perspectives on Psychological Science*, 8(3), pp. 223–241. Available at: https://doi.org/10.1177/1745691612460685.

Facebook (2017a) *Can I message members of a group if they are not my friends?*, *Facebook.com*. Available at: https://www.facebook.com/help/186518618066419?helpref=uf_permalink (Accessed: 11 July 2017).

Facebook (2017b) *Data Policy*, *Facebook*. Available at: https://www.facebook.com/about/privacy (Accessed: 28 June 2017).

Facebook (2017c) *Group Conversations*, *Facebook.com*. Available at: https://www.facebook.com/help/messenger-app/1759354747722950 (Accessed: 11 July 2017).

Facebook (2017d) *Updating Our Terms and Policies: Helping You Understand How Facebook Works and How to Control Your Information*, *Facebook*. Available at: https://www.facebook.com/about/terms-updates (Accessed: 28 June 2017).

Facebook (2017e) *What are the privacy settings for groups? | Facebook Help Centre*, *Facebook.com*. Available at: https://www.facebook.com/help/220336891328465

(Accessed: 11 July 2017).

Facebook (2020) *How can I adjust my Facebook privacy settings?*, *Facebook Help Centre*. Available at: https://web.facebook.com/help/193677450678703?_rdc=1&_rdr (Accessed: 2 November 2020).

Fan, X., Thompson, B. and Wang, L. (1999) 'Structural Equation Modeling : A Multidisciplinary Effects of sample size , estimation methods , and model specification on structural equation modeling fit indexes', *Structural Equation Modeling: A Multidisciplinary Journal*, 6(February), pp. 56–83. Available at: https://doi.org/10.1080/10705519909540119.

Farley, S. *et al.* (2015) 'Exploring the impact of workplace cyberbullying on trainee doctors', *Medical Education*, 49(4), pp. 436–443. Available at: https://doi.org/10.1111/medu.12666.

Federal Trade Commision (2013) 'Federal Register Notices January 17 2013 Vol 78 No 12'. Federal Trade Commision. Available at: https://www.ftc.gov/system/files/documents/federal_register_notices/2013/01/2012-31341.pdf (Accessed: 12 October 2016).

Federal Trade Commission (2019) *Privacy & Data Security Update: 2019*, *Federal Trade Commission*.

Feeney, M.K. and Porumbescu, G. (2020) 'The Limits of Social Media for Public Administration Research and Practice', *Public Administration Review* [Preprint], (August). Available at: https://doi.org/10.1111/puar.13276.

Feldman, R. (1998) 'Epistemology and ethics', *Routledge Encyclopedia of Philosophy. London: Routledge, Web. (September 27, 2016).* Available at: https://doi.org/10.4324/9780415249126-P017-1.

Fennell, K. (2019) *Must-Know Social Media News Stories Must-Know Social Media Updates of September 2019 Facebook gets creative*, *mavsocial.com*. Available at: 20 September 2019 (Accessed: 19 October 2019).

Ferlito, B. and Mametja, S. (2021) 'Social media for healthcare professionals: New ethical guidelines', *Current Allergy and Clinical Immunology*, 34(1), pp. 6–9. Available at: https://doi.org/10.520/ejc-caci-v34-n1-a2.

Filabi, A. and Bulgarella, C. (2018) ‘Organizational Culture Drives Ethical Behaviour: Evidence From Pilot Studies’, *2018 OECD Global Anti-Corruption & Integrity Forum2*, pp. 1–17. Available at: https://www.oecd.org/corruption/integrity-forum/academic-papers/Filabi.pdf.

Fire, M., Goldschmidt, R. and Elovici, Y. (2014) ‘Online Social Networks : Threats and Solutions’, *IEEE Communications Surveys & Tutorials*, 16(4), pp. 2019–2036. Available at: https://doi.org/10.1109/COMST.2014.2321628.

Fishbein, M. and Ajzen, I. (1975) *Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research*. MA: Addison-Wesley.

Florea, A.R. and Roman, M. (2019) ‘the Profile of Social Media Users in Romania: Individual Characteristics and the Number of Social Connections’, *Proceedings of the 18th International Conference on INFORMATICS in ECONOMY Education, Research and Business Technologies*, 2019, pp. 285–292. Available at: https://doi.org/10.12948/ie2019.04.21.

Floridi, L. *et al.* (2015) *The Advisory Council to Google on the Right to be Forgotten*.

Fogg, B. (2009a) ‘A behavior model for persuasive design’, *Proceedings of the 4th International Conference on Persuasive Technology - Persuasive ’09*, p. 1. Available at: https://doi.org/10.1145/1541948.1541999.

Fogg, B. (2009b) ‘Creating Persuasive Technologies: An Eight-Step Design Process’, *Proceedings of the 4th International Conference on Persuasive Technology - Persuasive ’09*, p. 1. Available at: https://doi.org/10.1145/1541948.1542005.

Fogg, B. (2016) *BJ Fogg’s Behavior Model*, *BJ Fogg’s Behavior Model*. Available at: http://www.behaviormodel.org/ (Accessed: 3 May 2017).

Fogg, B.J. and Euchner, J. (2019) ‘Designing for Behavior Change—New Models and Moral Issues’, *Research-Technology Management*, 62(5), pp. 14–19. Available at: https://doi.org/10.1080/08956308.2019.1638490.

Foley, M. (2016) *What Is A Snapchat Streak? Here’s Everything You Need To Know About Snapstreaks*, *bustle.com*. Available at: https://www.bustle.com/articles/162803-what-is-a-snapchat-streak-heres-everything-you-need-to-know-about-snapstreaks (Accessed: 30 May 2017).

Foltýn, T. (2019) *Twitter bug may have exposed private tweets of Android users for years*, *welivesecurity*. Available at: https://www.welivesecurity.com/2019/01/21/twitter-bug-may-exposed-private-tweets-android-users-years/ (Accessed: 2 November 2020).

Freire, C. and Pinto, M.I. (2021) 'Clarifying the mediating effect of ethical climate on the relationship between ethical leadership and workplace bullying', *Ethics and Behavior*, 00(00), pp. 1–12. Available at: https://doi.org/10.1080/10508422.2021.1941027.

Friemel, T.N. and Bixler, M. (2018) 'Networked Media Collectivities. The Use of Media for the Communicative Construction of Collectivities Among Adolescents', *Transforming Communication*, pp. 173–202. Available at: https://doi.org/10.1007/978-3-319-65584-0_8.

Frost, R.L. and Rickwood, D.J. (2017) 'A systematic review of the mental health outcomes associated with Facebook use', *Computers in Human Behavior*, 76, pp. 576–600. Available at: https://doi.org/10.1016/j.chb.2017.08.001.

Gadamer, H.-G. (2006) *Truth and method*. Second, Re. Edited by J. Weinsheimer and D.G. Marshall. London and New York: Continuum Publishing Group.

García, J.A., Olmos, F.C. y and Matheu, M.L. (2019) 'Self esteem levels vs global scores on the Rosenberg self- esteem scale', *Heliyon 5*, 5. Available at: https://doi.org/10.1016/j.heliyon.2019.e01378.

Garvey, J. (2016) *The Persuaders*. 1st edn. Icon Books Ltd.

Georgiadou, Y., De By, R.A. and Kounadi, O. (2019) 'Location privacy in the wake of the GDPR', *ISPRS International Journal of Geo-Information*, 8(3). Available at: https://doi.org/10.3390/ijgi8030157.

Gino, F. (2017) 'Radical Transparency Can Reduce Bias — but Only If It's Done Right', *Harvard Business Review*, pp. 2–6.

Glaser, B.G. (2016) 'Open Coding Descriptions', *Grounded Theory Review: An International Journal*, 15(2), pp. 108–110.

Glaser, B.G. and Strauss, A.L. (1967) *The Discovery of Grounded Theory: Strategies for Qualitative Research.* Chicago, IL: Aldine.

Gluck, J. *et al.* (2016) ‘How Short Is Too Short ? Implications of Length and Framing on the Effectiveness of Privacy Notices This paper is included in the Proceedings of the Implications of Length and Framing on the Effectiveness of Privacy Notices’, *the Symposium On Usable Privacy and Security (SOUPS)*, (Soups), pp. 321–340.

Goleman, D. *et al.* (2017) *Organizational awareness : a primer*. Florence: Key Step Media/More Than Sound.

Goncalves, L. *et al.* (2021) ‘Nomophobia in the last decade: a systematic review’, *Mental Health and Addiction Research*, 6(3). Available at: https://doi.org/10.15761/mhar.1000203.

Gottschalk, P. and Benson, M.L. (2020) ‘The Evolution of Corporate Accounts of Scandals from Exposure to Investigation’, *British Journal of Criminology*, 60(4), pp. 949–969. Available at: https://doi.org/10.1093/bjc/azaa001.

Gray, R. (2001) ‘Thirty years of social accounting, reporting and auditing: what (if anything) have we learnt?’, *Business Ethics: A European Review*, 10(1), pp. 9–15. Available at: https://doi.org/10.1111/1467-8608.00207.

Green, H. (2015) *Theft, Lies, and Facebook Video*, *Medium.com*. Available at: Hank Green (Accessed: 27 June 2017).

Griffith, M.D. and Kuss, D.J. (2017) ‘Adolescents in scial media addiction (revisited)’, *Education and Health*, 35(3), pp. 49–52.

Griffiths, M.D. (2013) ‘Social Networking Addiction : Emerging Themes and Issues’, *Journal of Addiction Research & Therapy*, 4(5), pp. 4–5. Available at: https://doi.org/10.4172/2155-6105.1000e118.

Grimes, R.A. (2015) *10 reasons why phishing attacks are nastier than ever*, *InfoWorld*. InfoWorld. Available at: http://www.infoworld.com/article/3000943/phishing/10-reasons-why-phishing-attacks-are-nastier-than-ever.html (Accessed: 16 October 2016).

Grimes, R.A. (2016) *Why we must defend our last shred of privacy*, *InfoWorld*. Available at: http://www.infoworld.com/article/3036472/security/why-we-must-defend-our-last-shred-of-privacy.html (Accessed: 16 October 2016).

Grimmelikhuijsen, S. (2012) ‘Linking transparency, knowledge and citizen trust in government: an experiment', *International Review of Administrative Sciences*, 78(1), pp. 50–73. Available at: https://doi.org/10.1177/0020852311429667.

Grobler, A. (2016) 'An adapted measure of ethical climate in organisations – a South African study'.

Grobler, C. and Dhai, A. (2016) 'Social media in the healthcare context: Ethical challenges and recommendations', *South African Journal of Bioethics and Law*, 9(1), p. 22. Available at: https://doi.org/10.7196/sajbl.2016.v9i1.464.

Groenewald, T. (2004) 'A Phenomenological Research Design Illustrated', *International Journal of Qualitative methods*, 3(1), pp. 1–26. Available at: https://doi.org/Retrieved from: http://www.ualberta.ca/~iiqm/backissues/3_1/html/groenewald.html.

Gusehl, J.S., Brendel, R.W. and Brendel, D.H. (2009) 'Medical professionalism in the age of online social networking', *Journal of Medical Ethics*, 35(9), pp. 584–586. Available at: https://doi.org/10.1136/jme.2009.029231.

Hackston, J. (2020) 'How Different Personality Types Cope with an Always-on Culture', *Harvard Business Review*, pp. 1–5. Available at: https://hbp.myhbp.org/leadingedge/public/distributions/51ef1e34-587c-429e-bade-ca667bebc6dd/assets/02aad9cf-93ca-43e4-b32f-350c77e64585.

Hagendorff, T. (2018) 'Privacy Literacy and Its Problems', *Thilo Hagendorff 127 Journal of Information Ethics*, 27(2), p. 127.

Hair, J.F.J. *et al.* (2014) *Multivariate Data Analysis*. Pearson Ne, *Exploratory Data Analysis in Business and Economics*. Pearson Ne. Essex CM20 2JE: Pearson Education Limited. Available at: https://doi.org/10.1007/978-3-319-01517-0_3.

Hajli, N. (2018) 'Ethical Environment in the Online Communities by Information Credibility: A Social Media Perspective', *Journal of Business Ethics*, 149(4), pp. 799–810. Available at: https://doi.org/10.1007/s10551-016-3036-7.

Hallen, E. (2014) *How To Use the Psychology Of Social Proof To Your Advantage*, *Fastcompany.com*. Available at: https://www.fastcompany.com/3030044/how-to-use-the-psychology-of-social-proof-to-your-advantage (Accessed: 28 June 2017).

Hammond, A.L. (2001) 'Digitally empowered development', *Foreign Affairs*, 80(2), p.

96. Available at: https://doi.org/10.2307/20050067.

Haraty, R. a. and Massalkhy, S. (2013) *Security and Privacy Preserving in Social Networks*, *Security and Privacy Preserving in Social Networks*. Available at: https://doi.org/10.1007/978-3-7091-0894-9.

Harris, T. (2014) *Is your web browser a credit card for your time ?* Available at: http://www.tristanharris.com/essays/ (Accessed: 30 May 2017).

Harris, T. (2016) 'How Technology Hijacks People's Minds — from a Magician and Google's Design Ethicist', *Medium.com*, pp. 1–24. Available at: https://medium.com/swlh/how-technology-hijacks-peoples-minds-from-a-magician-and-google-s-design-ethicist-56d62ef5edf3#.79q0unppa (Accessed: 30 May 2017).

Harris, T. and Swisher, K. (2019) *Tristan Harris says tech is " downgrading " humanity — but we can fix it*, *Vox.com*. Available at: https://www.vox.com/recode/2019/5/6/18530860/tristan-harris-human-downgrading-time-well-spent-kara-swisher-recode-decode-podcast-interview (Accessed: 20 October 2019).

Hartzog, W. (2017) 'The Inadequate, Invaluable Fair Information Practices', *Maryland Law Review (Baltimore, Md.)*, 76(4), p. 952.

Hartzog, W. (2018) *User Agreements Are Betraying You*, *Medium*. Available at: https://medium.com/s/trustissues/user-agreements-are-betraying-you-19db7135441f (Accessed: 1 July 2019).

Hawi, N.S. and Samaha, M. (2017a) 'The Relations Among Social Media Addiction, Self-Esteem, and Life Satisfaction in University Students', *Social Science Computer Review*, 35(5), pp. 576–586. Available at: https://doi.org/10.1177/0894439316660340.

Hawi, N.S. and Samaha, M. (2017b) 'The Relations Among Social Media Addiction, Self-Esteem, and Life Satisfaction in University Students', *Social Science Computer Review*, 35(5), pp. 576–586. Available at: https://doi.org/10.1177/0894439316660340.

Hawkridge, D. (2022) *New Information Technology in Education*, *New Information Technology in Education*. Available at: https://doi.org/10.4324/9781003312826.

Heemsbergen, L. (2016) 'From radical transparency to radical disclosure: Reconfiguring (in)voluntary transparency through the management of visibilities', *International Journal of Communication*, 10(1), pp. 138–151.

Heemsbergen, L.J. (2013) 'Radical transparency in Journalism: Digital evolutions from historical precedents', *Global Media Journal, Canadian Edition*, 6(1), pp. 45–65.

Van Heerden, G. and Jordaan, Y. (2017) 'Computers in Human Behavior Online privacy-related predictors of Facebook usage intensity', *Computers in Human Behavior*, 70, pp. 90–96. Available at: https://doi.org/10.1016/j.chb.2016.12.048.

Heimstädt, M. and Dobusch, L. (2020) 'Transparency and Accountability: Causal, Critical and Constructive Perspectives', *Organization Theory*, 1(4). Available at: https://doi.org/10.1177/2631787720964216.

Heirman, W. *et al.* (2016) 'An open book on Facebook? Examining the interdependence of adolescents' privacy regulation strategies', *Behaviour and Information Technology*, 35(9), pp. 706–719. Available at: https://doi.org/10.1080/0144929X.2016.1181210.

Helberger, N., Pierson, J. and Poell, T. (2018) 'Governing online platforms: From contested to cooperative responsibility', *Information Society*, 34(1), pp. 1–14. Available at: https://doi.org/10.1080/01972243.2017.1391913.

Herrando, C., Jimenez-Martinez, J. and Martin-De Hoyos, M.J. (2019) 'Tell me your age and I tell you what you trust: the moderating effect of generations', *Internet Research*, 29(4), pp. 799–817. Available at: https://doi.org/10.1108/IntR-03-2017-0135.

Hess, D. (2019) 'The transparency trap: Non-financial disclosure and the responsibility of business to respect human rights', *American Business Law Journal*, 56(1), pp. 5–53. Available at: https://doi.org/10.1111/ablj.12134.

Hirschprung, R.O.N., Toch, E. and Schwartz-Chassidim, H. (2017) 'Analyzing and Optimizing Access Control Choice Architectures in Online Social Networks', *ACM Transactions on Intelligent Systems and Technology*, 8(4).

Hocevar, K.P., Flanagin, A.J. and Metzger, M.J. (2014) 'Social media self-efficacy and information evaluation online', *Computers in Human Behavior*, 39, pp. 254–262. Available at: https://doi.org/10.1016/j.chb.2014.07.020.

Hofschneider, A. (2013) 'Bosses Say "Pick Up the Phone"', *Wall Street Journal*.

Available at: https://www.wsj.com/articles/bosses-say-pick-up-the-phone-1377643939?tesla=y.

Hooper, D., Coughlan, J. and Mullen, M. (2008) ‘Structural equation modelling: Guidelines for determining model fit. Electronic Journal of Business Research Methods’, *Electronic Journal of Business Research Methods*, 6(1), pp. 53–59. Available at: https://doi.org/10.1037/1082-989X.12.1.58.

Hootsuite & We Are Social (2016) ‘Digital 2016’, *Hootsuite & We Are Social* [Preprint].

Hord, J. (2005) *How SMS Works*, *HowStuffWorks.com*. Available at: http://computer.howstuffworks.com/e-mail-messaging/sms1.htm (Accessed: 21 June 2017).

Horn, I.S. *et al.* (2015) ‘Business reputation and social media: A primer on threats and responses’, *Journal of Direct, Data and Digital Marketing Practice*, 16(3), pp. 193–208. Available at: https://doi.org/10.1057/dddmp.2015.1.

Hou, Y. *et al.* (2019) ‘Social media addiction: Its impact, mediation, and intervention.’, *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 13(1).

Howe, N. (2015) ‘Why Millennials Are Texting More And Talking Less’, *Forbes*, pp. 15–18. Available at: https://www.forbes.com/sites/neilhowe/2015/07/15/why-millennials-are-texting-more-and-talking-less/#383a47bd5975.

Howe, N. and Strauss, W. (2007) ‘The next 20 years: How customer and workforce attitudes will evolve’, *Harvard Business Review*, 85(12), pp. 124–125.

Huang, H.Y. *et al.* (2020) ‘Smartphone Security Behavioral Scale: A New Psychometric Measurement for Smartphone Security’, *arXiv* [Preprint].

Hughes, D.J. *et al.* (2012) ‘A tale of two sites: Twitter vs. Facebook and the personality predictors of social media usage’, *Computers in Human Behavior*, 28, pp. 561–569. Available at: https://doi.org/10.1016/j.chb.2011.11.001.

IBM (2011) *Bringing big data to the enterprise: what is big data? Available*. Available at: http://www-01.ibm.com/software/data/bigdata/what-is-big-data.html (Accessed: 2 October 2016).

Ienca, M. and Haselager, P. (2016) ‘Hacking the brain: brain-computer interfacing technology and the ethics of neurosecurity', *Ethics and Information Technology*, 18(2), pp. 117–129. Available at: https://doi.org/10.1007/s10676-016-9398-9.

Iqbal, M. (2021) *Tinder Revenue and Usage Statistics (2021)*, *Business of Apps*. Available at: https://www.businessofapps.com (Accessed: 30 March 2021).

Iqbal, M., Nisha, N. and Rifat, A. (2018) 'E-Government Service Adoption and the Impact of Privacy and Trust', in *Encyclopedia of Information Science and Technology*. Fourth Edi. IGI Global, pp. 3579–3590. Available at: https://doi.org/10.4018/978-1-5225-2255-3.

Isaac, M. and Kang, C. (2019) 'Facebook expects to be fined up to $5 billion by FTC over privacy issues', *The New York Times*, pp. 24–25. Available at: https://www.nytimes.com/2019/04/24/technology/facebook-ftc-fine-privacy.html.

Isaak, J. and Hanna, M.J. (2018) 'User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection', *Computer*, 51(8), pp. 56–59. Available at: https://doi.org/10.1109/MC.2018.3191268.

Ishii, K., Lyons, M.M. and Carr, S.A. (2019) 'Revisiting media richness theory for today and future', *Human Behavior and Emerging Technologies*, 1(2), pp. 124–131. Available at: https://doi.org/10.1002/hbe2.138.

Jafarkarimi, H. *et al.* (2016) 'Behavioral intention in social networking sites ethical dilemmas: An extended model based on Theory of Planned Behavior', *Computers in Human Behavior*, 62, pp. 545–561. Available at: https://doi.org/10.1016/j.chb.2016.04.024.

Jaworski, M. (2019) *How YouTube is revolutionizing education*, *The Daily Dot*. Available at: https://www.dailydot.com/society/youtube-education-john-green-pbs-idea-channel/ (Accessed: 4 June 2019).

Jin, D. *et al.* (2020) 'Smartphones and wearable technology: benefits and concerns in cardiology', *Medical Journal of Australia*, 212(2), pp. 54-56.e1. Available at: https://doi.org/10.5694/mja2.50446.

Jollife, I.T. and Cadima, J. (2016) 'Principal component analysis: A review and recent developments', *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 374(2065). Available at:

https://doi.org/10.1098/rsta.2015.0202.

Jolliffe, I.T. (2002) *Principal Component Analysis*. 2nd edn. New York, NY: Springer New York, NY. Available at: https://doi.org/https://doi.org/10.1007/b98835.

Jones, A.S. (2019) *Cyberbullying and the Workplace: An Analysis of Job Satisfaction and Social Self-Efficacy*. Graduate College of The University of Iowa.

Jorgensen and Bradley (2003) 'Baby Boomers, Generation X and Generation Y?', *Foresight*, 5(4), pp. 41–49. Available at: https://doi.org/10.1108/14636680310494753.

Kahne, J. and Bowyer, B. (2018) 'The Political Significance of Social Media Activity and Social Networks', *Political Communication*, 35(3), pp. 470–493. Available at: https://doi.org/10.1080/10584609.2018.1426662.

Kahneman, D. (2012) *Thinking Fast and Slow*. Penguin.

Kahneman, D. and Frederick, S. (2007) 'Frames and brains: elicitation and control of response tendencies', *Trends in Cognitive Sciences*, 11(2), pp. 45–46. Available at: https://doi.org/10.1016/j.tics.2006.11.007.

Kannengiesser, U. and Gero, J.S. (2019) 'Design thinking, fast and slow: A framework for Kahneman's dual-system theory in design', *Design Science*, 5, pp. 1–21. Available at: https://doi.org/10.1017/dsj.2019.9.

Kapoor, K.K. *et al.* (2018) 'Advances in Social Media Research: Past, Present and Future', *Information Systems Frontiers*, 20(3), pp. 531–558. Available at: https://doi.org/10.1007/s10796-017-9810-y.

Kaptein, M. (2020) 'Encyclopedia of Business and Professional Ethics', *Encyclopedia of Business and Professional Ethics* [Preprint], (June). Available at: https://doi.org/10.1007/978-3-319-23514-1.

Kara, M. *et al.* (2019) 'Duration of daily smartphone usage as an antecedent of nomophobia : exploring multiple mediation of loneliness and anxiety multiple mediation of loneliness and anxiety', *Behaviour & Information Technology*, 0(0), pp. 1–14. Available at: https://doi.org/10.1080/0144929X.2019.1673485.

Kaufmann, K. and Peil, C. (2020) 'The mobile instant messaging interview (MIMI): Using WhatsApp to enhance self-reporting and explore media usage in situ', *Mobile*

Media and Communication, 8(2), pp. 229–246. Available at: https://doi.org/10.1177/2050157919852392.

Kaupins, G. and Park, S. (2011) ‘Legal and Ethical Implications of Corporate Social Networks’, *Employee Responsibilities and Rights Journal*, 23(2), pp. 83–99. Available at: https://doi.org/10.1007/s10672-010-9149-8.

Keles, B., Mccrae, N. and Grealish, A. (2020) ‘A systematic review : the influence of social media on depression , anxiety and psychological distress in adolescents’, *International Journal of Adolescence and Youth*, 25(1), pp. 79–93. Available at: https://doi.org/10.1080/02673843.2019.1590851.

Khandelwal, S. (2016) ‘Uh oh, Yahoo Data Breach May Have Hit Over 1 Billion Users’, *The Hacker News*. Available at: http://thehackernews.com/2016/09/yahoo-data-breach-billion.html (Accessed: 16 October 2016).

Kille, D.R. and Wood, J. V. (2012) *Self-Esteem*. 2nd edn, *Encyclopedia of Human Behavior: Second Edition*. 2nd edn. Elsevier Inc. Available at: https://doi.org/10.1016/B978-0-12-375000-6.00313-X.

King, R.C. and Dong, S. (2017) ‘Ihe impact of smartphone on young adults’, *The Business and Management Review*, 8(4), pp. 342–349.

Kiran, P. and Srivastava, A. (2018) ‘Whatsapp and its Impact on Social Life of Youngsters: A Perspective’, *Management Insight - The Journal of Incisive Analysers*, 14(1). Available at: https://doi.org/10.21844/mijia.14.01.9.

Kircaburun, K. and Griffiths, M.D. (2018) ‘Instagram addiction and the Big Five of personality: The mediating role of self-liking’, *Journal of Behavioral Addictions*, 7(1), pp. 158–170. Available at: https://doi.org/10.1556/2006.7.2018.15.

Kirchner, K. and Razmerita, L. (2019) ‘Managing the Digital Knowledge Work with the Social Media Business Value Compass’, *Proceedings of the 52nd Hawaii International Conference on System Sciences*, 6, pp. 6438–6447. Available at: https://doi.org/10.24251/hicss.2019.773.

Kiriakidis, S. (2015) ‘Theory of Planned Behaviour: the Intention-Behaviour Relationship and the Perceived Behavioural Control (PBC) Relationship with Intention and Behaviour’, *International Journal of Strategic Innovative Marketing*, 03, pp. 40–

51. Available at: https://doi.org/10.15556/ijsim.02.03.004.

Kirkwood, E. (2020) '"Where Now for the Right to Be Forgotten?: A Review of the Issues in Post-Google Spain With Particular Regard to the Decision Reached in the UK."', in *Personal Data Protection and Legal Developments in the European Union*, pp. 315–331. Available at: https://doi.org/10.4018/978-1-5225-9489-5.ch016.

Koch, T., Gerber, C. and De Klerk, J.J. (2018) 'The impact of social media on recruitment: Are you Linkedin?', *SA Journal of Human Resource Management*, 16, pp. 1–14. Available at: https://doi.org/10.4102/sajhrm.v16i0.861.

Kokkinos, C.M. and Antoniadou, N. (2019) 'Cyber-bullying and cyber-victimization among undergraduate student teachers through the lens of the General Aggression Model', *Computers in Human Behavior*, 98, pp. 59–68. Available at: https://doi.org/10.1016/j.chb.2019.04.007.

Kokolakis, S. (2017) 'Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon', *Computers and Security*, 64(July 2015), pp. 122–134. Available at: https://doi.org/10.1016/j.cose.2015.07.002.

Korich, A.L. (2016) 'Harnessing a Mobile Social Media App to Reinforce Course Content', *Journal of Chemical Education*, 93(6), pp. 1134–1136. Available at: https://doi.org/10.1021/acs.jchemed.5b00915.

Kotsilieris, T. *et al.* (2017) 'The impact of social networks on health care', *Social Network Analysis and Mining*, 7(1), pp. 1–6. Available at: https://doi.org/10.1007/s13278-017-0438-1.

Koukaras, P., Tjortjis, C. and Rousidis, D. (2020) *Social Media Types: introducing a data driven taxonomy*, *Computing*. Springer Vienna. Available at: https://doi.org/10.1007/s00607-019-00739-y.

Kowalski, R.M., Toth, A. and Morgan, M. (2017) 'Bullying and cyberbullying in adulthood and the workplace', *Journal of Social Psychology*, pp. 64–81. Available at: https://doi.org/10.1080/00224545.2017.1302402.

Kraus, M. (2017) 'Comparing Generation X and Generation Y on their preferred emotional leadership style', *Journal of Applied Leadership and Management Hochschule Kempten - University of Applied Sciences, Professional School of*

Business & Technology, Kempten, 5, pp. 62–75. Available at: http://www.journal-alm.org/article/view/18130%0D.

Kritzinger, E. (2016) 'Short-term initiatives for enhancing cyber-safety within South African schools', *South African Computer Journal*, 28(1), pp. 1–17. Available at: https://doi.org/10.18489/sacj.v28i1.369.

Krosnick, J.A. and Stanley, P. (2010) *Question and Questionnaire Design*, *Handbook of Survey Research. 2nd Edn. Emerald.* Available at: https://doi.org/10.1111/j.1432-1033.1976.tb10115.x.

Kubheka, B.Z., Carter, V. and Mwaura, J. (2020) 'Social media health promotion in South Africa: Opportunities and challenges', *African Journal of Primary Health Care and Family Medicine*, 12(12), pp. 1–7. Available at: https://doi.org/10.4102/PHCFM.V12I1.2389.

Kulik, C.T. *et al.* (2015) 'Can We Still be Friends? The Role of Exit Conversations in Facilitating Post-Exit Relationships', *Human Resource Management,* 53(1), pp. 115–130. Available at: https://doi.org/10.1002/hrm.

Kumar, J.A. *et al.* (2020) 'Behavioral intention to use mobile learning: Evaluating the role of self-efficacy, subjective norm, and whatsapp use habit', *IEEE Access*, 8, pp. 208058–208074. Available at: https://doi.org/10.1109/ACCESS.2020.3037925.

Kuss, D.J. and Griffiths, M.D. (2017) 'Social networking sites and addiction: Ten lessons learned', *International Journal of Environmental Research and Public Health*, 14(3). Available at: https://doi.org/10.3390/ijerph14030311.

Lapelle, N.R. (2004) 'Simplifying Qualitative Data Analysis Using General Purpose Software Tools In Press : Field Methods , Sage Publications'.

Lazi, M. and Jovanovi, V. (2018) 'The general self-efficacy scale : New evidence of structural validity , measurement invariance , and predictive properties in relationship to subjective well-being in Serbian samples', *Curr Psychol*, 40, pp. 699–710. Available at: https://doi.org/https://doi.org/10.1007/s12144-018-9992-6.

Leech, N.L. and Onwuegbuzie, A.J. (2008) 'The SAGE encyclopedia of qualitative research methods', in, pp. 816–817. Available at: https://doi.org/10.4135/9781412963909.

Leslie, I. (2016) ‘The scientests who makes apps addictive’, *The Economist*. Available at: https://www.1843magazine.com/features/the-scientists-who-make-apps-addictive.

Leung, L. (2013) ‘Generational differences in content generation in social media: The roles of the gratifications sought and of narcissism’, *Computers in Human Behavior*, 29(3), pp. 997–1006. Available at: https://doi.org/10.1016/j.chb.2012.12.028.

Lewis, K., Kaufman, J. and Christakis, N. (2008) ‘The taste for privacy: An analysis of college student privacy settings in an online social network’, *Journal of Computer-Mediated Communication*, 14(1), pp. 79–100. Available at: https://doi.org/10.1111/j.1083-6101.2008.01432.x.

Lexico.com (2019) *Lexico Powered by the Oxford Dictionary (Behaviour)*. Available at: https://www.lexico.com/en/definition/behaviour (Accessed: 22 March 2019).

Li, X. (2018) ‘Understanding eHealth Literacy From a Privacy Perspective: eHealth Literacy and Digital Privacy Skills in American Disadvantaged Communities’, *American Behavioral Scientist*, 62(10), pp. 1431–1449. Available at: https://doi.org/10.1177/0002764218787019.

Liang, Y. *et al.* (2019) ‘How Effective is Pulse Arrival time for Evaluating Blood Pressure? Challenges and Recommendations from a study using the MIMIC Database’, *Journal of Clinical Medicine*, 8(3). Available at: https://doi.org/10.3390/jcm8030337.

Lin, C.Y. *et al.* (2017) ‘Psychometric validation of the Persian bergen social media addiction scale using classic test theory and Rasch models’, *Journal of Behavioral Addictions*, 6(4), pp. 620–629. Available at: https://doi.org/10.1556/2006.6.2017.071.

Linke, A. and Zerfass, A. (2013a) ‘Social media governance: regulatory frameworks for successful online communications.’, *Journal of Communication Management*, 17(3), pp. 270–286. Available at: https://doi.org/10.1108/JCOM-09-2011-0050.

Linke, A. and Zerfass, A. (2013b) ‘Social media governance: Regulatory frameworks for successful online communications’, *Journal of Communication Management*, 17(3), pp. 270–286. Available at: https://doi.org/10.1108/JCOM-09-2011-0050.

LinkedIn (2016) *Notice of Data Breach: May 2016*, *LinkedIn Support*. Available at: https://www.linkedin.com/help/linkedin/answer/69603/notice-of-data-breach-may-

2016?lang=en (Accessed: 1 November 2020).

Lo, W.H., Lam, B.S.Y. and Cheung, M.M.F. (2021) ‘The Dynamics of Political Elections: A Big Data Analysis of Intermedia Framing Between Social Media and News Media’, *Social Science Computer Review*, 39(4), pp. 627–647. Available at: https://doi.org/10.1177/0894439319876593.

Loos-Sant’Ana, H. and Ferreira De Brito, M.R. (2017) ‘Atitude e Desempenho em Matemática , Crenças Autorreferenciadas e Família : uma path-analysis □ Attitude and Achievement in Mathematics , Self-Beliefs and Family : a path-analysis’, *Bolema, Rio Claro (SP)*, pp. 590–613.

Lucero, M.A., Allen, R.E. and Elzweig, B. (2013) ‘Managing Employee Social Networking: Evolving Views from the National Labor Relations Board’, *Employee Responsibilities and Rights Journal*, 25(3), pp. 143–158. Available at: https://doi.org/10.1007/s10672-012-9211-9.

Luszczynska, A., Scholz, U. and Schwarzer, R. (2005) ‘The General Self-Efficacy Scale: Multicultural Validation Studies’, *The Journal of Psychology*, 139(5), pp. 439–457. Available at: https://doi.org/10.3200/JRLP.139.5.439-457.

Macnamara, J. (2011) ‘Social Media Strategy & Governance: Gaps, risk and opportunities’, *Australian Centre for Public Communication*, p. 30. Available at: http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Social+Media+Strategy+and+Governance:+Gaps+,+risks+and+opportunities#2.

Macnamara, J. *et al.* (2016) ‘“PESO” media strategy shifts to “SOEP”: Opportunities and ethical dilemmas’, *Public Relations Review*, 42(3), pp. 377–385. Available at: https://doi.org/10.1016/j.pubrev.2016.03.001.

Mai, L.M. *et al.* (2015) ‘“i know you’ve seen it!” Individual and social factors for users’ chatting behavior on Facebook’, *Computers in Human Behavior*, 49(March 2019), pp. 296–302. Available at: https://doi.org/10.1016/j.chb.2015.01.074.

Malisetty, S., Rao, C.B.N. and Kumari, K.V. (2018) ‘Exploration of Employees Behaviour and Ethical Climate in IT Industry : Using Exploration of Employees Behaviour and Ethical Climate in IT Industry : Using Ethical Climate Questionnaire (ECQ)’, *OmniScience: A Multi-disciplinary Journal*, 8(1), pp. 8–12.

Malwade, S. *et al.* (2018) ‘Mobile and wearable technologies in healthcare for the ageing population’, *Computer Methods and Programs in Biomedicine*, 161, pp. 233–237. Available at: https://doi.org/10.1016/j.cmpb.2018.04.026.

Mannhardt, F., Petersen, S.A. and Oliveira, M.F. (2019) ‘A trust and privacy framework for smart manufacturing environments’, *Journal of Ambient Intelligence and Smart Environments*, 11(3), pp. 201–219. Available at: https://doi.org/10.3233/AIS-190521.

Marcum, T., Cameron, E. and Versweyveld, L. (2018) ‘Never off the Clock: The Legal Implications of Employees’ after Hours Work’, *Labor Law Journal*, 69(2), p. 73.

Marinos, L. and Lourenço, M. (2018) *ENISA Threat Landscape Report 2018 15 Top Cyberthreats and Trends*, *European Union Agency For Network and Information Security*. Available at: https://doi.org/10.2824/622757.

Martinez, A. (2020) ‘What employers should consider when drafting a social media policy’, *Forbes*, pp. 1–9. Available at: https://www.forbes.com/sites/alonzomartinez/2020/02/06/what-employers-should-consider-when-drafting-a-social-media-policy/?sh=4a11c831d6e1.

Martins, J.T. (2014) *Encyclopedia of Quality of Life and Well-Being Research*. Available at: https://doi.org/10.1007/978-94-007-0753-5.

Masur, P.K. (2020) ‘How online privacy literacy supports self-data protection and self-determination in the age of information’, *Media and Communication*, 8(2), pp. 258–269. Available at: https://doi.org/10.17645/mac.v8i2.2855.

Masur, P.K., Teutsch, D. and Dienlin, T. (2018) ‘Privatheit in der Online-Kommunikation’, in *Springer Reference Social Sciences.* Springer VS, Wiesbaden, pp. 1–29.

Masur, Philipp K, Teutsch, D. and Trepte, S. (2017a) ‘Development and validation of the Online’, *Diagnostica* [Preprint].

Masur, Philipp K, Teutsch, D. and Trepte, S. (2017b) ‘Entwicklung und Validierung der Online-Privatheitskompetenzskala (OPLIS)’, *Diagnostica*, (February), pp. 1–13. Available at: https://doi.org/10.1026/0012-1924/a000179.

Masur, Philipp K., Teutsch, D. and Trepte, S. (2017) ‘Entwicklung und Validierung der Online-Privatheitskompetenzskala (OPLIS)’, *Diagnostica*, pp. 1–13. Available at:

https://doi.org/10.1026/0012-1924/a000179.

Matthes, J. *et al.* (2020) '"Too much to handle": Impact of mobile social networking sites on information overload, depressive symptoms, and well-being', *Computers in Human Behavior*, 105. Available at: https://doi.org/10.1016/j.chb.2019.106217.

Matthews, K. (2019) *How Younger Employees Communicate in the Enterprise*, *informationweek*. Available at: https://www.informationweek.com/strategic-cio/team-building-and-staffing/how-younger-employees-communicate-in-the-enterprise/a/d-id/1335543 (Accessed: 10 October 2019).

Mccarthy-Jones, S. (2018) *The Conversation "Social Networking Sites May Be Controlling Your Mind – Here's How to Take Charge."*, *NeuroscienceNews*. Available at: https://neurosciencenews.com/social-networking-mind-8288/ (Accessed: 26 March 2021).

McCarthy, K. (2017a) *US Senate votes to let broadband ISPs sell your browser histories*, *The Register*. Available at: https://www.theregister.co.uk/2017/03/23/senate_votes_to_let_isps_sell_browser_histories/ (Accessed: 17 July 2017).

McCarthy, K. (2017b) *Your internet history on sale to highest bidder: US Congress votes to shred ISP privacy rules*, *The Register*. Available at: https://www.theregister.co.uk/2017/03/28/congress_approves_sale_of_internet_histories/ (Accessed: 17 July 2017).

Mcquinn, A. and Castro, D. (2019) 'The Costs of an Unnecessarily Stringent Federal Data Privacy Law', *Information Technology & Innovation Foundation* [Preprint], (August). Available at: itif.org.

McSweeney, M.A. (2018) *The Pragmatics of Text Messaging*. 1st edn, *The Pragmatics of Text Messaging*. 1st edn. Routledge Research in Language and Communication. Available at: https://doi.org/10.4324/9781315142340.

Meng, A. (2019) *What is Pinterest and how does it work?*, *infront*. Available at: https://www.infront.com/blog/the-blog/what-is-pinterest-and-how-does-it-work (Accessed: 24 October 2019).

Mennie, P. and Smith, P. (2013) *Social Media Governance Managing social media* *risk*.

Merriam, S.B. and Tisdell, E.J. (2016) *Qualitative Research: A Guide to Design and Implementation*. New York: Wiley.

Meshi, D., Tamir, D.I. and Heekeren, H.R. (2015) ‘The Emerging Neuroscience of Social Media’, *Trends in Cognitive Sciences*, 19(12), pp. 771–782. Available at: https://doi.org/10.1016/j.tics.2015.09.004.

Meule, A. (2019) ‘Contemporary Understanding of Mediation Testing’, *Meta-Psychology*, 3. Available at: https://doi.org/10.15626/mp.2018.870.

Michaelson, V. and Steeves, V. (2020) ‘“I’ll use it differently now”: using dual-systems theory to explore youth engagement with networked technologies’, *Canadian Journal of Public Health* [Preprint]. Available at: https://doi.org/10.17269/s41997-020-00347-w.

Miniard, P.W. and Cohen, J.B. (1981) ‘An examination of the Fishbein-Ajzen behavioral-intentions model’s concepts and measures’, *Journal of Experimental Social Psychology*, 17(3), pp. 309–339. Available at: https://doi.org/10.1016/0022-1031(81)90031-7.

Miranda, A. *et al.* (2019) ‘Parenting stress in mothers of children with autism without intellectual disability. Mediation of behavioral problems and coping strategies’, *Frontiers in Psychology*, 10(MAR), pp. 1–12. Available at: https://doi.org/10.3389/fpsyg.2019.00464.

Mitonga-Monga, J. (2018) ‘Ethical climate influences on employee commitment through job satisfaction in a transport sector industry’, *Journal of Psychology in Africa*, 28(1), pp. 15–20. Available at: https://doi.org/10.1080/14330237.2018.1426710.

Monacis, L. *et al.* (2017) ‘Social networking addiction, attachment style, and validation of the Italian version of the Bergen Social Media Addiction Scale’, *Journal of Behavioral Addictions*, 6(2), pp. 178–186. Available at: https://doi.org/10.1556/2006.6.2017.023.

Montag, C. *et al.* (2019) ‘Addictive Features of Social Media/Messenger Platforms and Freemium Games against the Background of Psychological and Economic Theories’, *International Journal of Environmental Research and Public Health*, 16(14), p. 2612.

Available at: https://doi.org/10.3390/ijerph16142612.

Montiel, I. *et al.* (2020) ‘New Ways of Teaching: Using Technology and Mobile Apps to Educate on Societal Grand Challenges’, *Journal of Business Ethics*, 161(2), pp. 243–251. Available at: https://doi.org/10.1007/s10551-019-04184-x.

Moore, M.M. and Brown, P.M. (2019) ‘The association of self-regulation , habit , and mindfulness with texting while driving’, *Accident Analysis and Prevention*, 123(May 2018), pp. 20–28. Available at: https://doi.org/10.1016/j.aap.2018.10.013.

Moreau, E. (2020) *Facebook Messenger: Everything You Need to Know*, *lifewire*. Available at: https://www.lifewire.com/facebook-messenger-4103719 (Accessed: 12 February 2021).

Morgan, P. (2011) ‘Some ethical and legal considerations in the use of Web 2.0’, in *Using Web 2.0 for Health Information*. Available at: https://doi.org/10.29085/9781856049276.011.

Morrison, K. (2014) *Facebook Auto-Play Videos Are a Data Suck*, *Adweek*. Available at: http://www.adweek.com/digital/facebook-auto-play-videos-data-suck/ (Accessed: 27 June 2017).

Mosseri, A. and Chudnovsky, S. (2020) *Say ? to Messenger: Introducing New Messaging Features for Instagram*, *Facebook*. Available at: https://about.fb.com/news/2020/09/new-messaging-features-for-instagram/.

Mott, N. (2014) *Thanks Facebook- Auto-play videos are eating up 60% more data on some networks*, *Pando*. Available at: https://pando.com/2014/09/04/facebooks-auto-play-videos-are-eating-up-60-more-data-on-some-networks/ (Accessed: 27 June 2017).

Mulaik, S.A. (2009) *Foundations of Factor Analysis (2nd ed.)*. 2nd edn. New York: Chapman and Hall/CRC. Available at: https://doi.org/https://doi.org/10.1201/b15851.

Mullan, K. and Wajcman, J. (2019) ‘Have Mobile Devices Changed Working Patterns in the 21st Century? A Time-diary Analysis of Work Extension in the UK’, *Work, Employment and Society*, 33(1), pp. 3–20. Available at: https://doi.org/10.1177/0950017017730529.

Murdoch, B. (2021) ‘Privacy and artificial intelligence: challenges for protecting health information in a new era', *BMC Medical Ethics*, 22(1), pp. 1–5. Available at: https://doi.org/10.1186/s12910-021-00687-3.

Mwaba, K., Saini, Y. and Abratt, R. (2017) 'Personality and content preferences on social network sites in South Africa', *South African Journal of Business Management*, 48(4), pp. 13–20. Available at: https://doi.org/10.4102/sajbm.v48i4.39.

My HR (2017) *Organizational Awareness*, *Government of Northwest Territories – My HR*. Available at: https://my.hr.gov.nt.ca/competencies/organizational-awareness (Accessed: 12 February 2021).

Naisbitt, J. (1984) *Megatrends: Ten New Directions Transforming Our Lives*. Canada: Wiley Publishing.

Naumovska, L. and Novkovska, B. (2018) 'Mind the gap : Generation Y and Z socio-economic choices Behavioral and Social Science', in *5th International Conference on Research in Behavioral and Social Science*, pp. 70–77.

Negriff, S. and Valente, T.W. (2018) 'Structural characteristics of the online social networks of maltreated youth and offline sexual risk behavior', *Child Abuse and Neglect*, 85(January), pp. 209–219. Available at: https://doi.org/10.1016/j.chiabu.2018.01.033.

Nevin, A.D. and Schieman, S. (2021) 'Technological Tethering, Digital Natives, and Challenges in the Work–Family Interface', *Sociological Quarterly*, 62(1), pp. 60–86. Available at: https://doi.org/10.1080/00380253.2019.1711264.

Nguyen, H.K. (2016) 'Kyosei: A Co-Living Approach in Japanese Culture and Design Practice', *Design Journal*, 19(5), pp. 789–808. Available at: https://doi.org/10.1080/14606925.2016.1206705.

Nguyen, M.H. *et al.* (2022) 'Staying connected while physically apart: Digital communication when face-to-face interactions are limited', *New Media and Society*, 24(9), pp. 2046–2067. Available at: https://doi.org/10.1177/1461444820985442.

Noakes, T.D. (2017) 'Use of social media by health professionals in South Africa', *South African Medical Journal*, 107(9), p. 724. Available at: https://doi.org/10.7196/SAMJ.2017.v107i9.12709.

Notre Dame College (2013) *The Psychology Behind a Grocery Store's Layout*, *Notre*

Dame College Online. Available at: http://online.notredamecollege.edu/psychology/the-psychology-behind-a-grocery-store’s-layout/ (Accessed: 28 June 2017).

Novinson, M. (2019) ‘The 11 Biggest Ransomware Attacks Of 2019’, *Crn.com*, pp. 1–2. Available at: https://www.crn.com/slide-shows/security/the-11-biggest-ransomware-attacks-of-2020-so-far-.

Nunan, D. and Di Domenico, M. (2013) ‘Market research and the ethics of big data’, *International Journal of Market Research*, 55(4), pp. 2–13. Available at: https://doi.org/10.2501/IJMR-2013-015.

Nyahodza, L. and Higgs, R. (2017) ‘Towards bridging the digital divide in post-apartheid South Africa: a case of a historically disadvantaged university in Cape Town’, *South African Journal of Libraries and Information Science*, 83(1), pp. 39–48. Available at: https://doi.org/10.7553/83-1-1645.

Nyangeni, T., Du Rand, S. and Van Rooyen, D. (2015) ‘Perceptions of nursing students regarding responsible use of social media in the Eastern Cape’, *Curationis*, 38(2), p. 1496. Available at: https://doi.org/10.4102/curationis.v38i2.1496.

Nys, T.R. and Engelen, B. (2016) ‘Judging Nudging: Answering the Manipulation Objection’, *Political Studies*, 65(1), pp. 199–214. Available at: https://doi.org/10.1177/0032321716629487.

Nyukorong, R. and Quisenberry, W. (2016) ‘Character Traits Of Effective Executives: A Phenomenological Study Of Ceos In Ghana’, *European Scientific Journal*, 12(20), pp. 1857–7881. Available at: https://doi.org/10.19044/esj.2016.v12n20p69.

O’Brolchain, F. and Gordijn, B. (2015) ‘Ethics of Brain–Computer Interfaces for Enhancement Purposes’, *Handbook of Neuroethics*, pp. 1–1850. Available at: https://doi.org/10.1007/978-94-007-4707-4.

O’Connor, K.W. and Schmidt, G.B. (2015) ‘“Facebook Fired”: Legal Standards for Social Media-Based Terminations of K-12 Public School Teachers’, *SAGE Open*, 5(1), pp. 2158244015575636-. Available at: https://doi.org/10.1177/2158244015575636.

O’Hanlon, B. (2010) *There Is a Fly in the Urinal. Praise for Happiness, Healing, Enhancement*. John Wiley&Sons, Inc., Hoboken, New Jersey. Available at:

http://simbi.kemenag.go.id/pustaka/images/materibuku/happiness-healing-enhancement.pdf#page=323.

Obalade, G.O. and Arogundade, K.K. (2019) ‘Ethical climate and deviant behavior among employees of selected public and private universities: The case of the emerging country’, *Corporate Governance and Organizational Behavior Review*, 3(2), pp. 30–39. Available at: https://doi.org/10.22495/cgobr_v3_i2_p3.

Obar, J.A. and Wildman, S. (2015) *Social Media Definition and the Governance Challenge - An Introduction to the Special Issue*. Available at: https://doi.org/http://dx.doi.org/10.2139/.

OECD (2008) ‘Malicious Software (Malware). A Security Threat to the Internet Economy.’, *DSTI/ICCP/REG(2007)5/FINAL* [Preprint], (2008).

Oeldorf-Hirsch, A. and Obar, J.A. (2019) ‘Overwhelming, Important, Irrelevant’, pp. 166–173. Available at: https://doi.org/10.1145/3328529.3328557.

Office of Human Resources (2019) *External and Organizational Awareness*, *National Institute of Health*. Available at: https://hr.nih.gov/working-nih/competencies/competencies-dictionary/external-and-organizational-awareness (Accessed: 12 February 2021).

Olsen, D.P. (2003) ‘Influence and coercion: Relational and rights-based ethical approaches to forced psychiatric treatment’, *Journal of Psychiatric and Mental Health Nursing*, 10(6), pp. 705–712. Available at: https://doi.org/10.1046/j.1365-2850.2003.00659.x.

Ongeso, J.P. (2022) ‘South Africa: Films and Publications Amendment Act comes into operation’, *Bowmans*, pp. 3–7. Available at: https://bowmanslaw.com/insights/technology-media-and-telecommunications/south-africa-films-and-publications-amendment-act-comes-into-operation/#:~:text=These amendments have been viewed,group characteristics%2C and that constitutes.

Opzeeland, P. van (2017) *The potential of messaging for your online customer relationships*, *Digital Commerce 360*. Available at: https://www.digitalcommerce360.com/2017/05/05/the-potential-of-messaging-for-your-online-customer-relationships/ (Accessed: 23 July 2017).

Orcutt, M. (2016a) *FTC Chairwoman- We Must Not Give Up on Privacy*, *MIT Technology Review*. Available at: https://www.technologyreview.com/s/602474/ftc-chairwoman-we-must-not-give-up-on-privacy/ (Accessed: 12 October 2016).

Orcutt, M. (2016b) ‘The Next President Will Inherit America’s Embarrassing Digital Divide’. MIT Technology Review. Available at: https://www.technologyreview.com/s/602393/the-next-president-will-inherit-americas-embarrassing-digital-divide/ (Accessed: 12 October 2016).

Osatuyi, B. and Turel, O. (2018a) ‘Tug of war between social self-regulation and habit: Explaining the experience of momentary social media addiction symptoms’, *Computers in Human Behavior*, 85, pp. 95–105. Available at: https://doi.org/10.1016/j.chb.2018.03.037.

Osatuyi, B. and Turel, O. (2018b) ‘Tug of war between social self-regulation and habit: Explaining the experience of momentary social media addiction symptoms’, *Computers in Human Behavior*, 85. Available at: https://doi.org/Tug of war between social self-regulation and habit: Explaining the experience of momentary social media addiction symptoms.

Ose, S.O. (2016) ‘Using Excel and Word to Structure Qualitative Data’, *Journal of Applied Social Science*, 10(2), pp. 147–162. Available at: https://doi.org/10.1177/1936724416664948.

Overton, M. (no date) ‘Rootkits: Risks, Issues and Prevention.’, *Source*, pp. 1–26.

Oviedo-Trespalacios, O. *et al.* (2019) ‘Problematic use of mobile phones in Australia…is it getting worse?’, *Frontiers in Psychiatry*, 10(March). Available at: https://doi.org/10.3389/fpsyt.2019.00105.

Pagliaro, S. *et al.* (2018) ‘On the effects of ethical climate(s) on employees’ behavior: A social identity approach’, *Frontiers in Psychology*, 9(JUN), pp. 1–10. Available at: https://doi.org/10.3389/fpsyg.2018.00960.

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J.P. and Duan N., & Hoagwood, K. (2013) ‘Purposeful Sampling for Qualitative Data Collection and Analysis in Mixed Method Implementation Research Purposeful Sampling for Qualitative Data Collection and Analysis’, *Springer Science Business Media*, (November 2013), pp. 1–13.

Available at: https://doi.org/DOI 10.1007/s10488-013-0528-y.

Paliwal, B. (2022) ‘Social Media: New Challenges and Opportunities for Corporate Governance’, *Law Audience Journal (e-ISSN:*, 4(1), pp. 192–205. Available at: https://www.lawaudience.com/social-media-new-challenges-and-opportunities-for-corporate-governance/.

Pallant, J. (2020) *SPSS Survival Manual A Step by Step Guide to Data Analysis Using IBM SPSS*. 7th Editio. London: Routledge/Taylor & Francis Group. Available at: https://doi.org/https://doi.org/10.4324/9781003117452.

Papakonstantinou, E. *et al.* (2022) ‘The medical cyborg concept.’, *EMBnet.journal*, 27, p. e1005. Available at: https://doi.org/10.14806/ej.27.0.1005.

Park, H. and Blenkinsopp, J. (2011) ‘The roles of transparency and trust in the relationship between corruption and citizen satisfaction’, *International Review of Administrative Sciences*, 77(2), pp. 254–274. Available at: https://doi.org/10.1177/0020852311399230.

Park, H., Blenkinsopp, J. and Park, M. (2014) ‘The Influence of an Observer’s Value Orientation and Personality Type on Attitudes Toward Whistleblowing’, *Journal of Business Ethics*, 120(1), pp. 121–129. Available at: https://doi.org/10.1007/s10551-013-1908-7.

Park, Y.J. (2013) ‘Digital Literacy and Privacy Behavior Online’, *Communication Research*, 40(2), pp. 215–236. Available at: https://doi.org/10.1177/0093650211418338.

Park, Y.J. (2015) ‘Do men and women differ in privacy? Gendered privacy and (in)equality in the Internet’, *Computers in Human Behavior*, 50, pp. 252–258. Available at: https://doi.org/10.1016/j.chb.2015.04.011.

Park, Y.J. and Mo Jang, S. (2014) ‘Understanding privacy knowledge and skill in mobile communication’, *Computers in Human Behavior*, 38, pp. 296–303. Available at: https://doi.org/10.1016/j.chb.2014.05.041.

Parsons, K. *et al.* (2019) ‘Predicting susceptibility to social influence in phishing emails’, *International Journal of Human Computer Studies*, 128(February), pp. 17–26. Available at: https://doi.org/10.1016/j.ijhcs.2019.02.007.

Patten, B.Y.E. and Perrin, A. (2015) *Who ' s left out in a Web-only survey and how it affects results*, *Pew Research Center*. Available at: http://www.pewresearch.org/fact-tank/2015/09/22/who-s-left-out-in-a-web-only-survey-and-how-it-affects-results/ (Accessed: 12 September 2016).

Patton, M. (2002) *Twelve major characteristics of qualitative research*. 3rd edn, *Qualitative Research and Evaluation Methods*. 3rd edn. Sage Publications.

Piazza, A.J. *et al.* (2019) 'Mobile device use while crossing the street: Utilizing the theory of planned behavior', *Accident Analysis and Prevention*, 127(February), pp. 9–18. Available at: https://doi.org/10.1016/j.aap.2019.02.006.

Pinder, C. *et al.* (2018) 'Digital behaviour change interventions to break and form habits', *ACM Transactions on Computer-Human Interaction*, 25(3). Available at: https://doi.org/10.1145/3196830.

Pino, I. and Zafra, J.L. (2019) 'Radical transparency: how to make the most of technology and boost stakeholder dialogue', *Developing Ideas from LLORENTE & CUENCA* [Preprint].

Pinola, M. (2019) *Lifewire.com*. Available at: https://www.lifewire.com/social-networking-strategies-for-personal-and-professional-use-2378017 (Accessed: 1 July 2019).

Plano Clark, V.L. (2019) 'Meaningful integration within mixed methods studies: Identifying why, what, when, and how', *Contemporary Educational Psychology*, 57, pp. 106–111. Available at: https://doi.org/10.1016/j.cedpsych.2019.01.007.

Porumbescu, G.A. (2015) 'Using Transparency to Enhance Responsiveness and Trust in Local Government: Can It Work?', *State and Local Government Review*, 47(3), pp. 205–213. Available at: https://doi.org/10.1177/0160323X15599427.

Porumbescu, G.A. *et al.* (2019) 'Does transparency lead to pay compression?', *Papers 6, TAD 14 The disciplines and the study of Public Administration: Transatlantic perspectives in the margin of the 14th Administration and Public Management International Conference, Bucharest, June 6-18 2018*, 125(5), pp. 1683–1721. Available at: https://doi.org/10.1086/693137.

Porumbescu, G.A., Cucciniello, M. and Gil-Garcia, J.R. (2020) 'Accounting for citizens when explaining open government effectiveness', *Government Information Quarterly*, 37(2), p. 101451. Available at: https://doi.org/10.1016/j.giq.2019.101451.

Pourkhani, A. *et al.* (2019) 'The impact of social media in business growth and performance: A scientometrics analysis', *International Journal of Data and Network Science*, 3(3), pp. 223–244. Available at: https://doi.org/10.5267/j.ijdns.2019.2.003.

Prat, M. (2014) *Sales Negotiations in Professional Service Firms: An Exploratory Study on Agenda Setting and Issue Management*. Springer Science & Business Media. Available at: https://doi.org/10.1007/978-3-658-04499-2.

Prensky, M. (2001) 'Digital Natives, Digital Immigrants Part 1', *On the Horizon*, 9(5), pp. 1–6. Available at: https://doi.org/10.1108/10748120110424816.

Price, G. and van der Walt, A.J. (2013) 'Changes in Attitudes Towards Business Ethics Held by Former South African Business Management Students', *Journal of Business Ethics*, 113(3), pp. 429–440. Available at: https://doi.org/10.1007/s10551-012-1314-6.

Price, R. (2019) 'Facebook says it "unintentionall y uploaded" 1.5 million people's email contacts without their consent', *Business Insider US*, pp. 1–8.

Qibtiyah, M. and Beriansyah, A. (2019) 'Instagram and Political Education for Net Generation in Indonesia Study on the Usage of Instagram for Political Education in Palembang City', (ICoCSPA 2018), pp. 205–210. Available at: https://doi.org/10.5220/0008819102050210.

Queenie, W. (2019) 'Millions of Facebook user phone numbers exposed online, security researchers say - CNET', *CNET*, pp. 1–5. Available at: https://www.cnet.com/news/millions-of-facebook-user-phone-numbers-exposed-online-security-researchers-say/.

Rajab, J.M., MatJafri, M.Z. and Lim, H.S. (2013) 'Combining multiple regression and principal component analysis for accurate predictions for column ozone in Peninsular Malaysia', *Atmospheric Environment*, 71, pp. 36–43. Available at: https://doi.org/10.1016/j.atmosenv.2013.01.019.

Ramokapane, K.M., Mazeli, A.C. and Rashid, A. (2019) 'Skip, Skip, Skip, Accept!!!: A Study on the Usability of Smartphone Manufacturer Provided Default Features and User Privacy', *Proceedings on Privacy Enhancing Technologies*, 2019(2), pp. 209–

227. Available at: https://doi.org/10.2478/popets-2019-0027.

Rascão, J.P. (2020) ‘Freedom of Expression, Privacy, and Ethical and Social Responsibility in Democracy in the Digital Age’, *International Journal of Business Strategy and Automation*, 1(3), pp. 1–23. Available at: https://doi.org/10.4018/ijbsa.2020070101.

Rawlins, B. (2008a) ‘Give the Emperor a Mirror: Toward Developing a Stakeholder Measurement of Organizational Transparency’, *Journal of Public Relations Research*, 21(1), pp. 71–99. Available at: https://doi.org/10.1080/10627260802153421.

Rawlins, B. (2008b) ‘Measuring the relationship between organizational transparency and trust’, *Public relations Journal*, 2(2), pp. 1–21. Available at: http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Measuring+the+relationship+between+organizational+transparency+and+employee+trust+.#0.

Raz, J. (1986) *The Morality of Freedom*. Clarendon Press.

Regina, A.A. *et al.* (2017) ‘Behavioral Patterns on WhatsApp’, *International Review of Management and Business Research*, 6(2), pp. 385–400.

Remišová, A., Lašáková, A. and Kirchmayer, Z. (2019) ‘Influence of Formal Ethics Program Components on Managerial Ethical Behavior’, *Journal of Business Ethics*, 160(1), pp. 151–166. Available at: https://doi.org/10.1007/s10551-018-3832-3.

Renaud, K. and Zimmermann, V. (2018) ‘Ethical guidelines for nudging in information security & privacy’, *International Journal of Human Computer Studies*, 120. Available at: https://doi.org/10.1016/j.ijhcs.2018.05.011.

Richey, M., Gonibeed, A. and Ravishankar, M.N. (2018) ‘The Perils and Promises of Self-Disclosure on Social Media’, *Information Systems Frontiers*, 20(3), pp. 425–437. Available at: https://doi.org/10.1007/s10796-017-9806-7.

Richter, F. (2019) *Pinterest Hits 300 Million User Milestone*, *Statista*. Available at: https://www.statista.com/chart/17642/monthly-active-users-of-pinterest/ Privacy (Accessed: 17 October 2019).

Ringel, L. (2019) ‘Unpacking the Transparency-Secrecy Nexus: Frontstage and backstage behaviour in a political party’, *Organization Studies*, 40(5), pp. 705–723. Available at: https://doi.org/10.1177/0170840618759817.

Robert F. Devellis (2003) *Scale Development Theory and Applications Second Edition*. 2nd edn. Sage Publications.

Roberts, A. (2012) ‘WikiLeaks: The illusion of transparency’, *International Review of Administrative Sciences*, 78(1), pp. 116–133. Available at: https://doi.org/10.1177/0020852311429428.

Robertson, V.H.S.E. (2020) ‘Excessive data collection: Privacy considerations and abuse of dominance in the era of big data’, *Common Market Law Review*, 57(1), pp. 161–190. Available at: https://kluwerlawonline.com/journalarticle/Common+Market+Law+Review/57.1/COLA2020006.

Robinson, J.P., Shaver, P.R. and Wrightsman, L.S. (2013) ‘Criteria for Scale Selection and Evaluation’, *Measures of Personality and Social Psychological Attitudes*, pp. 1–16. Available at: https://doi.org/10.1016/b978-0-12-590241-0.50005-8.

Robinson, M.T. (2016) *The Generations (sm- dm) Which Generation are You?*, *Career Planner.com*. Available at: https://www.google.co.za/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#q=generation z years (Accessed: 14 September 2016).

Rockwell, T. (2013) ‘Where should we look for mental representations? On the need for epistemic ethics.’, *Accountability in research*, 20(1), pp. 42–56. Available at: https://doi.org/10.1080/08989621.2013.749746.

Rodriguez, S.N. and Loos-Sant’Ana, H. (2015) ‘JOLLAS Self-concept , self-esteem and self-efficacy : The role of self-beliefs in the coping process of socially vulnerable adolescents’, *Journal of Latino/Latin American Studies* [Preprint], (September). Available at: https://doi.org/10.18085/1549-9502-7.1.33.

Roller, M.R. and Lavrakas, P.J. (2015) *Applied Qualitative Research Design*. 1st edn. Guilford Press.

Ronson, J. (2015) *How One Stupid Tweet Blew Up Justine Sacco’s Life*, *The News York Times Magazine*. Available at: http://www.nytimes.com/2015/02/15/magazine/how-one-stupid-tweet-ruined-justine-saccos-life.html?_r=0 (Accessed: 16 October 2016).

Rosen, L. (2010) *Rewired: Understanding the iGeneration and the way they learn*. Macmillan.

Rosen, L. and Samuel, A. (2015) 'Conquering digital distraction', *Harvard Business Review*, 2015(June).

Rosen, L.D. *et al.* (2013) 'Is Facebook creating "iDisorders"? The link between clinical symptoms of psychiatric disorders and technology use, attitudes and anxiety', *Computers in Human Behavior*, 29(3), pp. 1243–1254. Available at: https://doi.org/10.1016/j.chb.2012.11.012.

Rosen, L.P.D. (2014) *Our Social Media Obsession What is driving people to constantly check in with social media?*, *psychology today*. Available at: https://www.psychologytoday.com/blog/rewired-the-psychology-technology/201407/our-social-media-obsession (Accessed: 7 September 2016).

Rosenberg, M. (1965) *Society and the adolescent self-image*. Princeton, NJ: Princeton University Press.

Rosenthal, S. *et al.* (2019) 'A tripartite model of trust in Facebook: acceptance of information personalization, privacy concern, and privacy literacy', *Media Psychology*, 0(0), pp. 1–25. Available at: https://doi.org/10.1080/15213269.2019.1648218.

Rost, M. *et al.* (2016) 'Forget-me-not: History-less mobile messaging', *Conference on Human Factors in Computing Systems - Proceedings*, pp. 1904–1908. Available at: https://doi.org/10.1145/2858036.2858347.

Roy, M. *et al.* (2020) 'Ebola and Localized Blame on Social Media: Analysis of Twitter and Facebook Conversations During the 2014–2015 Ebola Epidemic', *Culture, Medicine and Psychiatry*, 44(1), pp. 56–79. Available at: https://doi.org/10.1007/s11013-019-09635-8.

Ruiz, S.L. and Stadtlander, L. (2015) 'Social Media as Support for Partners of Veterans With Posttraumatic Stress Disorder Partners of Veterans With PTSD', 9(1), pp. 1–18. Available at: https://doi.org/10.5590/JSBHS.2015.09.1.01.

Sætra, H.S. (2019) 'When nudge comes to shove: Liberty and nudging in the era of big data', *Technology in Society*, 59(February), p. 101130. Available at: https://doi.org/10.1016/j.techsoc.2019.04.006.

Sample, I. (2017) ‘Nudge theory: the psychology and ethics of persuasion - Science Weekly podcast’, *The Guardian*. Available at: https://www.theguardian.com/science/audio/2017/feb/22/nudge-theory-the-psychology-and-ethics-of-persuasion-science-weekly-podcast (Accessed: 17 June 2017).

Samuels, P. (2016) ‘Advice on Exploratory Factor Analysis’. Available at: https://doi.org/10.13140/RG.2.1.5013.9766.

Saridakis, G. *et al.* (2016) ‘Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users’, *Technological Forecasting and Social Change*, 102, pp. 320–330. Available at: https://doi.org/10.1016/j.techfore.2015.08.012.

Saris, W.E. and Gallhofer, I.N. (2007) *Design, Evaluation, and Analysis of Questionnaires for Survey Research*. John Wiley & Sons. Available at: https://books.google.co.za/books?id=HklIg49p_iwC&dq=The+art+of+Designing+a+questionnaire&lr=&source=gbs_navlinks_s.

Saunders, M., Lewis, P. and Thornhill, A. (2019) *Chapter 4: Understanding research philosophy and approaches to theory development*, *Research Methods for Business Students*.

Savić, N. *et al.* (2023) ‘“The Preliminary Validation of the Fogg Behavior Model (B= MAP) in Hypothetical Informal Educational Context.”’, in *EMPIRICAL STUDIES IN PSYCHOLOGY*, p. 60.

Sawaya, Y. *et al.* (2017) ‘Self-Confidence Trumps Knowledge: A Cross-Cultural Study of Security Behavior’, pp. 2202–2214. Available at: https://doi.org/10.1145/3025453.3025926.

Sawers, P. (2016) ‘Following Google, Microsoft expands right-to-be-forgotten filtering for Bing in Europe’. VentureBeat. Available at: http://venturebeat.com/2016/08/12/following-google-microsoft-expands-right-to-be-forgotten-filtering-for-bing-in-europe/ (Accessed: 16 October 2016).

Schaefer, M.W. (2016) ‘What Marketers Need to Know About Chat Apps’, *Harvard Business Review* [Preprint].

Schermelleh-Engel, K., Moosbrugger, H. and Müller, H. (2003) ‘Evaluating the fit of structural equation models: Tests of significance and descriptive goodness-of-fit measures’, *MPR-online*, 8(May), pp. 23–74.

Schleifer, P., Fiorini, M. and Auld, G. (2019) ‘Transparency in transnational governance: The determinants of information disclosure of voluntary sustainability programs’, *Regulation and Governance*, 13(4), pp. 488–506. Available at: https://doi.org/10.1111/rego.12241.

Schmidt, A.T. and Engelen, B. (2020) ‘The ethics of nudging: An overview’, *Philosophy Compass*, 15(4), pp. 1–13. Available at: https://doi.org/10.1111/phc3.12658.

Schmitz, S., Boothroyd, R. and Garland, P. (2012) *UK : Social Media Governance : Tips for In- House Counsel*.

Schneider, R.A. and A. (2017) ‘An App for Every Step – A psychological perspective on interoperability of Mobile Messenger Apps’, in *28th European Regional Conference of the International Telecommunications Society (ITS): ‘Competition and Regulation in the Information Age’, Passau, Germany, 30th July - 2nd August, 2017, International Telecommunications Society (ITS), Calgary*. Available at: http://hdl.handle.net/10419/169444%0AStandard-Nutzungsbedingungen:

Schober, P. and Schwarte, L.A. (2018) ‘Correlation coefficients: Appropriate use and interpretation’, *Anesthesia and Analgesia*, 126(5), pp. 1763–1768. Available at: https://doi.org/10.1213/ANE.0000000000002864.

Schwarzer, R. and Jerusalem, M. (1995) ‘General Self-Efficacy Scale (GES)’, in *J. Weinman, S. Wright, & M. Johnston, Measures in health psychology: A user’s portfolio. Causal and control beliefs*, pp. 35–37. Available at: http://userpage.fu-berlin.de/~health/engscal.htm.

Schwarzer, R. and Jerusalem, M. (2013) ‘Instrument Title: General Self-Efficacy Scale (GSE) General Self-Efficacy Scale but were afraid to ask’, pp. 35–37. Available at: https://doi.org/http://dx.doi.org/10.13072/midss.488.

Schwarzer, R. and Warner, L.M. (2013) ‘Perceived Self-Efficacy and Its Relationship to Resilience Conceptual Issues’, in *Prince-Embury S., Saklofske D. (eds) Resilience in Children, Adolescents, and Adults.* New York, NY: Springer. Available at:

https://doi.org/10.1007/978-1-4614-4939-3.

Scott, N. (2016) 'Digital Love : Where Does the Marital Communications Privilege Fit in the World of DIGITAL LOVE : WHERE DOES THE', *The John Marshall Journal of Information Technology & Privacy Law*, 32(2).

Scroxton, A. (2020) 'Surge in Ryuk ransomware attacks has hospitals on alert Russian', *Computer Weekly*, pp. 1–5. Available at: https://www.computerweekly.com/news/252491324/Surge-in-Ryuk-ransomware-attacks-has-hospitals-on-alert Privacy.

Semantha, F.H. *et al.* (2020) 'A systematic literature review on privacy by design in the healthcare sector', *Electronics (Switzerland)*, 9(3), pp. 1–27. Available at: https://doi.org/10.3390/electronics9030452.

Shacklock, A., Manning, M. and Hort, L. (2011) 'Dimensions and Types of Ethical Climate within Public Sector Human Resource Management', *Journal of New Business Ideas & Trends*, 9(1), pp. 51–66. Available at: http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=64151149&site=ehost-live&scope=site.

Shah, A. (2019) *How to Use Social Proof in Your Marketing Why Include Social Proof in Your Social Media Marketing ?*, *Social Media Examiner*. Available at: https://www.socialmediaexaminer.com/how-to-use-social-proof-marketing/ (Accessed: 19 October 2019).

Shah, R. *et al.* (2019) 'How accessible are you? A hospital-wide audit of the accessibility and professionalism of Facebook profiles', *British Dental Journal*, 226(11), pp. 878–882. Available at: https://doi.org/10.1038/s41415-019-0363-y.

Sheppard, M. and Vibert, C. (2019) 'Re-examining the relationship between ease of use and usefulness for the net generation', *Education and Information Technologies* [Preprint].

Showers, C.J. and Zeigler-hill, V. (2015) 'Self-Concept Structure and the Quality of Self-Knowledge', *Journal of personality*, 83(5), pp. 535–551. Available at: https://doi.org/10.1111/jopy.12130.Self-Concept.

Sievert, H. and Scholz, C. (2017) 'Engaging employees in (at least partly) disengaged companies. Results of an interview survey within about 500 German corporations on the growing importance of digital engagement via internal social media', *Public Relations Review*, 43(5), pp. 894–903. Available at: https://doi.org/10.1016/j.pubrev.2017.06.001.

Sifry, M.. (2011) *WikiLeaks and the Age of Transparency*. OR Books.

Sivarajah, U., Irani, Z. and Weerakkody, V. (2015) 'Evaluating the use and impact of Web 2.0 technologies in local government', *Government Information Quarterly*, 32(4), pp. 473–487. Available at: https://doi.org/10.1016/j.giq.2015.06.004.

Skinner, B.F. (1957) 'The experimental analysis of behavior', *American Scientist*, 45(4), pp. 343–371.

Small, C. and Lew, C. (2021) 'Mindfulness, Moral Reasoning and Responsibility: Towards Virtue in Ethical Decision-Making', *Journal of Business Ethics*, 169(1), pp. 103–117. Available at: https://doi.org/10.1007/s10551-019-04272-y.

Smith, A., Anderson, M. (2018) *Social Media Use in 2018*, *Pew Research Center, Inc.* Available at: https://doi.org/10.1201/b18431-6.

Smith, C. (2019) *110 Amazing WeChat Statistics and Facts (2019) | By the Numbers*, *DMR Publisher*. Available at: https://expandedramblings.com/index.php/wechat-statistics/ (Accessed: 16 October 2019).

Snail ka Mtuze, S. and Musoni, M. (2023) 'An overview of cybercrime law in South Africa', *International Cybersecurity Law Review*, 4(3), pp. 299–323. Available at: https://doi.org/10.1365/s43439-023-00089-8.

Social Networking (2017) *7 Online Psychological Tricks People Use To Manipulate On Facebook*, *Sexy Social Media*. Available at: http://www.sexysocialmedia.com/7-online-psychological-tricks-people-use-to-manipulate-on-facebook/ (Accessed: 10 June 2017).

Soga, L.R. *et al.* (2020) 'Web 2.0-enabled team relationships: an actor-network perspective', *European Journal of Work and Organizational Psychology*, 00(00), pp. 1–14. Available at: https://doi.org/10.1080/1359432X.2020.1847183.

Soror, A.A. *et al.* (2015) 'Good habits gone bad: Explaining negative consequences associated with the use of mobile phones from a dual-systems perspective', *Information Systems Journal*, 25(4), pp. 403–427. Available at: https://doi.org/10.1111/isj.12065.

Spectrm (2020) *Messaging Apps Have Taken Over | Usage & Growth Statistics*, *Spectrm.io*. Available at: https://spectrm.io/insights/blog/messaging-app-statistics-most-popular-communication-method-2020/ (Accessed: 28 April 2021).

Spooner, S. (2016) ‘Africa’s great digital divide: you’re more likely to have access to the internet as a wealthy man in a coastal country’. Available at: http://mgafrica.com/article/2016-04-29-africa-connectivity (Accessed: 12 October 2016).

Stamati, T., Papadopoulos, T. and Anagnostopoulos, D. (2015) ‘Social media for openness and accountability in the public sector: Cases in the greek context’, *Government Information Quarterly*, 32(1), pp. 12–29. Available at: https://doi.org/10.1016/j.giq.2014.11.004.

Statista (2021a) *Labor force distribution in the U . S . in 2017 , by generation This statistic shows the distribution of the labor force in the United States in 2017 , by generation . In 2017 , the greatest share of the labor force was made up of the Millennial generatio*. Available at: https://www.statista.com/statistics/801903/labor-force-composition-by-generation-us/.

Statista (2021b) *Most popular social networks worldwide as of July 2021, ranked by number of active users*, *Statista*.

Strachan, W. (2015) *6 THINGS YOUR SOCIAL MEDIA POLICY*, *werksmans*. Available at: https://www.werksmans.com/wp-content/uploads/2015/12/044339-WERKSMANS-dec-social-media-policy.pdf (Accessed: 4 February 2022).

Suciu, P. (2020) ‘There Isn’t Enough Privacy On Social Media And That Is A Real Problem’, *Forbes*, pp. 26–29. Available at: https://www.forbes.com/sites/petersuciu/2020/06/26/there-isnt-enough-privacy-on-social-media-and-that-is-a-real-problem/?sh=459785c44f11.

Sultan, A.J. (2014) ‘Addiction to mobile text messaging applications is nothing to “lol” about’, *Social Science Journal*, 51(1), pp. 57–69. Available at: https://doi.org/10.1016/j.soscij.2013.09.003.

Sunday Independent (2019) ‘South Africans divided on Adam Catzavelos ’ R150K apology’, *Sunday Independent*, pp. 1–5. Available at: https://www.iol.co.za/sundayindependent/news/south-africans-divided-on-adam-catzavelos-r150k-apology-31480037.

Sunstein, C.R. (2013) ‘Very preliminary draft 8/1/13 All rights reserved Is Deontology A Heuristic? On Psychology, Neuroscience, Ethics, and Law Cass R. Sunstein *’, *SSRN*, 2013(2011), pp. 1–18. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2304760.

Sunstein, C.R. (2016) ‘Fifty Shades of Manipulation’, *Journal of Marketing Behavior*, 1(3–4), pp. 214–244. Available at: https://doi.org/10.1561/107.00000014.

Swerling, J., Thorson, K. and Zerfass, A. (2014) ‘The role and status of communication practice in the USA and Europe’, *Journal of Communication Management*, pp. 2–15. Available at: https://doi.org/10.1108/JCOM-04-2013-0037.

Synodinos, N.E. (2003) ‘The “art” of questionnaire construction: some important considerations for manufacturing studies’, *Integrated Manufacturing Systems*, 14(3), pp. 221–237. Available at: https://doi.org/10.1108/09576060310463172.

Tabaka, M. (2017) *Here’s What’s Possibly Causing Your Smartphone Separation Anxiety*, *Inc.com*. Available at: https://www.inc.com/marla-tabaka/brain-hacking-why-you-have-smartphone-separation-anxiety.html (Accessed: 20 May 2017).

Takavarasha, S., Cilliers, L. and Chinyamurindi, W. (2018) ‘Navigating the unbeaten track from digital literacy to digital citizenship: A case of university students in South Africa’s Eastern Cape province’, *Reading & Writing*, 9(1), pp. 1–15. Available at: https://doi.org/10.4102/rw.v9i1.187.

Tang, S., Holmes, V. and Foley, T. (2020) ‘Ethical Climate , Job Satisfaction and Wellbeing : Observations from an Empirical Study of New’, *Georgetown Journal of Legal Ethics, Forthcoming*, pp. 1035–1068.

Tankovska, H. (2021) *Global social networks ranked by number of users 2021*, *Statista*. Available at: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ (Accessed: 28 April 2021).

Tapscott, D. (1998) *Growing Up Digital: The Rise of the Net Generation*. New York, NY: McGraw-Hill.

Tapscott, D. (2009) *Grown up digital: How the Net Generation is changing your world.* Mc Graw Hill.

Tapscott, D. and Ticoll, D. (2012) *The Naked Corporation: How the Age of Transparency Will Revolutionize Business*. Viking Canada.

Tarafdar, M. *et al.* (2015) ‘The Dark Side of Technology’, *MIT Sloan Management Review*, 56(2), pp. 600–623. Available at: http://sloanreview.mit.edu/article/the-dark-side-of-information-technology/?use_credit=de6eebf320b3847ebe4a8feb659fe440.

Taylor, D.G. (2019) ‘Social Media Usage, FOMO, and Conspicuous Consumption: An Exploratory Study: An Abstract’, *In: Rossi P., Krey N. (eds) Finding New Ways to Engage and Satisfy Global Customers. AMSWMC 2018. Developments in Marketing Science: Proceedings of the Academy of Marketing Science. Springer, Cham*, (02 April), pp. 23–24. Available at: https://doi.org/10.1007/978-3-030-02568-7.

Taylor, E.Z. and Curtis, M.B. (2018) ‘Mentoring: A Path to Prosocial Behavior’, *Journal of Business Ethics*, 152(4), pp. 1133–1148. Available at: https://doi.org/10.1007/s10551-016-3325-1.

tech2 News Staff (2017) *Court accepts double blue ticks on WhatsApp as proof of receipt of legal notice*, *Tech2*. Available at: http://tech.firstpost.com/news-analysis/court-accepts-double-blue-ticks-on-whatsapp-as-proof-of-receipt-of-legal-notice-376913.html (Accessed: 27 June 2017).

Tejedo-Romero, F. and Araujo, J.F.F.E. (2020) ‘E-government-enabled transparency: The effect of electoral aspects and citizen’s access to Internet on information disclosure’, *Journal of Information Technology & Politics*, 17(3), pp. 268–290. Available at: https://doi.org/10.1080/19331681.2020.1713958.

Teresi, M. *et al.* (2019) ‘Ethical climate(s), organizational identification, and employees’ behavior’, *Frontiers in Psychology*, 10(June). Available at: https://doi.org/10.3389/fpsyg.2019.01356.

Terkan, R. and Celebi, S.I. (2020) ‘How Whatsapp Changes the Way Business Work?’, *International Review of Management and Marketing*, 10(5), pp. 179–184. Available at: https://doi.org/10.32479/irmm.10769.

Thaler, R.H. and Sunstein, C.R. (2008) *Nudge: Improving Decisions About Health, Wealth, And Happiness.* New Haven : Yale University Press.

Thilakarathne, N.N. (2020) ‘Security and Privacy Issues in IoT Environment’, *International Journal of Engineering and Management Research*, 10(01), pp. 26–29. Available at: https://doi.org/10.31033/ijemr.10.1.5.

Thompson, C. (2007) ‘The See-Through CEO’, *Wired Magazine*. Available at: https://www.wired.com/2007/04/wired40-ceo/.

Thompson, C. (2011) ‘How Khan Academy Is Changing the Rules of Education’, *Wired Magazine*, pp. 1–18. Available at: https://www.wired.com/2011/07/ff_khan/.

Thompson, N. (2019) ‘Tristan Harris: Tech Is “Downgrading Humans.” It’s Time to Fight Back’, *Wired*, pp. 1–14. Available at: https://www.wired.com/story/tristan-harris-tech-is-downgrading-humans-time-to-fight-back/.

Tourangeau, R., Rips, L.J. and Rasinski, K. (2000) *The Psychology of Survey Response*. Cambridge University Press.

Towner, E.B., Everett, H.L. and Klemz, B.R. (2019) ‘Not So Different? Student and Professional Perceptions of Mobile Phone Etiquette in Meetings’, *Business and Professional Communication Quarterly* [Preprint]. Available at: https://doi.org/10.1177/2329490619836452.

Tracy, S.J. (2010) ‘Qualitative quality: Eight “big-tent” criteria for excellent qualitative research’, *Qualitative Inquiry*, 16(10), pp. 837–851. Available at: https://doi.org/10.1177/1077800410383121.

Tracy, S.J. (2013) *Qualitative research methods: Collecting evidence, crafting analysis, creating impact*. Available at: https://doi.org/10.5613/rzs.43.1.6.

Trepte, S. *et al.* (2015) ‘Do people know about privacy and data protection strategies? Towards the “online privacy literacy scale” (OPLIS)’, in *In Reforming European data protection law*, pp. 333–365. Available at: https://doi.org/10.1007/978-94-017-9385-8.

Trepte, S. (2020) ‘The Social Media Privacy Model: Privacy and Communication in the Light of Social Media Affordances’, *Communication Theory* [Preprint], (May 2020). Available at: https://doi.org/10.1093/ct/qtz035.

Treviño, L.K. and Brown, M.E. (2004) 'Managing to be ethical: Debunking five business ethics myths', *Academy of Management Executive*, 18(2), pp. 69–81. Available at: https://doi.org/10.5465/AME.2004.13837400.

Trevino, L.K. and Nelson, K.A. (2017) *Managing business ethics: Straight talk about how to do it right*. 7th edn. New York: John Wiley & Sons.

Trinkle, B. and Crossler, R. (2014) 'Voluntary Disclosures via Social Media and the Role of Comments', *Working Paper*, 29(3), p. Mississippi State University. Available at: https://doi.org/10.2308/isys-51133.

Troshani, I. and Wickramasinghe, Nilmini (2018) 'Contemporary Developments in e-Health', in N Wickramasinghe and J. Schaffer (eds) *Theories to Inform Superior Health Informatics Research and Practice.*, pp. 391–401. Available at: https://doi.org/10.1007/978-3-319-72287-0_24.

Tsay-Vogel, M., Shanahan, J. and Signorielli, N. (2018) 'Social media cultivating perceptions of privacy: A 5-year analysis of privacy attitudes and self-disclosure behaviors among Facebook users', *New Media and Society*, 20(1), pp. 141–161. Available at: https://doi.org/10.1177/1461444816660731.

Turel, O. and Bechara, A. (2016) 'A triadic reflective-impulsive-interoceptive awareness model of general and impulsive information system use: Behavioral tests of neuro-cognitive theory', *Frontiers in Psychology*, 7(APR), pp. 1–11. Available at: https://doi.org/10.3389/fpsyg.2016.00601.

Turel, O. and Bechara, A. (2017) 'Effects of motor impulsivity and sleep quality on swearing, interpersonally deviant and disadvantageous behaviors on online social networking sites', *Personality and Individual Differences*, 108, pp. 91–97. Available at: https://doi.org/10.1016/j.paid.2016.12.005.

Turel, O. and Qahri-Saremi, H. (2016) 'Problematic Use of Social Networking Sites: Antecedents and Consequence from a Dual-System Theory Perspective', *Journal of Management Information Systems*, 33(4), pp. 1087–1116. Available at: https://doi.org/10.1080/07421222.2016.1267529.

Turel, O. and Serenko, A. (2020a) 'Cognitive biases and excessive use of social media: The facebook implicit associations test (FIAT)', *Addictive Behaviors*, 105, p.

106328. Available at: https://doi.org/10.1016/j.addbeh.2020.106328.

Turel, O. and Serenko, A. (2020b) ‘Cognitive biases and excessive use of social media: The facebook implicit associations test (FIAT)’, *Addictive Behaviors*, 105(October 2019). Available at: https://doi.org/10.1016/j.addbeh.2020.106328.

Twitter (2020a) *About public and protected Tweets What is the difference between public and protected*, *help.twitter.com*. Available at: https://help.twitter.com/en/safety-and-security/public-and-protected-tweets (Accessed: 2 November 2020).

Twitter (2020b) *Retweet FAQs What is a Retweet ?*, *help.twitter.com*. Available at: https://help.twitter.com/en/using-twitter/retweet-faqs (Accessed: 2 November 2020).

Uhunoma, B. and Asekhauno, A.A. (2021) ‘Sociological and Philosophical Perspectives on the Ethics of Social Media: An African’s Diary’, *Icheke Journal of the Faculty of Humanities*, 19(1), pp. 303–315.

UNODC (2013) *Comprehensive Study on Cybercrime*, *United Nations Office on Drugs and Crime*. Available at: http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

Urban, A., Hewitt, C. and Moore, J. (2018) ‘Fake it to make it, media literacy, and persuasive design: Using the functional triad as a tool for investigating persuasive elements in a fake news simulator’, *Proceedings of the Association for Information Science and Technology*, 55(1), pp. 915–916. Available at: https://doi.org/10.1002/pra2.2018.14505501174.

Vashistha, A. *et al.* (2018) ‘“You can always do better!” The impact of social proof on participant response bias’, *Conference on Human Factors in Computing Systems - Proceedings*, 2018-April. Available at: https://doi.org/10.1145/3173574.3174126.

Verkijika, S.F. (2019) ‘“If you know what to do, will you take action to avoid mobile phishing attacks”: Self-efficacy, anticipated regret, and gender’, *Computers in Human Behavior*, 101(January), pp. 286–296. Available at: https://doi.org/10.1016/j.chb.2019.07.034.

Victor, B. and Cullen, J.B. (1987) ‘A Theory and Measure of Ethical Climate in Organizations’, *Research in Corporate Social Performance and Policy*, 9, pp. 51–71.

Victor, B. and Cullen, J.B. (1988) ‘The Organizational Bases of Ethical Work Climates’, *Source: Administrative Science Quarterly*, 33(1), pp. 101–125. Available at: https://doi.org/10.2307/2392857.

Viđak, M. *et al.* (2020) ‘Perception of Organizational Ethical Climate by University Staff and Students in Medicine and Humanities: A Cross Sectional Study’, *Science and Engineering Ethics*, 26(6), pp. 3437–3454. Available at: https://doi.org/10.1007/s11948-020-00270-w.

Vryonides, S. *et al.* (2018) ‘Ethical climate and missed nursing care in cancer care units’, *Nursing Ethics*, 25(6), pp. 707–723. Available at: https://doi.org/10.1177/0969733016664979.

Vuori, V. and Jussila, J. (2016) ‘The 5C categorization of social media tools’, *AcademicMindtrek 2016 - Proceedings of the 20th International Academic Mindtrek Conference*, pp. 26–33. Available at: https://doi.org/10.1145/2994310.2994367.

Wagner, K. (2017) *Twitter changed its direct messaging product to try to protect users from spam and abuse*, *Recode.net*. Available at: https://www.recode.net/2017/3/31/15137586/twitter-direct-messages-update-spam (Accessed: 11 July 2017).

Wang, P. *et al.* (2018) ‘Social networking sites addiction and adolescent depression: A moderated mediation model of rumination and self-esteem’, *Personality and Individual Differences*, 127(59), pp. 162–167. Available at: https://doi.org/10.1016/j.paid.2018.02.008.

Wang, X. *et al.* (2019) ‘Persuasion for Good: Towards a Personalized Persuasive Dialogue System for Social Good’, pp. 5635–5649. Available at: https://doi.org/10.18653/v1/p19-1566.

Wason, P.C. and Evans, J.S.B.T. (1974) ‘Dual processes in reasoning?’, *Cognition*, 3(2), pp. 141–154. Available at: https://doi.org/10.1016/0010-0277(74)90017-1.

Watkins, D.C. (2017) ‘Rapid and Rigorous Qualitative Data Analysis: The “RADaR” Technique for Applied Research’, *International Journal of Qualitative Methods*, 16(1), pp. 1–9. Available at: https://doi.org/10.1177/1609406917712131.

Watson, M.A. and Lopiano, G.R. (2016) ‘Case Study- Should He Be Fired for That Facebook Post.pdf’, *Harvard Buiness Review* [Preprint], (March).

We Are Social & Hootsuite. (2018) *Digital 2018 South Africa*. Available at: https://doi.org/10.1016/j.solener.2006.08.015.

We Are Social & Hootsuite. (2019) *Digital 2019 South Africa*. Available at: https://es.slideshare.net/DataReportal/digital-2019-argentina-january-2019-v01?from_action=save.

We Are Social & Hootsuite (2017) ‘Digital 2017’, *We Are Social & Hootsuite* [Preprint]. Available at: https://www.gothaer.de/media/ueber_uns_1/presse/studien_2/digitalisierung/gothaer-versicherung-digitalisierung-studie-2017.pdf.

We Are Social & Hootsuite (2018) ‘Digital 2018’, *We Are Social & Hootsuite*, p. 40. Available at: https://doi.org/10.1016/j.solener.2006.08.015.

We Are Social & Hootsuite (2019) ‘Digital 2019’, *We Are Social & Hootsuite*, p. 76. Available at: https://es.slideshare.net/DataReportal/digital-2019-argentina-january-2019-v01?from_action=save.

Weber, M.S., Fulk, J. and Monge, P. (2016) ‘The Emergence and Evolution of Social Networking Sites as an Organizational Form’, *Management Communication Quarterly*, pp. 0893318916629547-. Available at: https://doi.org/10.1177/0893318916629547.

Wegmann, E. *et al.* (2017) ‘Online-specific fear of missing out and Internet-use expectancies contribute to symptoms of Internet-communication disorder’, *Addictive Behaviors Reports*, 5(February), pp. 33–42. Available at: https://doi.org/10.1016/j.abrep.2017.04.001.

Wehrle, K. and Fasbender, U. (2018) ‘Self-concept’, *Encyclopedia of Personality and Individual Differences* [Preprint], (December). Available at: https://doi.org/10.1007/978-3-319-28099-8.

Wellisz, C. (2016) ‘The Dark Side of Technology’, *Finance & Development*, 53(3), pp. 14–17. Available at: http://www.imf.org/external/pubs/ft/fandd/2016/09/wellisz.htm.

WhatsApp (2020) *About forwarding limits Related resources :*, *faq.whatsapp.com*. Available at: https://faq.whatsapp.com/general/coronavirus-product-changes/about-forwarding-limits/?lang=en (Accessed: 2 November 2020).

Whitler, K.A. (2017) *Why More Firms Need A Social Media Governance Plan*, *LinkedIn*. Available at: https://www.linkedin.com/pulse/why-more-firms-need-social-media-governance-plan-kimberly-a-whitler/ (Accessed: 30 October 2019).

Widagdo, P.P. *et al.* (2021) 'The Influence of User Generation Differences on Individual Performance in Using Information Technology', *Journal of Physics: Conference Series*, 1803(1). Available at: https://doi.org/10.1088/1742-6596/1803/1/012031.

Wilkinson, M. (2013a) *Nudges manipulate , except when they don't*, *LSE British Politics and Policy*. Available at: http://blogs.lse.ac.uk/politicsandpolicy/nudges-manipulate-except-when-they-dont/ (Accessed: 5 June 2017).

Wilkinson, M. (2013b) 'Nudging and manipulation', *Political Studies*, 61(2), pp. 341–355. Available at: https://doi.org/10.1111/j.1467-9248.2012.00974.x.

Williams, M. and Moser, T. (2019) 'The Art of Coding and Thematic Exploration in Qualitative Research', *International Management Review*, 15(1), pp. 45–55.

Williams, O. (2016) *Autoplay video is a plague that can't be stopped*, *The Next web*. Available at: https://thenextweb.com/opinion/2016/08/26/autoplay-video-is-a-plague-that-cant-be-stopped/#.tnw_W6IArHC3 (Accessed: 27 June 2017).

Williams, S.P. and Hausman, V. (2017) 'Categorizing the Business Risks of Social Media', *Procedia Computer Science*, 121, pp. 266–273. Available at: https://doi.org/10.1016/j.procs.2017.11.037.

Wolfe, S. *et al.* (2014) *Whistleblower Protection Laws in G20 Countries Priorities for Action*. Available at: https://www.transparency.de/fileadmin/pdfs/Themen/Hinweisgebersysteme/Whistleblower-Protection-Laws-in-G20-Countries-Priorities-for-Action.pdf.

Wood, W. (2017) 'Habit in Personality and Social Psychology', *Personality and Social Psychology Review* [Preprint], (July). Available at: https://doi.org/10.1177/1088868317720362.

Yang, C. *et al.* (2019) 'The Relationship Between Self-Control and Self-Efficacy Among Patients With Substance Use Disorders : Resilience and Self-Esteem as Mediators', *Frontiers in Psychiatry*, 10(June), pp. 1–10. Available at: https://doi.org/10.3389/fpsyt.2019.00388.

Yang, Y. (2020) ‘Freedom and Responsibility: An Existential Analysis of Amir from The Kite Runner’, *Scientific and Social Research*, 2(3), pp. 0–3. Available at: https://doi.org/10.36922/ssr.v2i3.1002.

Yeung, K. (2012) ‘Nudge as Fudge’, *Modern Law Review*, 75(1), pp. 122–148. Available at: https://doi.org/10.1111/j.1468-2230.2012.00893.x.

Yihui, W. (2018) ‘Research on the Design of Mobile Social Products Based on BJ Fogg’s Behavior Model’, *CNKI* [Preprint]. Available at: http://en.cnki.com.cn/Article_en/CJFDTotal-CXYY201808002.htm.

Yin, L. *et al.* (2019) ‘Social networking sites addiction and FoMO: The mediating role of envy and the moderating role of need to belong’, *Current Psychology* [Preprint]. Available at: https://doi.org/10.1007/s12144-019-00344-4.

Yoganathan, V., Osburg, V.S. and Bartikowski, B. (2021) ‘Building better employer brands through employee social media competence and online social capital’, *Psychology and Marketing*, 38(3), pp. 524–536. Available at: https://doi.org/10.1002/mar.21451.

Yu, X. *et al.* (2020) ‘A new form of brand experience in online social networks: An empirical analysis’, *Journal of Business Research*, (February), pp. 0–1. Available at: https://doi.org/10.1016/j.jbusres.2020.02.011.

Zerfass, A., Fink, S. and Linke, A. (2011) ‘Social Media Governance: Regulatory frameworks as drivers of success in online communications’, *14th International Public Relations Research Conference*, (January), pp. 1–22. Available at: https://doi.org/10.1017/CBO9781107415324.004.

Zerfass, A. and Schramm, D.M. (2014) ‘Social Media Newsrooms in public relations: A conceptual framework and corporate practices in three countries’, *Public Relations Review*, pp. 79–91. Available at: https://doi.org/10.1016/j.pubrev.2013.12.003.

Zetter, K. (2015) ‘Hackers Finally Post Stolen Ashley Madison Data’, *Wired*, p. 1. Available at: http://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/.

Zhu, J. *et al.* (2019) ‘High impulsivity, low self-control and problematic mobile phone use: The effect of poor sleep quality’, *Current Psychology* [Preprint], (Duckworth

2011). Available at: https://doi.org/10.1007/s12144-019-00259-0.

Zikopoulos, P. *et al.* (2015) *Big Data Beyond the Hype*. McGraw-Hill.

Zivnuska, S. *et al.* (2019a) ‘Social media addiction and social media reactions: The implications for job performance’, *Journal of Social Psychology* [Preprint]. Available at: https://doi.org/10.1080/00224545.2019.1578725.

Zivnuska, S. *et al.* (2019b) ‘Social media addiction and social media reactions: The implications for job performance’, *Journal of Social Psychology*, 159(6), pp. 746–760. Available at: https://doi.org/10.1080/00224545.2019.1578725.

Zivnuska, S. *et al.* (2019c) ‘Social media addiction and social media reactions: The implications for job performance’, *Journal of Social Psychology*, 0(0), pp. 1–15. Available at: https://doi.org/10.1080/00224545.2019.1578725.

APPENDIX – QUANTITATIVE INSTRUMENT

1. Demographics
2. OSN Usage
3. Online Privacy Literacy Scale (OPLIS) & Security behaviour Intentions Scale (SeBIS)
4. Online Social Network Addiction Bergen Social Media Addiction Scale (BSMAS)
5. Online Privacy Self Efficacy
6. Rosenberg Self-Esteem Scale
7. Ethical Climate Questionnaire (ECQ)

Online Social Networks Usage and Business Transparency

*Required

Purpose of the survey

This is an academic research survey that should take no more that 10 to 15 minutes to complete to determine the effect of business transparency through the use of Online Social Networks (Social Media Apps) by all employees of this organisation.

Should you require more information regarding the research and the survey please click on the following link and open the corresponding PDF document. https://goo.gl/WcwXDY

You will remain Anonymous

This survey does not have links to any personal identifying information such as your name, identification number, employment identification, date of birth, email address or cell phone number.

Your participation is therefore anonymous.

This means that the survey must be completed and submitted once you have commenced. If you do not submit your survey selections after exiting the survey your selections will be lost and you will have to start from scratch as to maintain anonymity we cannot identify and link you to your non-submitted survey.

Your Participation

Your participation is voluntary and you are free to withdraw at any time and not submit your responses.

The results of the study will be used for academic purposes. We will provide you with a summary of our findings on request.

The questionnaire has been kept as brief as possible and should not take more than 10-15 minutes of your time.

I have read and understand the conditions and understand my rights concerning participating in the research and I am willing to participate in the survey. *

○ I Agree to participate in this survey

○ I do NOT Agree to participate in this survey

NEXT

Online Social Networks Usage and Business Transparency

*Required

A little about yourself (3 Questions)

1. Gender *

○ Female
○ Male

2. Year of Birth *

○ From 1953 to 1956
○ From 1957 to 1960
○ From 1961 to 1964
○ From 1965 to 1968
○ From 1969 to 1972
○ From 1973 to 1976
○ From 1977 to 1980
○ From 1981 to 1984
○ From 1985 to 1988
○ From 1989 to 1992
○ From 1993 to 1996
○ From 1997 to 2000

3. Highest Qualification*

○ Matric
○ Certificate
○ Diploma
○ Graduate
○ Post Graduate

BACK NEXT

Page 3 of 13

This content is neither created nor endorsed by Google. Report Abuse - Terms of Service

Online Social Networks Usage and Business Transparency

Hint: For the next few questions Smartphone Users rotate your phone to Landscape for better visibility.

BACK NEXT

Page 4 of 13

Online Social Networks Usage and Business Transparency

Social Media Usage (1 Question)

This question is about your average engagement with the most popular social media apps. If you have never come across an app mentioned select the "never" option or leave it blank.

How often do you engage with the following Online Social Networking sites?

	Hourly	Daily	Weekly	Monthly	Never
Facebook	○	○	○	○	○
YouTube	○	○	○	○	○
Facebook Messenger	○	○	○	○	○
LinkedIn	○	○	○	○	○

	Hourly	Daily	Weekly	Monthly	Never
WhatsApp	○	○	○	○	○
Instagram	○	○	○	○	○
Google +	○	○	○	○	○
Tumblr	○	○	○	○	○

	Hourly	Daily	Weekly	Monthly	Never
Pinterest	○	○	○	○	○
Viber	○	○	○	○	○
WeChat	○	○	○	○	○
Twitter	○	○	○	○	○

	Hourly	Daily	Weekly	Monthly	Never
Snap Chat	○	○	○	○	○
Skype	○	○	○	○	○
Email	○	○	○	○	○
Tinder	○	○	○	○	○

BACK NEXT

Page 5 of 13

Online Social Networks Usage and Business Transparency

Online Privacy Literacy (6 Questions)
Please check the best option that you think applies

1. Data collected through your user profile by Social Media Apps like Facebook ...

is deleted after five years

- ○ True
- ○ False
- ○ Not Sure

is passed on to other organisations

- ○ True
- ○ False
- ○ Not Sure

is protected using the default privacy settings

- ○ True
- ○ False
- ○ Not Sure

includes data on your non connected friends

- ○ True
- ○ False
- ○ Not Sure

2. What is the key function of the following browser functions? Select the most appropriate option.

Stores URLs of visited websites

○ Cache
○ Cookie
○ Browsing History
○ Not Sure

Creates a text file that recognises a user when revisiting

○ Cache
○ Cookie
○ Browsing History
○ Not Sure

Accelerates surfing

○ Cache
○ Cookie
○ Browsing History
○ Not Sure

3. What is the key purpose of the following applications? Select the most appropriate option.

Hides your IP address with a temporary one

○ Firewall
○ VPN
○ Trojan
○ Not Sure

A virus disguised as an application

○ Firewall
○ VPN
○ Trojan
○ Not Sure

Protects the computer from web attacks

○ Firewall
○ VPN
○ Trojan
○ Not Sure

Creates an encrypted connection over the Internet

○ Firewall
○ VPN
○ Trojan
○ Not Sure

4. When Surfing the Internet I can protect myself by ...

always using the same search engine

○ True
○ False
○ Not Sure

using a reputable VPN (Virtual Private Network)

○ True
○ False
○ Not Sure

deleting information like cookies/cache/browser history

○ True
○ False
○ Not Sure

never surfing in private browsing mode

○ True
○ False

○ Not Sure

never using false names / pseudonyms

○ True
○ False
○ Not Sure

5. When using passwords they should be...

the same for all my accounts

○ True
○ False
○ Not Sure

kept the same so I don't forget it

○ True
○ False
○ Not Sure

created using a phrase instead of a word

○ True
○ False
○ Not Sure

created using letters, numbers & symbols not just letters

○ True
○ False
○ Not Sure

6. The PoPI Act

Protects you from the unauthorised commercial use of your private data

○ True
○ False

○ Not Sure

Is aligned to the European Union General Data Protection Regulation (GDPR)

○ True
○ False
○ Not Sure

Allows social media companies to pass on data they collect about you without your permission

○ True
○ False
○ Not Sure

Protects you from private data collection even if it is required by law

○ True
○ False
○ Not Sure

BACK NEXT

Page 6 of 13

Online Social Networks Usage and Business Transparency

Online Security behaviour Intentions (6 Questions)
Please check the best option that you think applies

This section is a check on your current online habits. Please answer as honestly as possible. All data collected is completely anonymous intended to reveal our behaviour as an online community of users and not as individuals.

1. My Passwords

I change, even if I don't have to.

- ○ Never
- ○ Rarely
- ○ Sometimes
- ○ Often
- ○ Always

Are different for different accounts.

- ○ Never
- ○ Rarely
- ○ Sometimes
- ○ Often
- ○ Always

Is longer than 6 characters

- ○ Never
- ○ Rarely
- ○ Sometimes
- ○ Often
- ○ Always

Have special characters even if not required.

- ○ Never
- ○ Rarely
- ○ Sometimes
- ○ Often
- ○ Always

2. My Device / Computer

Is set to automatically lock when left for a while.

- ○ Never
- ○ Rarely
- ○ Sometimes
- ○ Often
- ○ Always

Is unlocked with a password/passcode.

- ○ Never
- ○ Rarely
- ○ Sometimes
- ○ Often
- ○ Always

I manually lock when I step away from it.

- ○ Never
- ○ Rarely
- ○ Sometimes
- ○ Often
- ○ Always

Requires a PIN or passcode to be unlocked

○ Never
○ Rarely
○ Sometimes
○ Often
○ Always

3. I will look at the URL of a website...

before I open a link someone has sent

○ Never
○ Rarely
○ Sometimes
○ Often
○ Always

even if I’m familiar with website’s look & feel

○ Never
○ Rarely
○ Sometimes
○ Often
○ Always

to check for https: or lock icon to submit data

○ Never
○ Rarely
○ Sometimes
○ Often
○ Always

by using a mouse over on links

○ Never
○ Rarely
○ Sometimes
○ Often
○ Always

if I suspect a security problem

○ Never
○ Rarely
○ Sometimes
○ Often
○ Always

4. When it comes to software updates I...

install the new update as soon as I'm notified

○ Never
○ Rarely
○ Sometimes
○ Often
○ Always

make sure programs are up-to-date

○ Never
○ Rarely
○ Sometimes
○ Often
○ Always

make sure my anti-virus updates itself

○ Never
○ Rarely
○ Sometimes
○ Often
○ Always

consider what is best for the protection of this organisation

○ Never
○ Rarely
○ Sometimes
○ Often
○ Always

5. Regarding Social Network Apps Privacy Policies I...

agree to without reading them

○ Never
○ Rarely
○ Sometimes
○ Often
○ Always

read thoroughly

○ Never
○ Rarely
○ Sometimes
○ Often
○ Always

review if I'm notified of an update

○ Never
○ Rarely
○ Sometimes
○ Often
○ Always

consider what is best for the protection of this organisation

○ Never
○ Rarely
○ Sometimes
○ Often
○ Always

6. Regarding Social Network Apps Privacy Settings I...

accept the default settings

○ Never
○ Rarely
○ Sometimes
○ Often
○ Always

don’t care about them

○ Never
○ Rarely
○ Sometimes
○ Often
○ Always

go with the flow like most people do

○ Never
○ Rarely
○ Sometimes
○ Often
○ Always

consider what is best for the protection of this organisation

○ Never
○ Rarely
○ Sometimes
○ Often
○ Always

BACK NEXT

Page 7 of 13

Online Social Networks Usage and Business Transparency

Smartphone Users may want to rotate your phone back to portrait mode for better ease of use.

BACK NEXT

Page 8 of 13

Online Social Networks Usage and Business Transparency

Online Social Network Habits (6 Questions)

Please rate the next 6 Questions in terms time spent on typical habits when engaging on Online Social Networks

1. I text while I drive

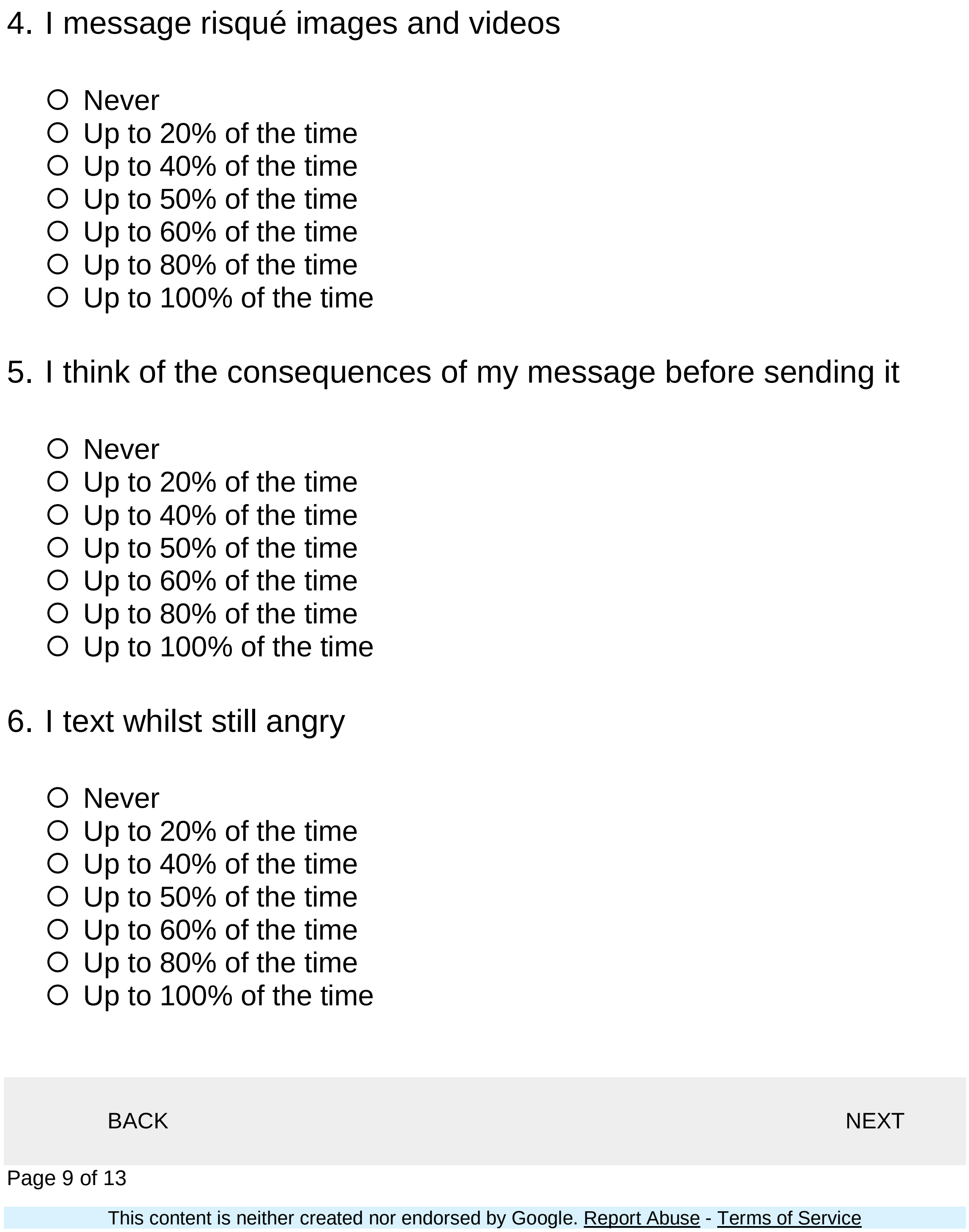
○ Never
○ Up to 20% of the time
○ Up to 40% of the time
○ Up to 50% of the time
○ Up to 60% of the time
○ Up to 80% of the time
○ Up to 100% of the time

2. I text when I have been drinking

○ Never
○ Up to 20% of the time
○ Up to 40% of the time
○ Up to 50% of the time
○ Up to 60% of the time
○ Up to 80% of the time
○ Up to 100% of the time

3. I check to see that I am sending to the correct recipient

○ Never
○ Up to 20% of the time
○ Up to 40% of the time
○ Up to 50% of the time
○ Up to 60% of the time
○ Up to 80% of the time
○ Up to 100% of the time



4. I message risqué images and videos

○ Never
○ Up to 20% of the time
○ Up to 40% of the time
○ Up to 50% of the time
○ Up to 60% of the time
○ Up to 80% of the time
○ Up to 100% of the time

5. I think of the consequences of my message before sending it

○ Never
○ Up to 20% of the time
○ Up to 40% of the time
○ Up to 50% of the time
○ Up to 60% of the time
○ Up to 80% of the time
○ Up to 100% of the time

6. I text whilst still angry

○ Never
○ Up to 20% of the time
○ Up to 40% of the time
○ Up to 50% of the time
○ Up to 60% of the time
○ Up to 80% of the time
○ Up to 100% of the time

Page 9 of 13

This content is neither created nor endorsed by Google. Report Abuse - Terms of Service

Online Social Networks Usage and Business Transparency

Online Social Network Addiction (6 Questions)

Please rate the next 6 Questions regarding the time you spend engaging on Online Social Networks

1. You spend a lot of time thinking about social media or planning how to use it.

○ Very Rarely
○ Rarely
○ Sometimes
○ Often
○ Very Often

2. You feel an urge to use social media more and more?

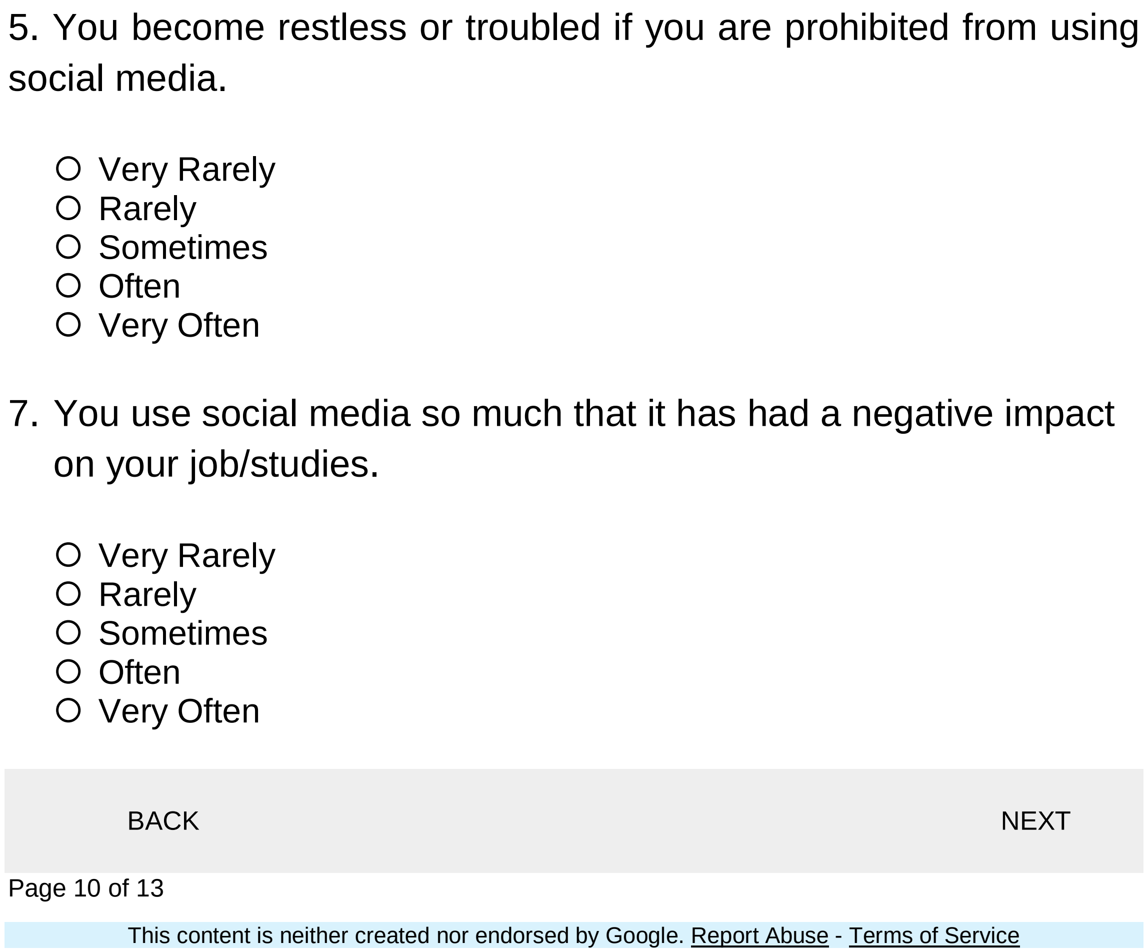
○ Very Rarely
○ Rarely
○ Sometimes
○ Often
○ Very Often

3. You use social media to forget about personal problems.

○ Very Rarely
○ Rarely
○ Sometimes
○ Often
○ Very Often

4. You have tried to cut down on the use of social media without success.

○ Very Rarely
○ Rarely
○ Sometimes
○ Often
○ Very Often



5. You become restless or troubled if you are prohibited from using social media.

○ Very Rarely
○ Rarely
○ Sometimes
○ Often
○ Very Often

7. You use social media so much that it has had a negative impact on your job/studies.

○ Very Rarely
○ Rarely
○ Sometimes
○ Often
○ Very Often

Page 10 of 13

Online Social Networks Usage and Business Transparency

Self-Efficacy (10 Questions)

1. I am able to protect myself from cyber threats.

○ Strongly Disagree
○ Disagree
○ Neither Agree or Disagree
○ Agree
○ Strongly Agree

2. If my online privacy is compromised I will be able to find a way to counter it within my legal privacy rights.

○ Strongly Disagree
○ Disagree
○ Neither Agree or Disagree
○ Agree
○ Strongly Agree

3. I know and maintain my Online Privacy rights.

○ Strongly Disagree
○ Disagree
○ Neither Agree or Disagree
○ Agree
○ Strongly Agree

4. I know how to protect my private data from being tracked by outside sources.

○ Strongly Disagree
○ Disagree
○ Neither Agree or Disagree
○ Agree
○ Strongly Agree

5. I do not believe anyone could crack my online passwords.

○ Strongly Disagree
○ Disagree
○ Neither Agree or Disagree
○ Agree
○ Strongly Agree

6. If my online activity is compromised by unknown malware or a virus I will be able to find a solution.

○ Strongly Disagree
○ Disagree
○ Neither Agree or Disagree
○ Agree
○ Strongly Agree

7. I am confident that my personal information will not be misused by Online Social Networking companies.

○ Strongly Disagree
○ Disagree
○ Neither Agree or Disagree
○ Agree
○ Strongly Agree

8. If my online activity is under threat by a virus or is being maliciously traced, I know how to stop it and remove the threat.

○ Strongly Disagree
○ Disagree
○ Neither Agree or Disagree
○ Agree
○ Strongly Agree

9. If my online activity has been compromised by malware or a virus I will be able to stop the attack and prevent further invasion.

○ Strongly Disagree
○ Disagree
○ Neither Agree or Disagree
○ Agree
○ Strongly Agree

10. Knowing how and protecting this organisation's private and client data from being tracked by outside sources is of prime importance for me.

○ Strongly Disagree
○ Disagree
○ Neither Agree or Disagree
○ Agree
○ Strongly Agree

BACK NEXT

Page 11 of 13

Online Social Networks Usage and Business Transparency

Self Esteem (10 Questions)
Well done so far... just a little more

1. On the whole, I am satisfied with myself.

○ Strongly Disagree
○ Disagree
○ Neither Agree or Disagree
○ Agree
○ Strongly Agree

2. At times I think I am no good at all.

○ Strongly Disagree
○ Disagree
○ Neither Agree or Disagree
○ Agree
○ Strongly Agree

3. I feel that I have a number of good qualities.

○ Strongly Disagree
○ Disagree
○ Neither Agree or Disagree
○ Agree
○ Strongly Agree

4. I am able to do things and most other people.

○ Strongly Disagree
○ Disagree
○ Neither Agree or Disagree
○ Agree
○ Strongly Agree

5. I feel I do not have much to be proud of.

○ Strongly Disagree
○ Disagree
○ Neither Agree or Disagree
○ Agree
○ Strongly Agree

6. I certainly feel useless at times.

○ Strongly Disagree
○ Disagree
○ Neither Agree or Disagree
○ Agree
○ Strongly Agree

7. I feel that I'm a person of worth, at least on an equal plane with others.

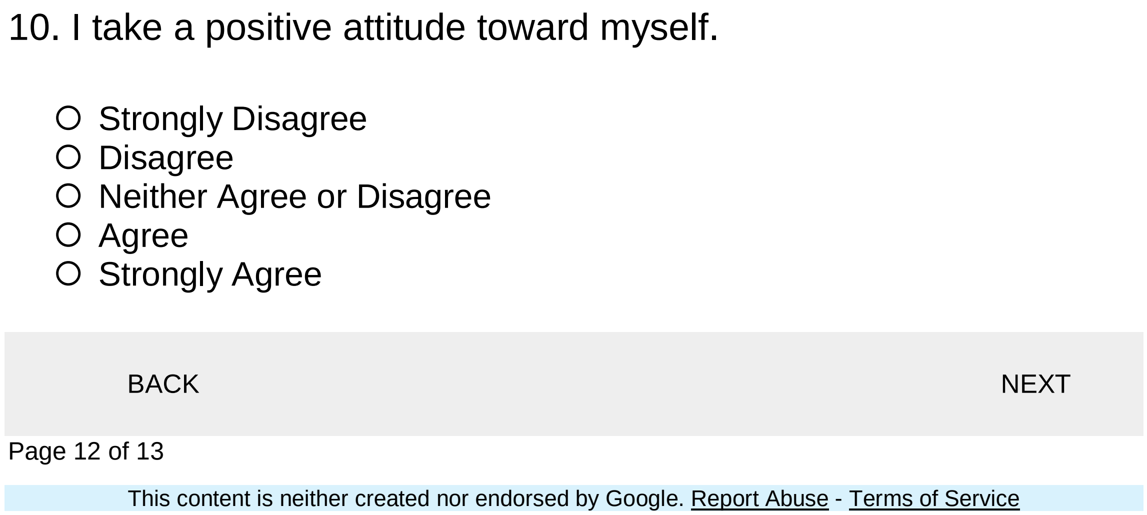
○ Strongly Disagree
○ Disagree
○ Neither Agree or Disagree
○ Agree
○ Strongly Agree

8. I wish I could have more respect for myself.

○ Strongly Disagree
○ Disagree
○ Neither Agree or Disagree
○ Agree
○ Strongly Agree

9. All in all, I am inclined to feel that I am a failure

○ Strongly Disagree
○ Disagree
○ Neither Agree or Disagree
○ Agree
○ Strongly Agree



10. I take a positive attitude toward myself.

- ○ Strongly Disagree
- ○ Disagree
- ○ Neither Agree or Disagree
- ○ Agree
- ○ Strongly Agree

Page 12 of 13

This content is neither created nor endorsed by Google. Report Abuse - Terms of Service

Online Social Networks Usage and Business Transparency

Ethical Climate Type (29 Questions)

We would like to ask you some questions about the general climate in your organisation. Please answer the following regarding how it is in reality in your organisation, or how you would prefer it to be. Please be as candid as possible, remember, all your responses will remain strictly anonymous.

Almost there....Last stretch

1. What is best for everyone in the organisation is the major consideration here.

○ Strongly Disagree
○ Mostly Disagree
○ Somewhat Disagree
○ Neither Agree or Disagree
○ Somewhat Agree
○ Mostly Agree
○ Strongly Agree

10. The most important concern is the good of all the people in the organisation as a whole.

○ Strongly Disagree
○ Mostly Disagree
○ Somewhat Disagree
○ Neither Agree or Disagree
○ Somewhat Agree
○ Mostly Agree
○ Strongly Agree

11. Our major concern is always what is best for the other person.

○ Strongly Disagree
○ Mostly Disagree
○ Somewhat Disagree
○ Neither Agree or Disagree
○ Somewhat Agree
○ Mostly Agree
○ Strongly Agree

12. In this organisation, people look out for each other's good.

○ Strongly Disagree
○ Mostly Disagree
○ Somewhat Disagree
○ Neither Agree or Disagree
○ Somewhat Agree
○ Mostly Agree
○ Strongly Agree

13. In this organisation, it is expected that you will always do what is right for the customer and public.

○ Strongly Disagree
○ Mostly Disagree
○ Somewhat Disagree
○ Neither Agree or Disagree
○ Somewhat Agree
○ Mostly Agree
○ Strongly Agree

14. The most efficient way is always the right way in this organisation.

○ Strongly Disagree
○ Mostly Disagree
○ Somewhat Disagree
○ Neither Agree or Disagree
○ Somewhat Agree
○ Mostly Agree
○ Strongly Agree

15. In this organisation, each person is expected above all to work efficiently.

○ Strongly Disagree
○ Mostly Disagree
○ Somewhat Disagree
○ Neither Agree or Disagree
○ Somewhat Agree
○ Mostly Agree
○ Strongly Agree

16. People are expected to comply with the law and professional standards over and above other considerations.

○ Strongly Disagree
○ Mostly Disagree
○ Somewhat Disagree
○ Neither Agree or Disagree
○ Somewhat Agree
○ Mostly Agree
○ Strongly Agree

17. In this organisation, the law or ethical code of their profession is the major consideration.

○ Strongly Disagree
○ Mostly Disagree
○ Somewhat Disagree
○ Neither Agree or Disagree
○ Somewhat Agree
○ Mostly Agree
○ Strongly Agree

18. In this organisation, people are expected to strictly follow legal or professional standards.

○ Strongly Disagree
○ Mostly Disagree
○ Somewhat Disagree
○ Neither Agree or Disagree
○ Somewhat Agree
○ Mostly Agree
○ Strongly Agree

19. In this organisation, the first consideration is whether a decision violates any law.

○ Strongly Disagree
○ Mostly Disagree
○ Somewhat Disagree
○ Neither Agree or Disagree
○ Somewhat Agree
○ Mostly Agree
○ Strongly Agree

20. It is very important to follow the organisation's rules and procedures here.

○ Strongly Disagree
○ Mostly Disagree
○ Somewhat Disagree
○ Neither Agree or Disagree
○ Somewhat Agree
○ Mostly Agree
○ Strongly Agree

21. Everyone is expected to stick by organisation rules and procedures.

○ Strongly Disagree
○ Mostly Disagree
○ Somewhat Disagree
○ Neither Agree or Disagree
○ Somewhat Agree
○ Mostly Agree
○ Strongly Agree

22. Successful people in this organisation go by the book.

○ Strongly Disagree
○ Mostly Disagree
○ Somewhat Disagree
○ Neither Agree or Disagree
○ Somewhat Agree
○ Mostly Agree
○ Strongly Agree

23. People in this organisation strictly obey the organisation policies.

○ Strongly Disagree
○ Mostly Disagree
○ Somewhat Disagree
○ Neither Agree or Disagree
○ Somewhat Agree
○ Mostly Agree
○ Strongly Agree

24. In this organisation, people protect their own interests above all else.

○ Strongly Disagree
○ Mostly Disagree
○ Somewhat Disagree
○ Neither Agree or Disagree
○ Somewhat Agree
○ Mostly Agree
○ Strongly Agree

25. In this organisation, people are mostly out for themselves.

○ Strongly Disagree
○ Mostly Disagree
○ Somewhat Disagree
○ Neither Agree or Disagree
○ Somewhat Agree
○ Mostly Agree
○ Strongly Agree

26. There is no room for one's own personal morals or ethics in this organisation.

○ Strongly Disagree
○ Mostly Disagree
○ Somewhat Disagree
○ Neither Agree or Disagree
○ Somewhat Agree
○ Mostly Agree
○ Strongly Agree

Almost done ... you been great so far ... a final small push ... 10 more quick questions on your company's expectations

27. People are expected to do anything to further the organisation's interests, regardless of the consequences.

○ Strongly Disagree
○ Mostly Disagree
○ Somewhat Disagree
○ Neither Agree or Disagree
○ Somewhat Agree
○ Mostly Agree
○ Strongly Agree

28. People here are concerned with the organisation's interests — to the exclusion of all else.

○ Strongly Disagree
○ Mostly Disagree
○ Somewhat Disagree
○ Neither Agree or Disagree
○ Somewhat Agree
○ Mostly Agree
○ Strongly Agree

29. Work is considered substandard only when it hurts the organisation's interests.

○ Strongly Disagree
○ Mostly Disagree
○ Somewhat Disagree
○ Neither Agree or Disagree
○ Somewhat Agree
○ Mostly Agree
○ Strongly Agree

30. The major responsibility of people in this organisation is to control costs.

○ Strongly Disagree
○ Mostly Disagree
○ Somewhat Disagree
○ Neither Agree or Disagree
○ Somewhat Agree
○ Mostly Agree
○ Strongly Agree

31. In this organisation, people are expected to follow their own personal and moral beliefs.

○ Strongly Disagree
○ Mostly Disagree
○ Somewhat Disagree
○ Neither Agree or Disagree
○ Somewhat Agree
○ Mostly Agree
○ Strongly Agree

32. Each person in this organisation decides for themselves what is right and wrong.

○ Strongly Disagree
○ Mostly Disagree
○ Somewhat Disagree
○ Neither Agree or Disagree
○ Somewhat Agree
○ Mostly Agree
○ Strongly Agree

33. The most important concern in this organisation is each person's own sense of right and wrong.

○ Strongly Disagree
○ Mostly Disagree
○ Somewhat Disagree
○ Neither Agree or Disagree
○ Somewhat Agree
○ Mostly Agree
○ Strongly Agree

34. In this organisation, people are guided by their own personal ethics.

○ Strongly Disagree
○ Mostly Disagree
○ Somewhat Disagree
○ Neither Agree or Disagree
○ Somewhat Agree
○ Mostly Agree
○ Strongly Agree

35. In this organisation, everyone's right to freedom of speech is respected.

○ Strongly Disagree
○ Mostly Disagree
○ Somewhat Disagree
○ Neither Agree or Disagree
○ Somewhat Agree
○ Mostly Agree
○ Strongly Agree

28. In this organisation, colleagues respect each other's privacy and do not broadcast other's personal information.

○ Strongly Disagree
○ Mostly Disagree
○ Somewhat Disagree
○ Neither Agree or Disagree
○ Somewhat Agree
○ Mostly Agree
○ Strongly Agree

36. This organisation believes all private and personal information gathered about others, is company property.

○ Strongly Disagree
○ Mostly Disagree
○ Somewhat Disagree
○ Neither Agree or Disagree
○ Somewhat Agree
○ Mostly Agree
○ Strongly Agree

Thank You! Your efforts to help conduct this important research is Very Much Appreciated... Please make sure you submit your answers.

BACK

SUBMIT

Page 13 of 13