EXPLORING THE PRIVACY CALCULUS ON SOCIAL NETWORKING SERVICES FROM A SOUTH AFRICAN PERSPECTIVE

B.G. MATHEW

2020

EXPLORING THE PRIVACY CALCULUS ON SOCIAL NETWORKING SERVICES FROM A SOUTH AFRICAN PERSPECTIVE

By

Boney George Mathew

Submitted in fulfilment of the requirements for the degree of Master of Technology
in Information Technology to be awarded at the Nelson Mandela University

April 2020

Supervisor: Prof LA Futcher

Co-Supervisor: Prof RA Botha

DECLARATION

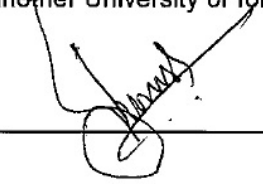
I, Boney George Mathew, hereby declare that

- The work in this dissertation is my own work
- All sources used or referred to, has been recognised and documented
- This dissertation has not previously been submitted in full or partial fulfilment of the requirements for an equivalent or higher qualification at any other recognised educational institute

TITLE OF PROJECT: EXPLORING THE PRIVACY CALCULUS ON SOCIAL NETWORKING SERVICES FROM A SOUTH AFRICAN PERSPECTIVE

DECLARATION:

In accordance with Rule G5.6.3, I hereby declare that the above-mentioned treatise/ dissertation/ thesis is my own work and that it has not previously been submitted for assessment to another University or for another qualification.



SIGNATURE: _____

DATE: 05/12/2019.

Boney George Mathew

ABSTRACT

Social Network Services (SNSs) have revolutionized the way we communicate, interact and present ourselves before others. The business model of SNS'S like Facebook is primarily based on SNS'S user self-disclosure of personal information. It is argued that the SNS'S user conducts a cost-benefit analysis before deciding to self-disclose their personal information, and this user behaviour forms the basis of the Privacy Calculus Theory. Enjoyment, Self-Presentation and Relationship Maintenance is considered as the benefits and the Privacy Concerns of the users is considered as the costs of disclosing personal information.

As national or regional culture could influence SNS'S user self-disclosure behaviour, it would be advantageous for multinational SNS'S's like Facebook to understand the perceptions of SNS'S user's from different nationalities. Currently, no studies have been conducted amongst the South African (SA) SNSs' users' self-disclosure behaviour. This research is aimed at understanding the South African SNSs' users' perceptions regarding their perceived costs, benefits and self-disclosure using the Privacy Calculus theory. This study is a replication of a similar study undertaken amongst the United States of America (US) and German SNS'S users. To remain competitive in the market and to sustain the viability of their business model, SNS like Facebook will have to encourage user self-disclosure. Studies have proven that national cultures play an important role on the nature and extent of user disclosure (Krasnova & Veltri, 2010; Lewis, Kaufman, & Christakis, 2008). However, no similar research has been undertaken in South Africa, and currently we do not understand South African SNS users' self-disclosure behaviour in terms of the privacy calculus theory.

The primary objective of this study is to understand the perceptions of South African SNS'S users regarding the perceived benefits, costs, moderating factors and self-disclosure, using the Privacy Calculus Theory. To achieve this objective, we initially undertook a detailed literature review to understand the concept of information privacy, privacy calculus, information privacy policy and legal framework, SNS'S and self-disclosure and the various factors affecting self-disclosure. We

then proceeded to validate the theoretical framework by collecting data from two South African universities, namely the Nelson Mandela University (NMU) and Walter Sisulu University (WSU (NMD Campus – Former University of Transkei)), by adopting the same methodology and instrument used in the original study (and the isiXhosa translation). The theoretical framework used for this study is based on the Privacy Calculus theory, which argues that users conduct a cost-benefit calculus before deciding to self-disclose their personal information. This analysis is further influenced by other moderating factors like trust, control and awareness. All these factors have been incorporated into the theoretical framework and the instrument, adapted from the original research was used to collect data from the participants.

The data from 239 respondents, who finally qualified for analysis was collated and proceeded with the analysis of that data. The data was analysed in four stages using established statistical tests. The first three phases were used to determine the actual value placed by the users on self-disclosure, its determinants and moderating factors, and the last phase concentrated on how each of the constructs included in the theoretical framework influenced the other constructs.

The results obtained from the analysis provided valuable insights into the self-disclosure behaviour of South African SNS'S users. Entertainment was the primary benefit the students derived from using SNS like Facebook, followed by relationship maintenance and those who enjoyed the platform more tended to Self-Disclose more. Those who tended to derive more benefits from the platform were found to trust the platform and the other users of the network. The theoretical framework was validated and it was determined that privacy paradox exists within the South African SNS'S user community, meaning that even with high privacy concerns, these SNS users are willing to self-disclose their personal information.

ACKNOWLEDGEMENTS

First of all, I thank my Lord Almighty for giving me the strength, perseverance and courage to complete this study, my parents for their prayers and continued support and my supervisors Professor Reinhardt A Botha and Professor Lynn Futcher for their guidance, motivation, patience, and for sharing their knowledge, skills and expertise.

TABLE OF CONTENTS

Chapter 3: Research Methodology

Chapter 4: Analysis

Chapter 5: Discussion of Results

Chapter 6: Conclusion

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ANOVA	Analysis of Variance
DPA	Data Protection Authority
EN	Entertainment
FB	Facebook
IDV	Individualism
LTO	Long Term Orientation
MAS	Masculinity
NMD	Nelson Mandela Drive Campus
NMU	Nelson Mandela University
PDI	Power Distance
POPI	Protection of Personal Information Act
RM	Relationship Maintenance
SA	South Africa
SATI	South African Translators Institute
SD	Self-Disclosure
SNS	Social Networking Service
SP	Self Presentation
TPB	Theory of Reasoned Behaviour
TRA	Theory of Reasoned Action
UAI	Uncertainty Avoidance
UN	United Nations
US	United States of America
WSU	Walter Sisulu University

Chapter 1: Introduction

1.1 Introduction

Social Network Services (SNS) are online services which allows their users to establish new connections or to maintain relationship with people with whom they share an offline connection. Self-disclosure of private information is the starting point for establishing and maintaining such relationships or connection (Boyd & Ellison, 2010). Intensity (Stutzman, Capra, & Thompson, 2011), integrity and intimacy (Li, X., & Chen, X. (2010), of SNS user self-disclosure is essential for the survival of SNS. The amount of self-disclosure is determined by different constructs like privacy concerns, perceived enjoyment, trust, perceived ease-of-use, perceived damage and the perceived likelihood of damage (Elmi, Iahad, & Ahmed, 2012) amongst others. As national or regional culture could influence SNS user behaviour, it would be advantageous for multinational SNS's like Facebook to understand the perceptions of SNS user's from different nationalities. Currently, no studies have been conducted amongst the South African (SA) SNS user's self-disclosure behaviour. This research is aimed at understanding the South African SNS user's perceptions regarding their perceived costs, benefits and self-disclosure using the privacy calculus theory. This study is a replication of a similar study undertaken amongst the United States of America (US) and the German SNS users. As such it will be ensured that the sample size is similar to that of the original study and the data will be collected using the same instruments, from a similar demographic. In the following sections, the objectives of this study will be stated after providing a brief description regarding the background and theoretical framework which forms the basis of this study.

1.2 Background

Many researchers across various disciplines have attempted to study the concept of privacy, its constructs and the relationships. As most of these relationships become inconsistent when viewed from multiple perspectives, a one-size-fit-all statement which defines privacy across multiple

disciplines has not emerged. Definitions like "*The right to be left alone*" (Warren & Brandeis, 1890) or "*The voluntary and temporary withdrawal of a person from the general society*" (Westin, 1968) were introduced by early researchers. However, the extent to which these statements describe privacy is greatly determined by the context. Though there are cultural variations, "*the right to privacy*" has been accepted as a basic human right and is guaranteed by the state in many countries. With an ever increasing trend towards computer mediated communication, information privacy has gained attention from companies, policy makers and the general public. Studies have confirmed that people are aware of the consequences of information privacy violations (Jensen, Potts, & Jensen, 2005; Norberg, Horne, & Horne, 2007). Increased privacy concerns may prevent people from disclosing their personal information. This is also true in the case of Social Networking Services (SNS).

SNSs can be defined as web based services which allows its users to publish their personal profile along with their list of connections, while being allowed to view and navigate the profiles and connections of other users within the system (Ellison, 2007). There are many SNSs available supporting a wide range of interests. While some SNSs cater for niche audiences based on ethnicity, nationality, or shared interests, most of them are tailored around supporting pre-existing social networks. Facebook and Myspace are examples of SNSs which help users to maintain pre-existing relationships at a relatively low cost. These services help the users to create a profile page by using the information which the user provides at the time of registering for these services. Once the profile page is created, users can search for and create a network of connections with other users sharing the service. Enjoyment, self-presentation and relationship maintenance can be considered as the significant benefits of participating in an SNS (Krasnova & Veltri, 2010). To sustain these benefits users must be encouraged to constantly interact with each other, while being truthful in their self-disclosures. However, privacy concerns may force SNS users to interact less and misrepresent themselves in their self-disclosures (Jiang, Heng, & Choi, 2013). This may eventually threaten the sustainability of many SNSs as constant communication and user self-disclosure are the corner stones of their business model.

In many studies regarding privacy violations, users have expressed fear that the information that they disclose on SNS is being used against them. A recent study (Youyou, Kosinski, & Stillwell, 2015) confirmed that life outcomes, behavioural traits and even personality of an SNS user can be deducted from the user self-disclosure. Knowledge of people's personalities can be used to manipulate and control them. This situation warrants strong information privacy laws which enables the SNS users to regain control of their digital foot prints. Many countries including South Africa, have passed laws and regulations aimed at information privacy, and may enact even stricter controls in the years to come. The European Union is planning to enact strict laws aimed at protecting the privacy of its citizens. One of their proposals is to force SNSs to provide "*privacy by default*" settings (European-Commission, 2012). This means that when a user registers on an SNS platform, the highest possible privacy settings will be applied to their profile by default. As many users tend to keep the default privacy settings, SNS like Facebook fear that this could negatively affect their business model. However, a study by Tschersich and Botha (2014) has concluded that imposing restrictive default privacy settings on SNS had limited impact.

Facebook was created in 2004 and was primarily aimed at university students. Gradually they started including schools and by 2006 anyone with a valid e-mail address could open an account with Facebook. Facebook is primarily aimed at maintaining offline connections at a relatively low cost, rather than for making new connections or relationships. Even though the platform does not encourage making contacts with strangers, it is mostly left to the discretion of the users. Most of the active users primarily use the platform to maintain offline connections, rather than to meet new people (Ellison, Steinfield, & Lampe, 2007). The popularity of Facebook has soured over the years and has reached 2.41 billion active users (http://investor.fb.com/) by the second quarter of the year 2019 (Refer to Figure 1.1). This increase in popularity could be due to the flexibility and versatility offered by Facebook (Tagtmeier, 2010). With more than 55 billion US dollars in revenue, Facebook is way ahead of its competitors. Most of this revenue comes from targeted advertisement, marketing and service fees (http://investor.fb.com/eventdetail.cfm). However, sustaining this success and popularity could be difficult if it does not adapt with the changing needs of the customers. As switching costs are relatively low, users of SNS's can switch from one service to the other at a relatively low cost. SNS's like Friendster, Myspace, and Orkut could not sustain

their early success. If privacy concerns prevent users from self-disclosure, they may not be motivated to use a particular SNS. Many studies have established that SNS users are concerned about their privacy and the use of their personal information. However, users are found to self-disclose more if they are motivated to exchange personal information for some perceived benefit, provided they have trust in the legal framework, the SNS, and the other users of the SNS. Researchers have attempted to study this paradox using the privacy calculus theory (Dinev & Hart, 2006; Elmi et al., 2012; Jiang et al., 2013; Krasnova, Kolesnikova, & Guenther, 2009).

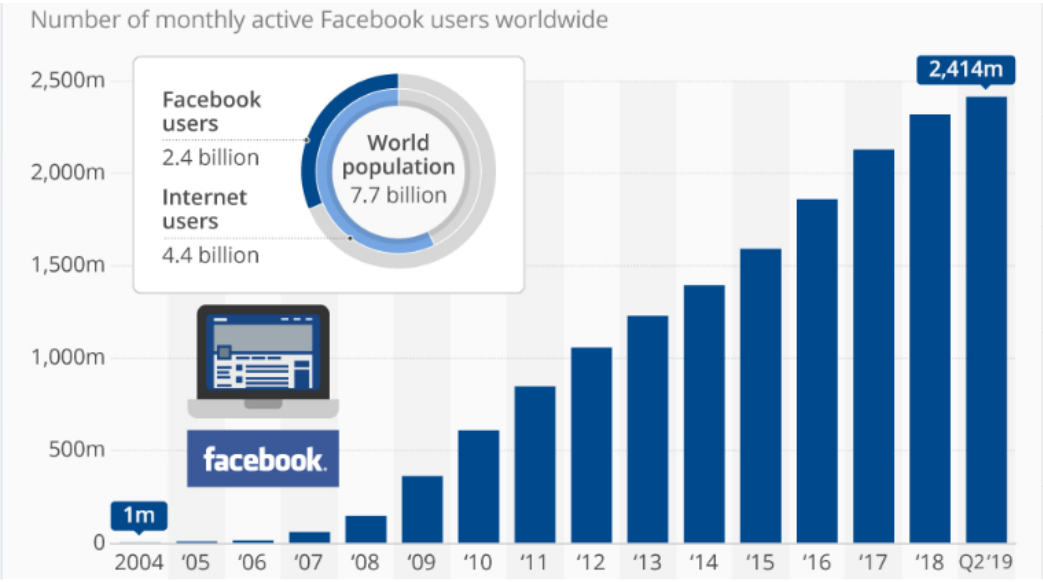


Figure 1.1: GROWTH IN THE NUMBER OF ACTIVE FACEBOOK USE (www.statistica.com and www.fb.com/companyinfo/pressreleases)

The privacy calculus theory views privacy from the economic perspective. It suggests that users weigh the potential risk and perceived benefit of self-disclosure, before sharing any personal information. A study by Krasnova and Veltri (2010) investigated the impact of cultural differences between the US and Germany on the dynamics of self-disclosure. The cultures of the two countries were compared using the five constructs as proposed by Hofstede and Hofstede (2001).

Hofstede and Hofstede (Hofstede, 1984; Hofstede, 2001) has proposed five dimensions that distinguish national cultures: power distance (PDI), individualism (IDV), masculinity (MAS), uncertainty avoidance (UAI), long term orientation (LTO) and has empirically derived a country index for each dimension.

Though Facebook is the leading SNS provider around the world, it is increasingly facing competition from local SNS's in various countries (mainly china and countries in Europe). This is mostly due to the local provider's ability to understand the culture specific traits of the target population. To remain competitive in international markets, and to retain its appeal to diverse populations, Facebook has to take these cultural differences into consideration.

Privacy Calculus theory is used to derive the constructs relevant for user self-disclosure on SNS. According to this theory self-disclosure takes place only if the perceived benefits of doing so outweigh the costs. Enjoyment, self-presentation and relationship maintenance are considered as the benefits of participating in an SNS (Krasnova & Veltri, 2010). User privacy concerns emanating from the perceived likelihood of privacy violation and the subsequent damage is considered as the cost of self-disclosure. The original study concluded that there are significant differences in the US and German Facebook user's perceptions regarding the privacy control, benefits, violations and damages while using an SNS. This research is aimed at determining the cultural influences of the South African society on SNS self-disclosure, by replicating the original study undertaken by Krasnova and Veltri (2010).

1.3 Theoretical Background

Self-disclosure can be defined as the act of revealing one's personal information to others. This can include information required for self-identification, personal likes and dislikes, orientation etc. Wheeless and Grotz (Wheeless, 1978; Wheeless & Grotz, 1976) has identified five dimensions of self-disclosure namely; intention (conscious or not), amount, nature (positive or negative), honesty (or accuracy) and intimacy of disclosure. Conscious revelation of intimate and accurate personal information within a closed group of SNS users has been found to positively influence the creation of social capital within that group. While visual anonymity and private self-awareness encourages self-disclosure, public self-awareness and accountability dissuades users from disclosing personal information (Jiang et al., 2013; Joinson, 2001). Bazarova (2012) has also reported that the context (private *vs* public) affects the intimacy of disclosure. An increase in social

capital is positively correlated with self-reported perceived benefits. In this research we try to understand the perceptions of South African SNS users towards self-disclosure using the privacy calculus theory.

The privacy calculus theory has been derived from the Theory of Reasoned Action (TRA) and the Theory of Planned Behaviour (TPB) (Dinev & Hart, 2006). According to privacy calculus theory, user's attitude towards self-disclosure is governed by two constructs namely; *perceived benefits* that could be derived from using the SNS and the *perceived costs* of revealing personal information. SNS users will disclose particular information if and only if the *perceived benefits* outweigh the *perceived costs* of sharing that information.

The benefits of using an SNS cannot be assigned a monetary value, and is usually subjective in nature. National culture can greatly influence these perceived benefits. Enjoyment, Self-Presentation and Relationship Maintenance are the benefits of being active on an SNS (Krasnova & Veltri, 2010). The intensity of Facebook use was found to be positively correlated with an increase in life satisfaction and self-esteem (Ellison et al., 2007). Perceived ease-of-use or enjoyment is an important determinant of perceived benefits that a user derives from using an SNS (Elmi et al., 2012). The opportunity to create a profile and to display their connections is another strong motivational factor (Ellison, 2007). This determinant can be termed as self-presentation. Finally, the opportunities offered by SNS's for Relationship-Maintenance with ease, and at a relatively low cost, is another benefit a user can derive from an SNS.

Privacy costs relate to the privacy concerns of the users of the SNS. Free online services like SNS's are mainly funded by collecting and analysing the users' personal data, and assigning an economic value to that information. Other than the platforms' legitimate use of SNS users' personal information, there is a real threat of privacy violations. Gross and Acquisti (2005) have identified some of the privacy concerns faced by SNS users, which includes but is not limited to stalking, re-identification, building a digital dossier and data security concerns. The perceived likelihood of a privacy violation and the resultant damage caused, informs the privacy concerns of SNS users.

Also, SNS users privacy concerns are determined mainly by the perceived likelihood of a violation and much less by the *perceived damage* that can be caused (Krasnova et al., 2009).

Studies have confirmed that users are aware of the privacy violations that could possibly occur. However, most of them do not take adequate measures to protect their privacy (Gross & Acquisti, 2005). Researchers have attempted to study this paradox and have stated various reasons for this phenomenon. The privacy calculus theory states that users of an SNS weigh the potential benefits vs the perceived costs of using the SNS, before they disclose personal information. However, this comparison is also subjective in nature and is influenced by other factors. Trust is an important factor a user considers when conducting the risk-benefit analysis. Trust in the legal framework, the SNS platform and the other users of the SNS are the major trust factors which influence a specific user's risk-benefit analysis. Nagy and Pecho (2009) reported that many users are not aware of the privacy settings at their disposal. SNS user's awareness of the available privacy settings of the SNS platform, will positively influence the perceived control a user has over his personal information. A user who is well informed of the privacy policy of the SNS platform and the privacy settings under his/her disposal can decide the target audience for his/her personal information. This will positively influence the users trust towards the SNS platform and the other users within his network (Wu, Huang, Yen, & Popova, 2012). Trust in the legal framework is another significant trust component which SNS users takes into consideration while trading personal information (Liu, Marchewka, & Ku, 2004). Users tend to withhold information or give false information in online transactions if they do not have faith in the legal framework.

Sometimes users tend to trade long term privacy for short term benefits (Acquisti & Grossklags, 2005). The inability of the user to accurately conduct a risk-benefit analysis when trading personal information could be the reason for this behaviour. Culture (Cullen, 2009), age (Nosko, Wood, & Molema, 2010), demographics (Zukowski & Brown, 2007), peer pressure, gender and the intensity of online activity have also been found to have a significant impact on self-disclosure (Lewis et al., 2008).

Using the above mentioned constructs a theoretical framework can be built. In this model it can be argued that the SNS users conduct a cost-benefit analysis before self-disclosure and that this analysis in turn is influenced by trust factors. Figure 1.2, shows the theoretical framework of our study.

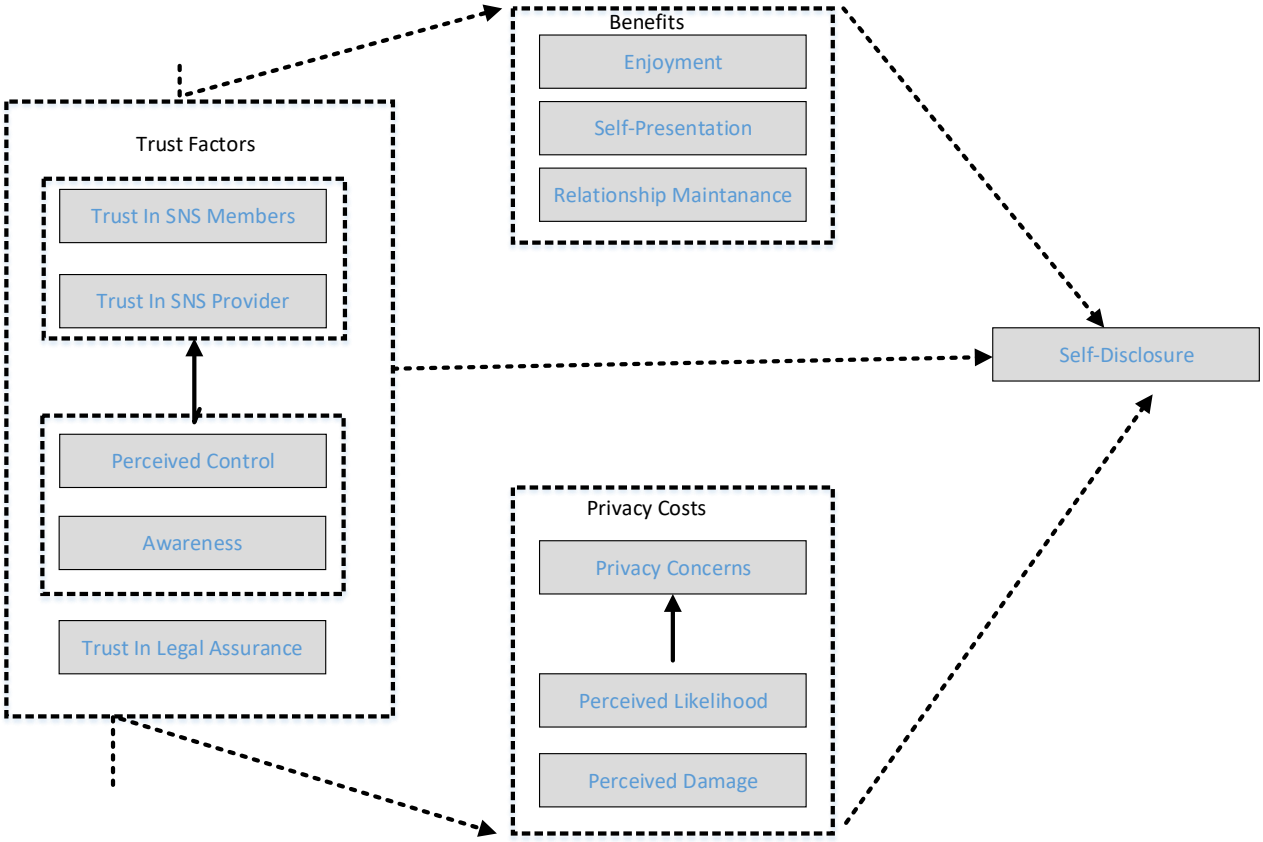


Figure 1.2: THEORETICAL FRAMEWORK (Krasnova & Veltri, 2010)

1.4 Problem Statement

To remain competitive in the market and to sustain the viability of their business model, SNS like Facebook will have to encourage user self-disclosure. Studies have proven that national cultures play an important role on the nature and extent of user disclosure (Krasnova & Veltri, 2010; Lewis et al., 2008).

Currently we do not understand South African SNS users' self-disclosure behaviour in terms of the privacy calculus theory.

1.5 Research Objectives

This study is aimed at understanding the perceptions of South African SNS users regarding the perceived benefits, costs, moderating factors and self-disclosure, using the privacy calculus theory, by replicating the study undertaken by Krasnova and Veltri (2010).

Primary Objective: To understand the perceptions of South African SNS users regarding the perceived benefits, costs, moderating factors and self-disclosure, using the privacy calculus theory. To achieve the primary objective three sub-objectives were also defined.

1. To understand information privacy, privacy calculus, moderating factors and self-disclosure as they relate to SNS users.

2. To determine the value placed on the determinants of SNS user self-disclosure by South African Facebook users.

3. To establish whether the privacy paradox manifest in the use of SNS by South African Facebook users

1.6 Research Approach

Since this is a replication of the original study, we target data from two South African universities, namely Nelson Mandela University (NMU) and Walter Sisulu University (WSU (NMD Campus – Former University of Transkei)), by adopting the same methodology and instrument used in the original study. WSU (NMD) is located in Mthatha, which is the former capital of Transkei, and is still considered as a rural area. WSU mainly serves the community in and around the former Transkei region. Nelson Mandela University is located in Port Elizabeth, which is one of the biggest

cities in South Africa. University students have been selected for three reasons. Firstly, the original US and German study involved university students; secondly university students are often forerunners in the adoption of new communication technologies, and their communication networks tend to be dense and multi-layered; and lastly a great majority of SNS users in South Africa are currently enrolled in universities or are university graduates (Bidwell, 2010).

1.7 Instrument

Questionnaires used in the original study were used for collecting data from the participants. The questionnaire (Table 1.1) is divided into 10 sections, each relating to a key determinant as follows:

Table 1.1: A BRIEF SUMMARY OF THE QUESTIONNAIRE (Krasnova & Veltri, 2010)

S. No	Section / Determinant	Description
1	Expected Benefits	*The expected benefits from using the SNS is enjoyment, self-presentation and relationship maintenance. This section measures to what extend the user enjoys using the SNS and the extent to which an SNS is used for self-presentation and relationship maintenance.*
2	Privacy Concerns	*Measures to what extend the information submitted on SNS can be misinterpreted or can be used for unintended or unforeseen purposes.*
3	Perceived Damage	*Measures the amount of the damage to the SNS user (financial, to your reputation, social, psychological) resulting from any privacy violation.*
4	Perceived Likelihood	*Measures the perceived likelihood of a privacy violation.*
5	Trust in SNS provider	*Measures the amount of trust an SNS user has towards their SNS provider*
6	Trust in SNS users	*Measures the amount of trust an SNS user has towards the other users of the platform*
7	Trust in Legal Assurance	*Measures the amount of trust an SNS user has in the legal framework*

8	Awareness	*Measures the SNS user awareness*
9	Control over personal information	*Measures how much control (e.g. through functionality, privacy policies) an SNS user has over his personal information:*
10	Self-Disclosure	*Measures the extent to which an SNS user discloses personal information.*

A copy of the questionnaire is included herewith as Appendix A.

1.8 Limitations

The sample of students which we draw from among the students at Nelson Mandela University and WSU may not be representative of the South African Society in general and SNS users in particular. And as students are only selected from two universities in South Africa, based on their relative ease of access, there is also a possibility of selection bias. And also as we could not obtain the raw data from the original study, we were unable to compare the results of the two studies.

1.9 Ethical Clearance

Participation in the study was voluntary. The purpose and scope of the study was presented to all the participants. Necessary precautions were taken to ensure the safety and integrity of data. The survey participants were not required to give any information which could lead to identification of that person. However, since the participants are university students from Nelson Mandela University and Walter Sisulu University (Diggelmann & Cleis, 2014), necessary permission was sought from the appropriate structures in the respective universities. All necessary precautions and guidelines as outlined in the Belmont Report (United States National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, 1979) were strictly adhered to. Also ethical clearance was obtained from the ethics committee at Nelson Mandela University (H15-ENG-ITE-001).

1.10 Chapter Outline

As we have presented the background to the problem, the problem statement and objectives of this study in chapter 1, we will proceed with a detailed literature review in the next chapter. Also the theoretical framework, and its various constructs, which forms the basis of this study, will also be presented in chapter 2. In Chapter 3, we will discuss the methodology in detail, which will include the research process, details of the original study, the instrument design and the details of data collection and analysis. Analysis of the data obtained and the results of the data analysis will be presented in Chapter 4. The discussion of the obtained results will be presented in chapter 5 and finally we will present our conclusions in Chapter 6. A brief outline of the chapters is provided in Table 1.2.

Table 1.2: OUTLINE OF CHAPTERS

Chapter. No	Name	Description
Chapter 1	Introduction	Background to the problem, problem statement & Objectives
Chapter 2	Related Literature	Detailed description on privacy, SNS's, Privacy Calculus & self-disclosure
Chapter 3	Research Methodology	Research Process, Original Study, Instrument Design, Data collection and Analysis
Chapter 4	Analysis	Analysis of data and the results obtained
Chapter 5	Discussion of Results	Discussion of the Results
Chapter 6	Conclusion	Conclusions arrived at

1.11 Conclusion

A detailed road map for conducting this study was outlined in this chapter. A general background and the theoretical basis for this study was also presented. The problem statement and the objectives, that this aims to achieve was clearly stated. The instrument that will be used to collect data was also introduced. The limitations of this study and the ethical clearance process was

detailed next. A detailed discussion regarding related literature will be presented in the next chapter.

Chapter 2: Related Literature

2.1 Introduction

In the previous chapter we have outlined the road map for our study. The objectives of the study was presented after outlining the background to the study and the theoretical framework. We have also seen the significance of this study both from a South African perspective and also for the participating SNS's. In this chapter we will discuss some of the previous works relevant for our study. The concept of information privacy and the possible costs of a privacy violation will be presented. We will also discuss the theoretical model in detail and the various constructs used in the theoretical framework and the rationale behind including them in our theoretical framework. Finally, we will conclude with a brief description of the original study.

2.2 Privacy

Privacy is not entirely a new concept, and the definition or the meaning associated with it is still evolving. People from all over the world have been practicing it in different forms (Diggelmann & Cleis, 2014), even though privacy as a human right originated in the western world.

Many scholars have tried to define privacy. Definitions like "The right to be left alone" (Warren & Brandeis, 1890), "the state of being free from unwanted or undue intrusion or disturbance in one's private life or affairs" or "the voluntary and temporary withdrawal of a person from the general society" (Westin, 1968) were introduced by early researchers. These definitions have however, failed to cover all disciplines and contexts as different people, cultures, and nations have different expectations about how much privacy a person is entitled to or what constitutes an invasion of privacy.

Privacy, *ie* the ability to control or selectively reveal one's own self, material processions, and the information that defines one, is increasingly being accepted as a basic human right (Boyd & Ellison, 2010). The concept of privacy is a modern construct primarily associated with western culture,

and remained virtually unknown in some cultures until recent times (Boyd & Ellison, 2010). In fact, intrusion into a person's private space, own affairs, or wish for solitude, was (and is still) not viewed as a privacy violation in many parts of the world. However, with the rapid spread of the internet, this collectivist cultural mind-set brought about new challenges. Personal information, or information that defines a person, could no longer be constrained or contained by geographical boundaries. This, in turn, increased the significance of information privacy over physical privacy. Physical privacy refers to preventing intrusions into one's physical space, while information privacy refers to the collection and control of information about a person or entity (Pavlou, 2011). As this study focuses on information privacy, in the following sections, the term "privacy" refers to information privacy.

2.3 Information Privacy

Information privacy refers to a person's expectation of privacy in the collection and sharing of personal information. Personal information refers to the collection of personally identifiable information along with information like political beliefs or associations, orientation, financial, educational, employment and health information, affiliations, hobbies and traits, likes and dislikes etc. Personal information can be divided into sensitive and non-sensitive information. Financial, political, health and medical information are generally treated as sensitive information, while contact details, biographical information, shopping trends, hobbies etc. are treated as non-sensitive information (Phelps, D'Souza, & Nowak, 2001). People are generally more comfortable with disclosing non-sensitive personal information than sensitive information. Like physical privacy, researchers have tried to provide a universal definition for information privacy, and have met with similar fate. Definitions like "the option to limit the access others have to one's personal information" (Lange, 2007), "control over others' use of information about oneself" (Acquisti & Grossklags, 2005; Gross & Acquisti, 2005) or a "person's ability to participate in society without having other individuals and organizations collect information about themselves" (Gavison, 1980), were provided by various scholars from different disciplines. However, none of these were applicable across all contexts.

Studies focusing on information privacy has mainly tried to answer three questions, namely; (1) what is (and what is not) privacy, (2) the relationship between privacy and other constructs, and (3) the influence of context on these relationships (Smith, Dinev, & Xu, 2011).

Information privacy refers to a person's expectation of access and control offered (by virtue of legal right or fair information practice) by an entity in the collection and sharing of data about one's self (Solove, 2012). Access can be defined as the person's ability to participate in an information society without being subjected to privacy violation (Introna, 1997). Control can be defined as the level of actual control a person has over the information that has already been transferred to a third party (Smith et al., 2011). Though the domain of privacy partially overlaps the constructs of anonymity, secrecy, and confidentiality, there are fundamental differences between these constructs and privacy (Smith et al., 2011). Anonymity refers to the limited availability of personal identifiers when participating in an information society. Though the concept of privacy and anonymity interrelate, they are not the same. Secrecy refers to the intentional concealment or withholding of information which is negatively valued by the general society (Warren & Laslett, 1977). Privacy and secrecy are not the same, as privacy refers to protecting personal information which is valued by the society. While privacy refers to the control a person has over his information, confidentiality refers to the control which should be exercised by a third party over the information that has already been transferred to that person or entity (Boyd & Ellison, 2010; Smith et al., 2011).

The right to privacy is our right to keep a domain around us, which includes all those things that are part of us, such as our body, home, property, thoughts, feelings, secrets and identity (Ahmed & Zulhuda, 2015). The right to privacy gives us the ability to choose which parts in this domain can be accessed by others, and to control the extent, manner and timing of the use of those parts we choose to disclose.

Privacy law is the area of law concerning the protection and preservation of privacy rights of individuals. While there is no universally accepted privacy law among all countries, some

organizations promote the adoption of certain standards in the countries they operate (Lehikoinen, Olsson, & Toivola, 2008).

In nearly every nation, numerous statutes, constitutional rights, and judicial decisions seek to protect privacy. The first mention of personal privacy is found in Article 12 of the United Nations Universal Declaration of Human Rights (UN, 1948). The declaration focuses on territorial and communications privacy but not on the other dimensions of personal privacy. In the constitutional law of many countries around the globe, privacy is enshrined as a fundamental human right.

Many African countries have failed to legislate privacy laws. This could be due to the African worldview of "Ubuntu" which drives much of African values and social thinking. The African Charter of Human and Peoples' Rights adopted in June 1981 fails to mention privacy at all. The failure to mention privacy indicates that privacy was simply not seen as a necessary right for Africans to live freely and peacefully. However, by 1990, the concept of privacy had begun to emerge as an important right and privacy is mentioned as a right for a child (not all human beings) in the Charter of 1990.

Many African Union leaders have started to feel the need for data privacy laws. This could be partly due to the need for maintaining trade relationships with the western countries, which have strict privacy laws. The African Union approved the African Union Convention on Cyber Security and Personal Data Protection, during the 23rd ordinary session of the Assembly of the Union, held on the 27th of June, 2014. As per the Convention, each member state of the African Union is required to have a national data protection authority (DPA) — an independent administrator to ensure that the processing of personal data is conducted in accordance with the Convention. South Africa is one of the few African countries that have already legislated data privacy laws. Current legislation regarding digital privacy and availability of information in South Africa include:

1. Protection of Personal Information Act, 2013, Act No. 4 of 2013 (POPI)
2. Constitution of the Republic of South Africa 108 of 1996

3. Promotion of Access to Information Act, Act No. 2 of 2000
4. Electronic Communications and Transactions Act, Act No. 25 of 2002

Among these the POPI Act directly relates to protecting the personal information of South African citizens. However, all the privacy laws, SNS privacy policies and privacy settings are useless if the user willingly determine to self-disclose. This attitude of the SNS user, to self-disclose, while having great privacy concerns, is described as privacy-paradox.

Ensuring personal information privacy faces another important challenge. In the physical world a person could, to a certain extent, ensure his privacy by locking the door and limiting access to the personal self. However, this is near impossible in the virtual world where computers can permanently record, store, index, duplicate, analyse and transmit personal information at speeds unimaginable in the physical world. This leads a person to increasingly rely on laws and best practices to protect his privacy. This in turn requires the quantification or categorization of information privacy. As it is difficult to measure privacy as such, most studies have tried to measure privacy concerns (Malhotra, Kim, & Agarwal, 2004; Van Zoonen, 2016).

2.4 Privacy Concerns

Privacy concerns exist wherever uniquely identifiable data relating to a person or persons are collected and stored, in digital form or otherwise. In some cases, these concerns refer to how data are collected, stored, and associated. In other cases, the issue is who is given access to information or the control over others' use of information about oneself. Other issues include the ability to participate in society without having other individuals and organizations collect information about them.

Some studies (Bidwell, 2010; Booysen, 2001; Boyd & Ellison, 2010; Cullen, 2009; Falk & Riel, 2013; Kokolakis, 2017; Lehikoinen et al., 2008; Stutzman & Hartzog, 2012; Westin, 1968) have investigated the effect of privacy experiences, privacy beliefs, privacy awareness, culture and demographics on individual privacy concerns. While other studies (Joinson, 2001; Liu et al., 2004)

have considered privacy concern as the independent variable and have measured the behavioural reactions of the users. They have also investigated the moderating effect of constructs like trust, regulation, privacy policy and cost-benefit analysis. However, it has been noted that these measurements are heavily influenced by the context.

A person may develop different threat perceptions regarding the same personal information accessed by different audiences. For example, a person may possess private information which he does not want to share with anyone, or information which he likes to share only with family members or close friends but not his colleagues. In this context, an individual usually applies the information boundary theory (Xu, Dinev, Smith, & Hart, 2008), to determine whether an information access is considered a potential risk. The information boundary theory posits that each individual forms an informational space (or territory) around him or her with clearly defined boundaries, and such boundaries determine what information can be shared. Depending on the situational and personal factors, an attempt by an external entity to penetrate these boundaries may be deemed a threat. However, it has been noticed that an individual can be enticed into communicating his or her personal information to a wider audience if sufficient motivation exists. This phenomenon of disclosing personal information to a wider audience on an online platform is called self-disclosure (Derlaga & Berg, 2013).

Self-disclosure is a process of communication by which one person reveals information about himself or herself to another (Krasnova, Veltri, & Günther, 2012). The information can include thoughts, feelings, aspirations, goals, failures, successes, fears, and dreams, as well as one's likes, dislikes, and favourites. When a user self-discloses personal information on an online platform, essentially the user is transferring the ownership of such information to a third party. The recipient can view, store, duplicate, index, analyse and transmit this information. This will lead to the loss of privacy to the person who has disclosed that information.

Millions of users willingly transmit ownership of their personal information onto online platforms every day, often knowing that they are sacrificing their privacy. To fully understand this

phenomenon, one needs a basic understanding about Social Networking Services (SNS's) and their related business model.

2.5 Social Networking Services

SNS's were originally conceived as a social exchange medium for people and communities who share common interests. Over the years, the focus has shifted to converge around users of the platform (Xu, Yang, Cheng, & Lim, 2014). Each individual user gets a feeling that he or she is the epicentre of the system. SNS's can be defined as web based services which allow their users to publish their personal profile along with their list of connections, while being allowed to view and navigate the profiles and connections of other users within the system. There are many SNS's available supporting a wide range of interests. While some SNS's cater for niche audiences based on ethnicity, nationality, or shared interests (Gonzalez, 2010), most of them are tailored around supporting pre-existing offline social networks. Facebook and Myspace are examples of SNSs which help users to maintain pre-existing relationships at a relatively low cost. These services help the users create a profile page by using the information which the user provides at the time of registering for these services. Once the profile page is created, users can search for and create a network of connections with other users sharing the service. Users can display pictures in their online albums, describe their personal interests and hobbies, express their views, "like", or "tag" items, and list their friends and social networks. SNSs also allows users to interact with one another through comments and messages.

SNS users can be divided as follows: passive users, who have an account but access it very rarely and almost never update their information, observers or passive followers, who access the account only to look at other users profiles, irregularly post information on their account, especially only for major events or social occasions, and addicts, who access their account and update their profile information or status almost daily (Brandtzaeg & Heim, 2011).

SNSs platforms like Facebook, want all their members to be addicts, as self-disclosure of personal information by users on SNSs play a vital role in the self-sustainability of online social networking service provider platforms (Xu & Chen, 2013). SNSs collate the personal information disclosed by users and sell it to third party companies and organizations (Fourli, 2010; Krombholz, Merkl, & Weippl, 2012). The companies and organizations who receive this information use it for targeted advertisement and marketing, among other things. Since Facebook is the most widely used SNS, and this study focuses on understanding self-disclosure patterns of South African Facebook users.

2.6 Facebook

Facebook is the most popular SNS, with more than 2.4 billion active users on Facebook alone and the company claims (www.newsroom.fb.com) that around 2.71 billion users use any of their services (Facebook, Instagram, WhatsApp or Messenger). This represents 33% of all internet users. Even though Facebook's user base is dominated by adults over the age of 25, they still have around 50 million users who are below the age of 25 (www.facebook.com/info). Usage among seniors continues to increase. Some 56% of internet users aged 65 and older now use Facebook. Women are also particularly likely to use Facebook compared with men (http://www.pewinternet.org/). Since Facebook is experiencing more active user sign-up in countries like India, Brazil and African countries, they have turned more attention towards these places. In South Africa also, Facebook is the leading SNS with 14 million active users. The number of users is roughly split into two half's based on gender, with woman being more active in the 13 to 25 age group (Alexa.com).

Facebook was created in 2004 and was primarily aimed at university students. Gradually they started including schools and by 2006 anyone with a valid e-mail address could open an account with Facebook. Facebook is primarily aimed at maintaining pre-existing relationships at a relatively low cost, rather than for making new connections or relationships. Even though the platform does not encourage making contacts with strangers, it is mostly left to the discretion of the users. Most of the active users primarily use the platform to maintain pre-existing relationships, rather than to meet new people (Ellison et al., 2007). Facebook requires users to disclose a certain amount of personally identifiable information at the time of registration. Apart from providing personally

identifiable information, SNS users reveal other private information such as hobbies, tastes in music, books, movies, relationship status and sexual preferences on their profiles. Furthermore, it is common to upload one's photos and communicate news on the Wall or by posting comments. Self-disclosure of personal information can be generally divided into three categories namely; Personal information, contact information and interest information. Details like name, age, date of birth, place of birth, home town, status, and school and university information all falls under personal information. Contact information includes one's phone number, e-mail address, current residential address and in general any details about you that can be used to contact you or that gives an indication about one's willingness to be contacted by a particular person. Interest information includes all information about ones Likes, status updates, comments and messages to other users, places visited, events attended, and so forth. Of these categories, personal interest information is the kind of personal information which is of greater interest to the SNS service provider. This information will help the SNS service provider and other third party companies to understand user likes, dislikes, strengths, weaknesses, personalities and other personal traits.

Sustaining Facebook's success and popularity could be difficult if it does not adapt with the changing needs of the customers. As switching costs are relatively low, users of SNS can switch from one service to the other at a relatively low cost. SNS like Friendster, Myspace, and Orkut could not sustain their early success. Understanding the privacy concerns and benefits which influence user participation in an SNS is essential for ensuring the sustainability of platform. Facebook does have a privacy policy which incorporates best practices from around the world.

When it started as a Harvard University Network in 2004, it did not have any privacy policy. The contents which one shared over the network was accessible to anyone inside the network. Facebook slowly started expanding to include other networks, starting with prestigious universities. Gradually they started including schools, some companies and regional networks and finally by 2006 the service became accessible to the general public (anyone with any e-mail address). However, at this point, Facebook did not allow its users to share content with anyone

outside their respective networks. Facebook discontinued the practice of requiring users to join a specific network in 2009, as some networks started crossing geographic boundaries.

Even though Facebook currently has a comprehensive privacy policy and privacy settings at the disposal of the users, there is significant mismatch between the available privacy settings and user expectations (Liu, Gummadi, Krishnamurthy, & Mislove, 2011). Many people face difficulties in choosing and configuring the available privacy settings (Madejski, Johnson, and Bellovin, 2012). Failure to understand the limitations of privacy settings is also a concern. Facebook modified and simplified their privacy settings to make it less complicated for users. The user acceptance of these changes to their privacy settings has helped Facebook to regain public trust in the platform. This is evident from the increase in unique Facebook user accounts from 608 million in 2010 to over 1.4 billion in 2016. Facebook regularly updates its privacy features to make it more user-friendly and to align its privacy policy with the changing information privacy rules and regulations across the world.

2.7 Privacy paradox

Facebook offers a great platform for its users to stay connected and to share content. The privacy concerns of users are not preventing them from self-disclosing. This attitude of SNS users has been the subject of many research studies (Krasnova, Veltri, & Günther, 2012; Krasnova & Veltri 2010; Kwak, Choi, & Lee, 2014; Li-Barber, 2012; Trepte & Reinecke, 2013) around the world and several researchers have offered many reasons and theories to explain this phenomenon. This study uses the most widely used and accepted theory, *i.e.* the Privacy Calculus theory which encompasses most of the reasons offered. The following section briefly discusses some of the explanations offered by these researchers and then proceeds with a detailed explanation of our theoretical framework and its constructs.

2.8 Related studies on the Privacy-paradox phenomenon

A discrepancy between privacy concerns and actual behaviour, or privacy paradox, could be the result of the competing demand between using SNS platform to participate in an online

community or be left out in the cold. However, the amount of actual self-disclosure is influenced by several factors like culture, age, gender, attitude, subjective norm, bounded rationality and hyperbolic discounting.

Culture, age and demographics have been one of the biggest factors influencing SNS self-disclosure. (Cullen, 2009; Falk & Riel, 2013; Vasalou, Joinson, & Courvoisier, 2010; Zukowski & Brown, 2007). Though women are more active than men in using SNSs, men provide their telephone numbers and addresses on their SNS profiles more often than women. However, women post their preferences about movies, books, and religion more often (gender differences in privacy related measures). Though studies have come up with different and often conflicting results, age is another significant factor which influences self-disclosure. Young people were considered to self-disclose more than the more matured SNS users. However, recent studies observe that young people care about their privacy and adopt privacy protective behaviour like refusal and misrepresentation (Kokolakis, 2017). National culture is another factor which influences self-disclosure (Cullen, 2009).

Attitude is another important factor which influences the SNS user's self-disclosure behaviour. Many users, though they are aware of the privacy threats often consider that it will never happen to them (Kehr, Kowatsch, Wentzel, & Fleisch, 2015; Krasnova et al., 2009).

Subjective norm is believed to influence intention to disclose in the context of an SNS (Lehikoinen et al., 2008). If in a given social network site, everyone tended to share real personal information with one another, then that behaviour would be considered a subjective norm on that site.

Bounded rationality (Yu, Hu, & Cheng, 2015) and hyperbolic discounting (Kokolakis, 2017) are further significant factors identified by the researchers. Bounded rationality is the idea that when individuals make decisions, their rationality is limited by the information they have, the cognitive limitations of their minds, and the time available to make the decision. Hyperbolic discounting refers to the tendency for people to discount future threats over immediate gratification.

National culture influences bounded rationality and hyperbolic discounting, attitude and subjective norm to a great extent. The impact of national culture on the above mentioned attitudes is briefly explained in section 2.12. Our study focuses on the perceptions of South African Facebook users on self-disclosure, and how they make the decision to self-disclose. We argue that SNS users perform a cost-benefit analysis, before they decide to self-disclose. This cost benefit analysis is referred to as privacy calculus.

2.9 Privacy Calculus Theory

According to the Theory of Reasoned Action (TRA) and the Theory of Planned Behaviour (TPB) (Fishbein, 1979), the adoption of some behaviours must be directly related to some benefit. The Privacy Calculus Theory which is based on TRA and TPB (Li, 2012), assigns an economic value to an individual's personal information and postulates that an SNS user conducts a cost-benefit analysis before deciding to self-disclose. The cost of self-disclosure is privacy violation that could take place and the resulting damage caused. The benefits of using SNSs are enjoyment, self-presentation and relationship maintenance. This cost-benefit analysis is again influenced by factors like trust in other members of the platform, trust in the provider, trust in legal assurance, awareness regarding the available privacy controls and the user's perceived control. Studies have shown that national cultures influence all the above mentioned constructs (Cullen, 2009; Falk & Riel, 2013; Krasnova & Veltri, 2010). In the next section, the costs, benefits and the moderating factors, and the theoretical framework adopted for this study is explained in detail.

2.10 Theoretical Framework

This study is a replication of another study conducted in Germany and the US to understand the perceptions of German and US Facebook users regarding perceived costs, benefits and self-disclosure. The researchers developed a theoretical framework based on the privacy calculus theory. This framework empirically explores the simultaneous effect of personal beliefs, including privacy costs, benefits, and moderating factors all associated with inhibiting or facilitating the intention to self-disclose. This framework argues that, before the user decides to self-disclose, a

cost-benefit analysis is conducted, and if the benefits outweigh the costs, the user self-discloses. This cost-benefit analysis is in turn influenced by other moderating factors. The following sub-sections discuss the related benefits and costs of using an SNS and the moderating factors that influence the cost-benefit analysis.

Normally people will not give away their personal information, if they do not see any benefits in doing so (J. Phelps, Nowak, Ferrell, & Marketing, 2000). People are motivated to part with their personal information in a number of ways. Loyalty programs aimed at understanding shopping behaviour or offering cash, coupons or discounts in exchange for parting with personal information are some of the methods employed for gathering personal information. However, the perceived benefits on SNSs are not discounts or free services, but the foundation of social capital or community attachment. Enjoyment, self-presentation, relationship maintenance and the accumulation of social capital are the benefits of being active on SNS (Krasnova, Veltri, & Günther, 2012).

Enjoyment is considered as the most important benefit of being an SNS user. The intensity of Facebook use was found to be positively correlated with an increase in life satisfaction and self-esteem (Alhabash, Park, Kononova, Chiang, & Wise, 2012). Furthermore, perceived ease-of-use or enjoyment is an important determinant of perceived benefits that a user derives from using an SNS.

The opportunity to create a completely new identity is another benefit of using a SNS like Facebook. The process of creating a new virtual identity is termed as self-presentation. Identity is an important part of the self-concept and can be defined as "something by which we are known to others" (Zhao, Grasmuck, & Martin, 2008). It comprises of two different processes, namely (1) Announcement where one announces or transmit their identity, and (2) placement whereby the audience should receive or accept our announcement (Brandtzæg & Heim, 2009; Krasnova, Spiekermann, Koroleva, & Hildebrand, 2010). In an offline world, it is very difficult to pretend to be someone else which is in sharp contrast to or inconsistent with our physical appearance and our background information (Seidman, 2013). But in the online environment, it becomes possible

for individuals to interact with one another on the Internet in fully disembodied text mode (combined with advanced graphics, applications etc.) that reveals nothing about their physical characteristics. In a normal physical world where there are established social norms, any deviation from those norms will be punished or ridiculed. In such a world a person will be forced to wear masks to hide their true selves. However, in the online world, people can take these masks off and can express their true selves, by taking advantage of the anonymity offered by the online world. Once a user has created his or her identity, he or she can enhance it by posting photos, videos or other applications, expressing their views on issues or other posts, and also by displaying their list of connections.

SNSs help their users to search for and maintain contacts with former relationships at a relatively low cost. It can also be used for meeting new people based on shared interests and create a new circle of friends. More advanced internet techniques have provided diverse methods to maintain relationships online, such as address lists with power function and video conference. This has enabled the number of weak ties an SNS user can handle to sharply increase (Ellison, Vitak, Gray, & Lampe, 2014). Therefore, relationship maintenance is another significant advantage of participating in an SNS.

Another advantage an SNS user derives from participation is the sense of belonging and the accumulation of social capital. The accumulation of social capital permits people to attain rich resources, such as information linkages, organizing and cooperative abilities and tapping into a web of relationships.

While SNSs offer many benefits to their participating members, these could come at the expense of personal privacy. The resulting damage emanating from a possible privacy violation could affect an individual physically, emotionally or financially. This is considered as the cost of self-disclosure on an SNS.

Social networks and third-party applications on social networks often gather data from users in order to sell them to marketing data starved companies, like advertisers or software developers

(Cătoiu, Orzan, Macovei, & Iconaru, 2014; Young & Quan-Haase, 2009). Third party applications collect personally identifiable information and behaviour traits of users using "cookies", click-stream analysis, data mining techniques and data-warehousing technology. For example, SNSs have used consumer profile information, their social relationships, and their behaviour to upload advertisements on their social network platform and elsewhere on the Web. Demographic information serves to segment people and, coupled with behaviours, helps SNS providers to tailor advertising (Tucker, 2014). When people use applications or join groups or fan pages, this information can be shared with third parties. Though users derive some advantages, like personalization and discounts for specific products from these legitimate uses of personal information, they can also be exposed to damages as a result of these privacy violations.

The privacy concerns faced by SNS users include cyber stalking, re-identification, building a digital dossier, data security (Gross & Acquisti, 2005), price discrimination, blackmailing, surveillance and cyber bullying (Kwan & Skoric, 2013). The perceived likelihood of a privacy violation and the resultant damage caused, informs the privacy concerns of SNS users. Also, SNS users' privacy concerns are determined mainly by the perceived likelihood of a violation and much less by the perceived damage that can be caused (Krasnova et al., 2009).

Cyber stalking is the use of the Internet or other electronic means to stalk an individual. Using information available on the profile page of an individual, his or her physical location can be determined in real time. An active SNS user who regularly publishes content including photos and schedules is at risk of being cyber stalked. A cyber stalker relies upon the anonymity afforded by the Internet to allow them to stalk their victim without being detected.

Re-identification is the process by which anonymised personal data is matched with its true owner through data linkage techniques. Even though a user misrepresents or limits information provided on an SNS, advanced data mining technologies makes it possible to link multiple sets of data from different platforms. Even a photograph can prove to be an identifier, as powerful face recognition software is now available (Acquisti, Gross, & Stutzman, 2014).

The privacy implications of revealing personal and sensitive information may extend beyond their immediate impact. As the technology for duplicating, storing and mining data is getting faster and cheaper, it is possible to build a digital dossier of the SNS user. Even ones personality can be deducted from the information that one provides on SNS (Youyou et al., 2015). College students, even if currently not concerned about the visibility of their personal information, may become concerned as they enter sensitive and delicate jobs a few years from now - when the data currently mined could still be available.

Bullying which takes place over communication platforms like email, chat rooms, mobile phones and websites is termed cyberbullying. Cyberbullying is more dangerous and damaging than normal bullying because of the presence of large audience, and because the information can be stored, duplicated and transmitted over long distances and is easily searchable (Willard, 2006).

Another possible privacy violation involves government agencies. With the recent spate of terrorist activities across the world and the resultant "islamophobia", people are willingly transferring their digital privacy to state agencies, and governments across the world are more than willing to comply by enacting laws which gives no regard to individual privacy.

Furthermore, participation in SNS platforms can cause other emotional problems (Sagioglou & Greitemeyer, 2014) like social comparison and envy, which could endanger an SNS user's life satisfaction (Krasnova, Wenninger, Widjaja, & Buxmann, 2013). Also many SNS users have a tendency of forwarding the information which they get, without properly checking the authenticity or source of that information.

All these privacy violations can cause a great amount of damage to an SNS user who falls victim to such privacy violations. Even with such high costs associated with participating in an SNS, users still self-disclose, since they feel that the benefits outweigh the costs. However, this cost-benefit analysis is also influenced by other moderating factors as discussed in the following sub-section.

2.11 Moderating Factors

Moderating factors incorporated into the theoretical framework include trust, control and awareness. These factors influence the cost-benefit analysis and ultimately the intention to self-disclose to a great extent.

Trust in the service provider or SNS platform, the other users of the network, and legal assurance are the trust factors that are incorporated into our theoretical framework. Trust may entice users to believe that they can realise the benefits, without suffering the costs. In other words, if they have trust in the SNS platform, the users and legal assurance, SNS users may be led to believe that the likelihood and resultant damage of a privacy violation is negligible.

Awareness regarding privacy policies, laws, and the available privacy settings will have a positive impact on the amount of perceived control a user has over self-disclosed information. This perceived control can tilt the scales towards the benefits side, when the user conducts the privacy calculus, and in turn could positively influence the decision to self-disclose.

Several studies have concluded that a variety of factors affect a user's decision to self-disclose personal information on an SNS (Christofides, Muise, & Desmarais, 2009; Laufer & Wolfe, 1977; Livingstone, 2008). According to Livingstone (2008), adolescents and university students do not perceive information like age, religion, political affiliation, sexual preferences as private and as such may be more willing to disclose them. Children may have an entirely different perception about privacy (Laufer & Wolfe, 1977), and adults may not disclose the kind of information that they have shared when they were young. Factors like gender also influences disclosure behaviour (Fogel & Nehmad, 2009), and it has been noticed that women disclose more although they perceive more damage from a perceived privacy violation. The behavioural intention to self-disclose is also driven by the actions of other members of the group that one belongs to. If the members of a group self-disclose more it will elicit similar reaction from other members of the group. The need to belong and the need for popularity are also found to be significant predictors

of self-disclosure (Gangadharbatla, 2008). Time spent on Facebook, account length, trust, self-esteem and awareness of the consequences of self-disclosure, also affects the nature of self-disclosure.

2.12 The original study

This study is a replication of another study titled "Privacy Calculus on Social Networking Sites: Explorative Evidence from Germany and USA", undertaken by Krasnova and Veltri (2010) . As user self-disclosure drives the sustainability of SNSs, it is important for the providers to understand the factors that affect self-disclosure. The original study was aimed at determining the factors that influence user self-disclosure and whether the national culture influences these factors. To achieve that a survey was conducted to explore the differences in perceptions of disclosure-relevant determinants between German and US Facebook users.

They developed a conceptual framework based on the privacy calculus theory. Privacy calculus theory posits that SNS users conduct a cost-benefit analysis before they decide to self-disclose. In other words, an SNS user will only self-disclose their private information if and only if the benefits of doing so outweigh the costs associated with it. After conducting an extensive literature review, Krasnova and Veltri (2010) developed the theoretical framework for the study. The theoretical framework incorporated the costs, benefits and the moderating factors that affect user self-disclosure.

Relationship Maintenance, Entertainment and Self-Presentation were determined as the benefits of participating in SNSs, while privacy concerns informed by the perceived damage and perceived likelihood of a privacy violation were considered as the cost. Trust in legal framework, the other users of the network, and the service provider and awareness regarding the various control features of the platform were considered as the moderating factors. The determinants of the theoretical framework is explained in detail in the previous chapter.

An instrument was developed based on the theoretical framework and a survey was administered among US and Germen university students. Each construct was measured with several items on a 7-point Likert scale. 1=Strongly Disagree (SD); 2=Disagree; 3=Slightly Disagree; 4=Neutral; 5=Slightly Agree; 6=Agree; 7=Strongly Agree (SA). Participants for the online survey were recruited among FB users by posting announcements on university email lists, campus bulletin boards and on FB group walls. Participants were also offered 5 US Dollar in the US and 5 Euro in Germany. A total of 237 responses were collected in Germany and 254 in the USA of which 138 German and 193 US responses were finally included into the subsequent analysis.

The mean responses of the two samples were determined for the various constructs and the results were analysed. The differences in the values were explained using the values of national culture as derived by Hofstede. According to Hofstede's calculations both Germans and Americans have low perception of Power Distance (PDI) in society because they believe in opportunity and equality for each citizen and hence tend to reject unequal distribution of power among societal levels. Both countries are rated high on masculinity (MAS) as well, indicating that they are self-confident, forceful and competitive personalities and would enjoy ego-enhancing activities. Both Germany and US are rated low on the Long Term Orientation (LTO) dimension as well, which indicates that they value instant gratification as opposed to future rewards. However, when it comes to Individualism (IDV) and Uncertainty Avoidance (UAI), these countries differ significantly. US society is found to be more individualistic than the Germans. This means that the Germans are more concerned about potential consequences of their behaviour than the Americans. And finally since the Germans exhibit a much higher UAI than the Americans, they can be expected to more risk averse.

The researchers found out that the Americans perceive more benefits from using Facebook than the Germans. The US Facebook users derive more enjoyment, thinks it is very useful for relationship maintenance and self-presentation. When it comes to privacy concerns, the US Facebook users were more concerned than the Germans, that their personal information can be misused or misinterpreted and ultimately used against them. However, the US Facebook users

were less concerned than the Germans when it comes to the Perceived Likelihood and Perceived Damage from a potential privacy violation. The Americans think that they are less likely to be subjected to a privacy violation and if at all it happens, they perceive little damage from such a violation. Though both the US and German users generally do not trust the other users in the network and the legal framework, their attitude differs when it comes to trusting the service provider. The German users generally do not trust the service provider (this could be also due to the fact that Facebook is a foreign company for them), while their US counterparts generally agree that they can trust the service provider (Facebook). The US Facebook users tends to be a bit more aware regarding Facebook's information privacy policy than the Germans. However, both US and German users think that Facebook is clearly not communicating or not being fully transparent regarding what information can be collected and what it is being used for. The Americans perceive more control over their personal information that they have disclosed on the network than the Germans. And finally the researchers found out that German Facebook users self-disclose significantly less personal information than the Americans.

The researchers concluded by recommending that to ensure the sustainability of SNS platforms, much emphasis should be given to the national cultures. PDI has a positive influence on self-disclosure, trust in SNS provider and other members and negative influence on privacy concerns. Individuals with high Uncertainty Avoidance will be less tolerant of uncertainty and ambiguity. UAI has a positive influence on perceived likelihood of a privacy violation, perceived damage and privacy concerns. However, UAI is negatively correlated with self-disclosure, trust in SNS provider, members and legal assurance, perceived control and expected benefits. IDV is positively correlated with perceived likelihood of a privacy violation, perceived damage, privacy concerns, awareness and expected benefits. It is negatively correlated with trust in SNS provider and members. Team members with high masculinity place a high emphasis on material possessions, including money. MAS will have a positive influence on privacy concerns, perceived likelihood of a violation, perceived damage, awareness and perceived control and will have a negative influence on trust in SNS provider and other members. Communities with high LTO will disclose less, expects less benefits and will have little or no trust in SNS provider, other members and legal assurance.

LTO will positively influence perceived likelihood of a privacy violation, perceived damage and privacy concerns. People in societies classified by a high score in IND generally exhibit a willingness to realise their impulses and desires with regard to enjoying life and having fun. They possess a positive attitude and have a tendency towards optimism. In addition, they place a higher degree of importance on leisure time, act as they please and spend money as they wish.

2.13 Conclusion

The influence of the dimensions of National culture on the perceived costs, benefits and self-disclosure of SNS users makes a South African study worthwhile. This study is aimed at understanding the perceptions of South African SNS users regarding the perceived benefits, costs, moderating factors and self-disclosure, using the privacy calculus theory. This is a replication of a similar study conducted by Krasnova and Veltri (2010), titled "Privacy calculus on social networking sites: Explorative evidence from Germany and USA". The original study aimed at understanding the difference in perceptions of German and USA Facebook users on the determinants of self-disclosure and the amount of perceived self-disclosure. A brief outline of the methodology, measurement, instrument, and analysis is provided in the next chapter.

Chapter 3: Research Methodology

3.1 Introduction

The previous chapter discussed the literature relating to information privacy, privacy concerns, SNSs, privacy paradox, the cost, benefits and moderating factors influencing an SNS user's decision to self-disclose. It concluded with a discussion on the original study. This study titled "Exploring the privacy calculus on social networking services (SNS) from a South African perspective" is a replication of the original study conducted by Krasnova and Veltri (2010), entitled "Privacy Calculus on Social Networking Sites: Explorative Evidence from Germany and USA". As this is a replication study, the methodology and instruments used in the original study were used for this study. In the following sections, the details of the research process including instrument design, sampling, ethical clearance, administration and data collection and data analysis is outlined in detail. Figure 3.1 provides a roadmap for this chapter.

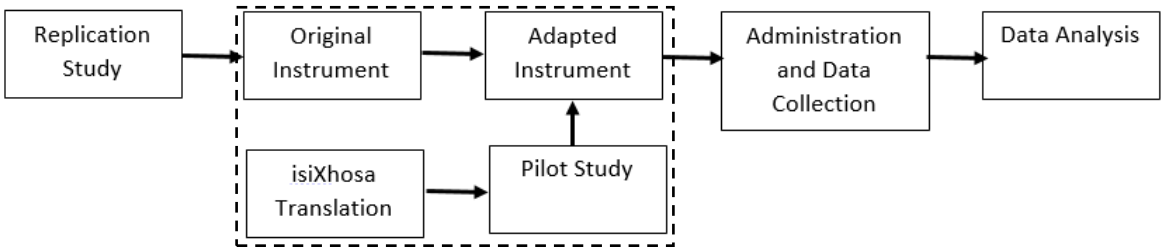


Figure 3.1: ROAD MAP FOR THIS CHAPTER

3.2 Replication Study

Replication represents the deliberate or conscious repetition of a previous research study, using the same methods, intended to confirm or extend previously or simultaneously obtained findings. When researchers can successfully replicate a study on a different sample set, like different subjects, age groups, races, locations, cultures or any such variables, then the original study can be considered as generalizable. While generalizing a study, the researcher has to make sure that it can withstand the test of external validity. Or in other words generalization is the extent to which relations among variables in research studies can be demonstrated among a wide

variety of people and across different settings. When the design of a research study is generalizable to additional populations and settings, the study demonstrates external validity. As the original study involved participants from two different national cultures, and as the researchers were trying to establish the effect of culture on people's perceptions on the determinants of self-disclosure, it can be argued that this study is generalizable across different national cultures. In other words, the original study has already been replicated across different national cultures. This research is a replication of the original study in South Africa using the same design, framework, methods and instrument used in the original study.

Replication will also be considered as an unnecessary exercise, if the researcher is not able to establish the significance of such an endeavour. The replication of the above mentioned study is quite important both from the national and academic point of view. By replicating this study, the influence of culture on the constructs of user self-disclosure and the amount of actual self-disclosure can be determined. Understanding the national culture of a country is very important for organizations planning to gain a foothold within that country. It is even more significant for policy makers as any policy will be a failure if they fail to understand and incorporate the culture of people it is expected to help. Not many studies have been conducted to determine the national culture of South Africa. The few studies that have been conducted came up with contradicting results.

To achieve the objectives of this study, the determinants and moderating factors of South African user self-disclosure was measured using the instrument adopted from the original study. Necessary permission was obtained from the researchers who conducted the original study, before adopting the instrument. The original instrument was slightly modified to include two more sections. The original instrument was modified only to the extent necessary to accommodate the South African context and the objectives of this study. The necessary ethical clearance was also obtained before integrating the changes. The details of the instrument design and the changes made is explained in section 3.3. The benefits, costs, moderating factors and the actual user self-disclosure as outlined in the conceptual framework was measured using the described instrument. A brief description of these constructs and the moderating effect of national culture is provided in the following sections.

3.3 Instrument Design

This section details the particulars of instrument design and the changes that were adopted to suit the unique South African context.

3.3.1 The original instrument

An instrument in the form of a questionnaire was developed by Krasnova and Veltri (2010) for the purposes of the original study. The instrument was intended to understand the differences in perceptions of US and German users on the various constructs (based on the conceptual framework) of user self-disclosure. Every construct was measured on a seven point Likert scale. The scale started from 1 which stood for "strongly disagree", 2 (disagree), 3 (slightly disagree), 4 (neutral), 5 (slightly agree), 6 (agree), and 7 which stood for "strongly agree". For some constructs, pre-tested scales were available. But in other cases, the scales had to be modified or developed anew to address the unique context of SNS. The instrument consisted of 10 sections, namely Expected Benefits, Privacy Concerns, Perceived Damage, Perceived Likelihood, Trust in SNS Provider, Trust in SNS Users, Trust in Legal Assurance, Awareness, Perceived Control, and Self-Disclosure. Under these main sections there was of a total of 54 questions, to measure the various determinants. A summary of the questionnaire is provided in Table 3.1 (Refer to Appendix A for the detailed questionnaire). Participants were asked to rate each of the questions based on their perceptions. As this study is a replication of the original study, it adopted the same instrument. However, some changes were made to the original instrument to address the unique South African context and to realize the objectives of this study.

Table 3.1: SUMMARY OF THE ORIGINAL QUESTIONNAIRE

Section	Construct Name	Number of Questions
3	Expected Benefits	Q 3.1 – Q 3.7 (7)
4	Privacy Concerns	Q 4.1 – Q 4.4 (4)
5	Perceived Damage	Q 5.1 – Q 5.7 (7)

6	Perceived Likelihood	Q 6.1 – Q 6.7 (7)
7	Trust in SNS Provider	Q 7.1 – Q 7.7 (7)
8	Trust in SNS Members	Q 8.1 – Q 8.6 (6)
9	Trust in Legal Assurance	Q 9.1 – Q 9.3 (3)
10	Awareness	Q 10.1 – Q 10.2 (2)
11	Control	Q 11.1 – Q 11.5 (5)
12	Self-Disclosure	Q 12.1 – Q 12.6 (6)

3.3.2 Changes to the Original Instrument

While replicating the original study and adopting the instrument, the original English wording of every item in the questionnaire was used. Care was taken to ensure that the replication was complete and faithful to the objectives of the original study except for the nationality of the respondents. Two additional sections were added to the original instrument. The instrument used for this study consists of 12 sections as opposed to 10 sections in the original instrument. All the questions in the original instrument were retained in the new instrument, from section 3 to 12, to measure the perceptions of SNS users on the various constructs as described in the conceptual framework.

In Section 1 the participants were asked to provide their age, gender, race and name of the school where they have completed their schooling. As the target population consisted of undergraduate students from both Walter Sisulu University and Nelson Mandela University, they were also asked for the institution where they were currently registered and the number of years they were registered in a tertiary institution. They were also asked to grade their perceived end-user computing skills on a scale of 1 to 5, with 1 indicating that “they have no skills’ and 5 indicating that “they were highly skilled”.

In Section 2, the participants were asked to provide general information regarding their Facebook use and activities. They were asked questions like “How do you access Facebook?”, “How long have you been using Facebook?”, “How frequently do you use Facebook?” and finally for their “Activities on Facebook”. A brief outline of the two new sections added to the original questionnaire is outlined in Table 3.2 (Refer to Appendix A on page for a detailed questionnaire.).

Table 3.2: SUMMARY OF ADDITIONAL TWO SECTIONS ADDED TO THE ORIGINAL QUESTIONNAIRE

Section	Construct Name	Number of Questions
1	Demographics	Q 1.1 – Q 1.8 (8)
2	Facebook usage pattern and general computer skills.	Q 2.1 – Q 2.4 (4)

Apart from these two new sections that were added to the original questionnaire, we also provided the isiXhosa translation of each of the items in the questionnaire. Great care was taken to ensure that the original meaning of each item was retained. The next section provides details regarding the translation of the questionnaire from English to isiXhosa.

3.3.3 isiXhosa version of the original instrument

An official at Walter Sisulu University University was approached for translating the questionnaire from English to isiXhosa. She completed the translation, and handed over the text. The translation along with the original English version of the questionnaire was forwarded to the language department at WSU, where two staff members checked it. They returned the text, commenting that it is an acceptable literary isiXhosa translation of the original questionnaire.

The isiXhosa translation of the original questions was included in the original English questionnaire. The translation for each question was included right below the English version of the question. After that the questionnaire was released for pilot study. It was piloted among postgraduate students at Nelson Mandela University and Walter Sisulu University and they were asked to comment on the questions, the structure of the questionnaire and the isiXhosa

translation. A total of 7 students participated in the pilot study and they provided feedback on the structure of the questionnaire and the translation for some of the questions.

The questionnaire along with the comments from the students on translation was forwarded to another SATI Accredited Professional Translator for English and isiXhosa. She made some changes to the translation. After that the original questionnaire and the new translation (excluding the feedback from the students) was forwarded to a third SATI Accredited Professional Translator for English and isiXhosa. The third translator belonged to a company dedicated to professional translation. The third translator was approached to ensure objectivity and to get feedback from a new perspective. She approved the translation without any changes and stamped and signed the questionnaire (with the translated text in isiXhosa). Two undergraduate students from Walter Sisulu University was given the isiXhosa version of the questionnaire and they were asked to translate it back to English. Though their English translation was not an exact English version of the original questionnaire, the English translation communicated almost the same message. Changes to the structure and formatting of the questionnaire was made with the help of Professor Reinhardt A Botha from Nelson Mandela University. After that the questionnaire was piloted for a second time at Nelson Mandela University. This time the students did not have any problems with the questionnaire.

After this stage the questionnaire was approved for collecting data from the participants. As the sample was derived from registered undergraduate students of Walter Sisulu University and Nelson Mandela University, the link for completing the questionnaire was sent to official e-mail accounts of all undergraduate students registered at Nelson Mandela University and WSU.

3.4 Sampling

Convenience sampling was used to select the participants. Convenience sampling is a specific type of non-probability sampling method that relies on data collection from population members who are conveniently available to participate in study. In this sampling method the first available primary data source will be used for the research without additional requirements. In convenience sampling no inclusion criteria is identified prior to the selection of subjects. All

subjects are invited to participate. This approach was used because of two reasons. Firstly the original study used convenience sampling to obtain data. And secondly due to the limitations of the researchers to administer the instrument across South Africa in all the Universities and campuses belonging to these Universities. The sample was derived from undergraduate students registered at Walter Sisulu University and Nelson Mandela University. All registered undergraduate students were invited to participate. The sample derived did not reflect the racial, gender or cultural demographics of South Africa, as the instrument was sent to all registered students and the participation was voluntary. Walter Sisulu University (NMD campus) is located in Mthatha, which is the former capital of Transkei, and is still considered as a rural area. Walter Sisulu University mainly serves the community in and around the former Transkei region. Nelson Mandela University is located in Port Elizabeth, which is one of the biggest cities in South Africa. As we derived sample from a formerly disadvantaged rural University, and also from a University located in the city, we believe that the sample will be representative, as far as the urban-Rural digital divide is concerned.

University students have been selected for three reasons. Firstly, the original US and German study involved university students; secondly university students are often forerunners in the adoption of new communication technologies, and their communication networks tend to be dense and multi-layered; and lastly a great majority of SNS users in South Africa are currently enrolled in universities or are university graduates

In the original study a total of 237 and 254 responses were collected from Germany and US respectively and a total of 138 German and 193 US responses were found to be valid. Since this is a replication of the study we aimed for at least 250 students as participants from Nelson Mandela University and Walter Sisulu University (WSU (NMD Campus – Former University of Transkei)). However, our sample size was limited to 244 undergraduate students. All precautions and instructions as stipulated by the ethics committee of Nelson Mandela University and the Directorate of Research at Walter Sisulu University was strictly adhered to while collecting the data. The details of ethical clearance and the conditions attached is explained in the next section.

3.5 Ethical Clearance

The ethical clearance (Ref. No: H15-ENG-ITE 001) for the study was issued by the Research Ethics Committee (Human) at Nelson Mandela University, on 1st July, 2015. The ethical clearance certificate stipulated that the researchers should inform the ethics committee of any changes in the agreed methodology and protocols. After obtaining the ethical clearance certificate from Nelson Mandela University, an application was submitted to the office of the DVC (AA&R) at Walter Sisulu University, *via* the Directorate of Research Development, for the necessary permission to obtain data from Walter Sisulu University students. The necessary permission to obtain data from registered undergraduate students was issued by the Directorate of Research Development, on condition that a completed copy of the study should be submitted to the Department of Research Innovation & Development at Walter Sisulu University.

The objectives, rationale, methodology, sampling and data collection methods of the study was communicated to the ethics committee at Nelson Mandela University. The researchers agreed to follow certain procedures while selecting the sample, administering the instrument and obtaining data from the target population, to do full justice to the objectives and rationale of the study.

As the primary objective of the research is to determine the impact of national culture on self-disclosure and privacy calculus, cultural derivation and some background information like age, gender, level of education, address of school where the person attended matric will be collected. However, no information leading to the identification of that person (like name, ID number, physical characteristics etc.) will be collected.

Necessary permissions has been obtained from the researchers who developed the instrument, for adopting the questionnaires used in the original study. All necessary precautions and guidelines as outlined in the Belmont Report (United States National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, 1979) and the relevant sections of the POPI Act will be strictly adhered to while administering, collecting, analysing and storing the data.

3.6 Data Collection

The invitation letter was sent via institutional helpdesk of both Universities and information posters were placed on several notice boards at Walter Sisulu University. The invitation letter, informed consent form and the questionnaire was delivered via the institutional helpdesk, to ensure that a specific group of students could not be targeted. In the invitation letter, it was explicitly stated that participation in the study was voluntary and that the participant can withdraw at any point in time, should he/she chooses to do so. Also students were not allowed to continue with the questionnaire if they have indicated that they were not consenting to participate or if they were not registered Facebook users. The questionnaire was also provided in a printed (hard copy) format at Walter Sisulu University. A total of 800 questionnaires and informed consent forms were placed at the main entrance to the student residences at Walter Sisulu University. It was done in three segments over a period of 40 days. Boxes were kept next to the questionnaires for the students to return the completed forms. A total of 136 online questionnaires was completed, and a total of 252 printed forms was returned. Of the 136 online participants only 54 of them could be accepted because the others were only partially completed. Of the returned printed forms 62 of them were rejected, either because they were incomplete or the student have indicated “no” to voluntary consent. This left us with a total of 244 completed questionnaires, of which a further 5 of them were rejected after close scrutiny. Only 239 responses were considered for the final analysis.

As the students did not have to provide any information which could lead to their personal identification in the questionnaire, their privacy and anonymity was protected. The collected information will not be used for any purpose other than for the objectives and the scope as defined and communicated to the participants before collecting information from them. The data will be stored for the purpose of analysis and verification and for guaranteeing the quality and integrity of the study. No information which links the participants with their respective responses was collected or stored.

After analysing the collected data, the results will be published in the form of written thesis and a journal publication. The participants will be informed about the outcome of the research via e-mail and will also be invited to view the thesis and journal publication. As data was also collected from Walter Sisulu University students, Directorate of Research at Walter Sisulu University will also be provided with the summarised results of the study along with a bound copy of the final thesis and hard copies of any research publications emanating from this study.

The survey respondents provided answers for 65 questions on the questionnaire, of which 11 questions were either demographic related or related to technology or usage pattern. The remaining 54 questions was related to the 10 different constructs included in the theoretical framework. The survey participants were asked to rate these questions on a 7 point Likert scale, with 1 standing for Strongly disagree and 7 for Strongly agree.

3.7 Analysis

The data obtained for the survey respondents was analysed in four stages. First the data was analysed to obtain the mean values, secondly the data was analysed to check for mean differences (if any) and thirdly the (if any) mean differences existed, the data was analysed to pinpoint the mean differences and finally the mean values obtained for each of the constructs included in the theoretical model was analysed to determine if any significant correlation existed amongst them. The following sub-sections provides details of the analysis and the actual statistical tests that were employed for this purpose.

3.7.1 Data Analysis for Mean Values

The data for all the 239 respondents was collated and the mean response for each question was determined. Also the number of participants who strongly disagreed and strongly agreed for each of the question was determined and was presented as a percentage of the total number of participants. After computing the mean values for each of the individual questions posted under the different constructs, the actual values obtained for each of the individual questions was compared to check for any possible mean differences.

3.7.2 Checking for mean differences

The theoretical model employed for this study has 10 different constructs and a total of 54 questions were posted under these constructs. The individual questions posted under these constructs will have to be compared to determine the dominating factor which influenced the respondent's perception regarding that particular construct under question. In other words each of the individual question was compared with the other questions to determine the (significant) mean differences. Repeated Measures One Way ANOVA and the Friedman's test (for parametric and non-parametric respectively) are the most commonly used tests for this purpose. An instrument using Likert scale usually generates non-parametric data.

A Likert scale can never generate normally distributed data, nor can it generate continuous data. However as a Likert scale is designed in such a way that the "distance" between each item category is "equivalent" ('strongly disagree", "disagree", "slightly disagree", "neutral", "slightly agree", "agree", "strongly agree"), it presents symmetry of categories and therefore, equidistant attributes will typically be more clearly observed or, at least, inferred. When a Likert scale is symmetric and equidistant it will behave more like an interval-level measurement and therefore, in practice, Likert scales are often viewed as an interval scale. In fact the normality of the data set can be ignored and parametric methods of analysis can be employed when the group sizes are equal (Carifio & Perla, 2007; Glass, Peckham, & Sanders, 1972). So for the analysis of data to determine the mean differences, Repeated Measures one way ANOVA was used for this study.

However, as Repeated Measures one way ANOVA will only report whether there is a significant difference between the mean values for the individual questions that we have analysed, a post-hoc analysis needs to be conducted to determine where exactly these differences lie. The next sub-section details the post-hoc test that was used for this study.

3.7.3 Post-hoc Analysis

Bonferroni post-hoc analysis was conducted to compute the mean differences between each of the individual questions. In other words, if there are n number of questions included in a

particular construct, then the number of comparisons will be n x (n - 1). This gives us a clear indication as to the exact reason/s which influenced the respondents perception regarding the particular construct included in the theoretical model. The next section details the test for checking how the constructs included in the theoretical model influences each other.

3.7.4 Correlation

Finally, each construct was compared with the other constructs to determine the extent of correlation between the data sets. Pearson's Rank correlation coefficient test was used to check for significance between the different constructs. Once the significant correlation is established between the constructs, the theoretical model will be validated and the results will be reported. The details of the analysis and results obtained is provided in the Chapter 4.

3.8 Conclusion

As this is a replication study the methodology and instrument used for the original study was used for this study as well. The instrument was only slightly modified to include some questions regarding demographic details and Facebook usage patterns. All necessary ethical clearances and permissions were obtained before administering the questionnaire. No personally identifiable questions were included in the questionnaire. Participation in the study was voluntary and informed consent was obtained from all the survey participants. Data was collected and was analysed to obtain the results. The details of data analysis and the results obtained is detailed in the next chapter.

Chapter 4: Analysis

4.1 Introduction

The methodology used for this study was discussed in Chapter 3. It discussed the instrument used and the changes made to the instrument, administration and data collection. It also addressed the ethical considerations and precautions that were taken to ensure the integrity of the data. This chapter starts with a brief analysis on the demographic information obtained from the survey conducted and then proceeds with the analysis of the data obtained under the various constructs included in the theoretical model.

4.2 General Demographic Information

As explained in the previous chapters, a few more questions were added to the original questionnaire to collect some general demographic information, end user computer skills, and the general pattern of Facebook use by the survey participants. This data was analysed to determine the location where the participant has attended school (village, location, or city), gender, race, age, years of tertiary experience, current institution, perceived end user computer skills, years of Facebook use and frequency of Facebook use (how often does a participant visits Facebook).

A total of 244 students participated in the survey of which 4 of the respondents were finally excluded from the analysis after a close scrutiny (Refer to Chapter 3, Section 3.6). 101 participants were from schools located in towns, 54 from schools located in locations or townships, 78 from villages or agricultural administrations (A/A) and two from schools outside the Republic of South Africa. The location of 5 respondents could not be determined either because the information was not entered or the names of the schools were misspelled. In cases where the respondent did not explicitly indicate the location of the school (as village, location or town), Google maps was used to determine the nature of the location. Also the service of a few educators working for the Department of Education, was also used to determine the nature of the location of the schools. Twelve schools located in towns offered Information Technology in their curriculum, with the majority of the schools located in towns having proper infrastructure and good facilities. However, these details could not be verified for schools in locations and villages.

The average age group of the participants was 22 years old, with the maximum representation (92.2%) from the students aged between 18 and 25 years. Of the 239 participants 127 (53.14 %) were males and the remaining 112 (46.86 %) were females. While 203 (84.94%) students were from Walter Sisulu University only 36 (15.06 %) students from Nelson Mandela University participated in the survey. The majority of the participants were blacks (94.2%), with only a few participants from the other races.

Of the 239 participants whose data was analysed 68 (28 %) of them had only one year of tertiary experience, 66 (28 %) of them had two years, 51 (21 %) of them had three years, 24 (10 %) of them had four years, 14 (6 %) of them had five years and 17 (7 %) of them had more than five years of experience. While 147 (60 %) of them use only their phone to access Facebook, a further 56 (23 %) of them are using their phone along with other devices to access Facebook. That indicates that a large percentage (83 %) of the participants preferred to use their phone to access Facebook. Very few participants use only a Tablet (10 %) or only a Computer (7 %) to gain access to Facebook as depicted in Figure 4.1.

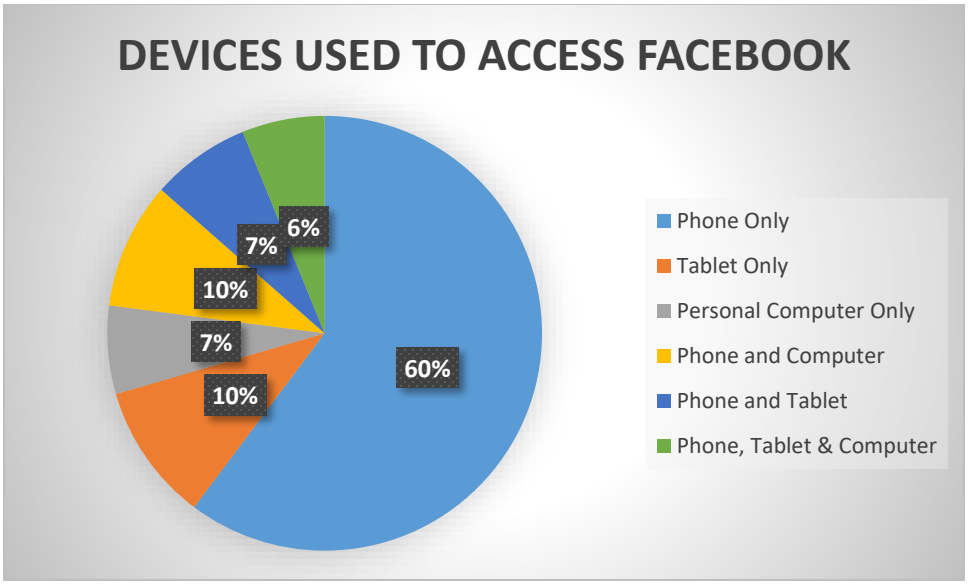


Figure 4.1: DEVICES USED TO ACCESS FACEBOOK

While sixty nine (29 %) of the participants had been using Facebook for more than five years, twenty (8 %) of them indicated that they had been using it for less than a year. One hundred and fifty five (64 %) of them had been using Facebook for between 3 and 5 years, with around 36%

of those participants (using Facebook for more than 3 years) indicating that they had been using Facebook for around 5 years.

Participants were also asked to indicate on a scale of 1 to 5 on the frequency of their Facebook use, with 1 indicating that they rarely visit Facebook and 5 indicating that they frequently visit Facebook. Seventy Four (30%) of the participants visit Facebook frequently, while thirty nine (16%) indicated that they visit Facebook only rarely. The others visit their Facebook page, somewhat on a regular basis.

This general demographic information that was collected will help us in understanding the South African SNS user's usage patterns and perceptions about self-disclosure using the privacy calculus theory. The following sections present the results for the various constructs included in the theoretical model.

4.3 Expected Benefits

As stated in the original survey the expected benefits of using an SNS was measured across three main focus areas, namely Relationship Maintenance, Entertainment and Self Presentation. The participants were asked to rate a total of seven questions under this section on a scale of 1 to 7, with 1 indicating "strongly disagree" and 7 indicating "strongly agree". Forty one percentage of the participants agreed or strongly-agreed that SNS supports Relationship Maintenance, as opposed to only 28% using it for Self Presentation. However, 47% of them use it for Entertainment. It is also interesting to note that the respondents use it mainly for supporting existing relationships rather than developing new ones. The mean values derived for the "Expected Benefits" construct is detailed in Table 4.1.

Table 4.1: EXPECTED BENEFITS (MEAN VALUES)

EXPECTED BENEFITS		Mean	Combined
Relationship Maintenance	Q1. FB is useful in supporting relationships with my friends.	4.7	4.84
	Q2. FB is convenient to stay in touch with my friends.	5.08	
	Q3. FB is useful for developing Relationships to people (business or private).	4.74	
Entertainment	Q4. I have fun on FB.	5.03	4.94
	Q5. I spend enjoyable and relaxing time on FB.	4.73	
Self-presentation	Q6. FB allows me to make a better impression on others.	4	4.05
	Q7. FB allows me to present myself in a favourable way to others.	4.09	

It has been noticed that the primary use of using SNS like Facebook is Entertainment (4.94) and Relationship Maintenance (4.84). On an average around 40% of the respondents indicated that they "agree" or "strongly agree" that they derive benefits from using Facebook, while only 6% indicated that they do not derive any benefits from using Facebook.

Around 28% of the respondents did not agree with the last two questions pertaining to Self-Presentation, *i.e.* "FB allows me to make a better impression on others" and "FB allows me to present myself in a favourable way to others" as opposed to around 11% of the respondents for the other two categories.

To check whether there is any significant difference between the mean values obtained for Relationship Maintenance, Entertainment and Self-Presentation, we hypothesise that

$H0_a$ - There is no significant difference between the mean values for Relationship Maintenance, Entertainment and Self-Presentation.
$H1_a$ – There is a significant difference between at least one of mean values for Relationship Maintenance, Entertainment and Self-Presentation.

The mean values for Relationship Maintenance, Entertainment and Self-Presentation was tested sing Repeated Measures One Way ANOVA (Refer to Chapter 3, Section 3.2). A significant

difference was observed between the mean values derived for Relationship Maintenance, Entertainment and self-presentation ($F(1.9, 453.994) = 60.966$, $p = 0.000$, $\dot{\eta}_p^2 = 0.203$). Therefore, we reject the null hypothesis $H0_a$ and state that there is a significant difference between at least one of mean values for Relationship Maintenance, Entertainment and Self-Presentation. Bonferroni post hoc tests (Refer to Chapter 3, Section 3.8.3) showed that the main benefits that the participants expected from Facebook is Entertainment (mean 4.95) and Relationship Maintenance (mean 4.88 when compared with self-presentation (mean 4.05). However, no significant difference was observed between Entertainment and Relationship Maintenance. Refer to Table 4.2 for a breakdown regarding the mean differences between Relationship Maintenance, Entertainment and Self-Presentation. (For information on the test results, Refer to Appendix B1, Table B1.1 and Table B1.2)

Table 4.2: EXPECTED BENEFITS (MEAN DIFFERENCES)

Expected Benefits	Q1	Q2	Q3
Q1. Relationship Maintenance		-0.092	0.835*
Q2. Entertainment	0.092		0.927*
Q3. Self-Presentation	-0.835*	-0.927*	

* - Mean difference significant at 0.05 level.

To check whether there is any significant difference between the mean values obtained for the individual questions under Relationship Maintenance, we hypothesise that

$H0_b$ - There is no significant difference between the mean values for individual questions posted under Relationship Maintenance.
$H1_b$ – There is a significant difference between at least one of the mean values for individual questions posted under Relationship Maintenance.

The mean values for individual questions under Relationship Maintenance was tested using Repeated Measures One Way ANOVA. A significant difference was observed between the mean values for individual questions under Relationship Maintenance ($F(1.962, 468.932) = 60.966$, $p =$

0.000, $\dot{\eta}_p^2$ = 0.203). Therefore, we reject the null hypotheses $H0_b$ and state that there is a significant difference between at least one of the mean values for individual questions under Relationship Maintenance. Bonferroni post hoc tests confirmed that Facebook is mainly used to support existing relationships and stay in touch with friends, than for developing new relationships. Refer to Table 4.3 for a breakdown regarding the mean differences between individual questions under Relationship Maintenance. (For information on the test results, Refer to Appendix B2, Table B2.1 and Table B2.2)

Table 4.3: RELATIONSHIP MAINTAINENCE (MEAN DIFFERENCES)

Relationship Maintenance	**Q1**	**Q2**	**Q3**
Q1. FB is useful in supporting relationships with my friends.		-0.379*	-0.037
Q2. FB is convenient to stay in touch with my friends.	0.379*		0.342*
Q3. FB is useful for developing Relationships to people (business or private).	0.037	-0.342*	

* - Mean difference significant at 0.05 level.

To check whether there is any significant difference between the mean values obtained for the individual questions under Entertainment, we hypothesise that

$H0_c$ - There is no significant difference between the mean values for individual questions under Entertainment.

$H1_c$ – There is a significant difference between at least one of the mean values for individual questions under Entertainment.

The mean values for individual questions under Entertainment was tested using Repeated Measures One Way ANOVA. A significant difference was observed between the mean values for individual questions under Entertainment (F(1.000, 239.000) = 21.807, p = 0.000, $\dot{\eta}_p^2$ = 0.084). Therefore, we reject the null hypotheses $H0_C$ and state that there is a significant difference between at least one of the mean values for individual questions under Entertainment.

Bonferroni post hoc test was conducted to check for mean differences. Refer to Table 4.4 for a breakdown regarding the mean differences between individual questions under Entertainment. (For information on the test results, Refer to Appendix B3, Table B3.1 and Table B3.2)

Table 4.4: ENTERTAINMENT (MEAN DIFFERENCES)

Entertainment	**Q4**	**Q5**
Q4. I have fun on FB.		0.329*
Q5. I spend enjoyable and relaxing time on FB.	-0.329*	

* - Mean difference significant at 0.05 level.

The results of the test confirmed that, respondents perceive, having fun is the primary benefit of using Facebook rather than spending a relaxing time when using Facebook.

To check whether there is any significant difference between the mean values obtained for the individual questions under Self Presentation, we hypothesise that

$H0_{c1}$ - There is no significant difference between the mean values for individual questions under Self-Presentation.

$H1_{c1}$ – There is a significant difference between at least one of the mean values for individual questions under Self-Presentation.

The mean values for individual questions under Self Presentation was tested using Repeated Measures One Way ANOVA. After conducting the test, no significant difference was observed between the individual questions under Self-Presentation ($F(1.000, 239.000) = 1.005$, $p = 0.317$, $\dot{\eta}_p^2 = 0.004$). As the p value is not significant we have to accept the null hypotheses $H0_{c1}$ and state that there is no significant difference between the mean values for individual questions under Self-Presentation. Table 4.5 lists the mean differences between the two questions under Self-Presentation sub-section of the Expected Benefits construct (as stated above the differences are not significant).

Table 4.5: SELF-PRESENTATION (MEAN DIFFERENCES)

Self-presentation	**Q6**	**Q7**
Q6. FB allows me to make a better impression on others.		-0.088
Q7. FB allows me to present myself in a favourable way to others.	0.088	

* - Mean difference significant at 0.05 level.

Entertainment is the primary benefit that users derive from using Facebook, followed by Relationship Maintenance. Facebook does not seem to be the primary SNS platform when it comes to Self-Presentation. However, users still derive significant benefits from using SNS like Facebook. The next section presents the results relating to Privacy Concerns.

4.4 Privacy concerns

This section measured the Privacy Concerns of the respondents. Four questions were posted to the respondents and they were asked to indicate how concerned they were about the posted situations on a 7-point Likert scale where 1 indicates that they are "not concerned at all" and 7 indicates that they are "very concerned". Privacy Concerns refer to the ways in which personal information privacy can be compromised, once personal information is transferred to a social media platform. Forty eight percentage of the respondents were concerned or very concerned about a personal information privacy violation. This indicates that the population in general is concerned about a possible information privacy violation. Table 4.6 presents the mean values obtained for the individual questions under the "Privacy Concerns" construct.

Table 4.6: PRIVACY CONCERNS (MEAN VALUES)

How much are you concerned that the information submitted on FB: (*Using Likert Scale*)	Mean
Q.1…can be used in a way you did not foresee	4.64
Q.2…can become available to someone without your knowledge.	5.01
Q.3…can be misinterpreted.	4.80
Q.4 …can be continuously spied on (by someone unintended).	4.84

To check whether there is any significant difference between the mean values obtained for the individual questions under the Privacy Concerns construct, we hypothesise that

$H0_d$ - There is no significant difference between the mean values obtained for the individual questions under the "Privacy Concerns" construct.

$H1_d$ – There is a significant difference between at least one of the mean values for the individual questions under the "Privacy Concerns" construct.

The mean values obtained for the individual questions under the "Privacy Concerns" construct was tested using Repeated Measures One Way ANOVA. A significant difference was observed between the mean values derived for individual questions under the "Privacy Concerns" construct ($F (2.823, 674.604) = 2.733$, $p = 0.046$, $\dot{\eta}_p^2 = 0.012$). Therefore, we reject the null hypotheses $H0_d$ and state that there is a significant difference between at least one of the mean values for individual questions under Privacy Concerns and a Bonferoni post hoc test was conducted. Refer to Table 4.7 for a breakdown regarding the mean differences between individual questions under Privacy Concerns. (For details of the test Refer to Appendix B4, Table B4.1 and Table B4.2). Bonferroni post hoc tests confirmed that users were more concerned about their information being made available to someone without their knowledge than the other scenarios presented before them.

Table 4.7: PRIVACY CONCERNS (MEAN DIFFERENCES)

Privacy Concerns	**Q1**	**Q2**	**Q3**	**Q4**
Q.1…can be used in a way you did not foresee		-0.375*	-0.167	-0.200
Q.2…can become available to someone without your knowledge.	0.375*		0.208	0.175
Q.3…can be misinterpreted.	0.167	0.208		-0.033
Q.4 …can be continuously spied on (by someone unintended).	0.200	-0.175	0.033	

* - Mean difference significant at 0.05 level.

The respondents were more concerned about the possibility of their personal information they submit on Facebook may be used in ways they did not foresee, when compared with the other scenarios presented before them. However, it is also interesting to note that 29 (12%) respondents were not concerned at all about their personal information privacy.

Respondents in general indicated having very high privacy concerns, with many indicating that their personal information will be shared without their knowledge and will be continuously spied on by others. In general, around 48% of the respondents are concerned or very concerned about the loss of personal information privacy on SNS like Facebook. It is also interesting to note that around 12 % (29) of the respondents were not concerned about their privacy. As Privacy Concerns of users is informed by Perceived Damage and Perceived Likelihood of a privacy violation, the next two sections will concentrate on those two constructs.

4.5 Perceived Damage

In this section, the respondents were asked to rate the Potential Damage they may suffer in the event of a privacy violation on Facebook. A total of seven questions were provided under this section and the respondents were asked to rate the questions on a 7-point Likert Scale, with 1 indicating “very low damage” and 7 indicating “very high damage”. The respondents rated the damage they may suffer, if any privacy violations occur, or if they were exposed to certain situations. Forty two percentage of the respondents were concerned or very concerned about the potential damages if they were exposed to any personal information privacy violations. Surprisingly, around twenty percentage of the respondents were not concerned at all or they did not perceive any damages or threats. Table 4.7 lists the mean values obtained for the individual questions posted under the “Perceived Damage” construct.

Table 4.8: PERCEIVED DAMAGE (MEAN VALUES)

Please assess the amount of the resulting damage to you (financial, to your reputation, social, psychological) if the following events took place? Information you provide on FB: (1=Very Low Damage; 4=Moderate Damage; 7=Very High Damage)	Mean
Q1. …was used for commercial purposes (e.g. market research, advertising).	3.95
Q2. …was shared with other parties (e.g. employer, governmental agencies, etc.).	4.07
Q3. …became available to unknown individuals or companies without your knowledge.	4.63
Q4. …was accessed by someone you don't want (e.g. "ex", parents, teacher, employer, unknown person, etc.).	4.49
Q5. …was used against you by someone.	4.93
Q6. .was used to embarrass you by someone.	4.62
Q7. .was continuously spied on (by someone to whom it was not intended).	4.48

To check whether there is any significant difference between the mean values obtained for the individual questions under the Perceived Damage construct, we hypothesise that

$H0_e$ - There is no significant difference between the mean values obtained for the individual questions under the "Perceived Damage" construct.

$H1_e$ – There is a significant difference between at least one of mean values for the individual questions under the "Perceived Damage" construct.

The mean values obtained for the individual questions under the "Perceived Damage" construct was tested using Repeated Measures One Way ANOVA Test. A significant difference was observed between the mean values derived for at least one of the individual questions under the "Perceived Damage" construct ($F(4.514, 1078.812) = 12.041$, $p = 0.000$, $\dot{\eta}_p^2 = 0.048$). Therefore, we reject the null hypothesis $H0_e$ and state that there is a significant difference between at least one of mean values for the individual questions under the "Perceived Damage" construct. Bonferroni post hoc tests confirmed that users perceived little or no damage if their personal information that they shared on Facebook was used for genuine commercial purposes. Refer to Table 4.9 for a breakdown regarding the mean differences between individual questions posted

under Perceived Damage Construct (Refer to Appendix B5, Table B5.1 and Table B5.2). Significant differences were observed between questions Q1 and Q3, Q1 and Q4, Q1 and Q5, Q1 and Q6, Q1 and Q7, Q2 and Q3, Q2 and Q4, Q2 and Q5, Q2 and Q6, Q2 and Q7, Q4 and Q5, Q5 and Q6, Q5 and Q7 (Refer to Table 4.8 and Table 4.9).

Table 4.9: PERCEIVED DAMAGE (MEAN DIFFERENCES)

Perceived Damage	**Q1**	**Q2**	**Q3**	**Q4**	**Q5**	**Q6**	**Q7**
Q1. …was used for commercial purposes (e.g. market research, advertising).		-0.112	-0.679*	-0.533*	-0.979*	-0.667*	-0.529*
Q2. …was shared with other parties (e.g. employer, governmental agencies, etc.).	-0.112		-0.567*	-0.421	-0.867*	-0.554*	-0.417
Q3. …became available to unknown individuals or companies without your knowledge.	0.679*	0.567*		0.146	-0.300	0.013	0.150
Q4. …was accessed by someone you don't want (e.g. "ex", parents, teacher, employer, unknown person, etc.).	0.533*	0.421	-0.146		-0.446	-0.133	0.004
Q5. …was used against you by someone.	0.979*	0.867*	0.300	0.446		0.313	0.450*
Q6. .was used to embarrass you by someone.	0.667*	0.554*	-0.013	0.133	-0.313		0.138
Q7. .was continuously spied on (by someone to whom it was not intended).	0.529*	0.417	-0.150	-0.004	-0.450*	-0.138	

* - Mean difference significant at 0.05 level.

Respondents in general did not think they would be subjected to a potential damage, if their information was used for commercial purposes or if their personal information was shared with third party companies or Government agencies. However, the respondents have indicated that they will be subjected to a potential damage if it is not done with their knowledge. This is evident from the rating that they have provided for Questions 3 and 4. They also do not want their personal information to be accessed by someone for whom that information was originally

intended for, and then that very same personal information being used against them. Being continuously spied on is also one of the potential damage that they perceive.

Around forty five percentage of the respondents believe that they can suffer potential damages in the event of a personal information privacy violation, with thirty four percentage believing that they can suffer very high damage. And around twenty percentage of the respondents think that they will suffer no damages in the event of a privacy violation.

The theoretical framework suggests that privacy concerns of SNS users is informed by the damage that they perceive in the event of an information privacy violation, and the damage that they perceive is informed by the possible likelihood of an information privacy violation. To test this relationship, we hypothesise that

Hypothesis $H0_f$: Privacy Concerns of an SNS user is informed by the Perceived Damage resulting from an information privacy violation.

Hypothesis $H1_f$ Privacy concerns of an SNS user is not informed by the Perceived Damage resulting from an information privacy violation.

Hypothesis $H0_{f1}$: Perceived Damage of an SNS user is informed by the Perceived Likelihood of an information privacy violation.

Hypothesis $H1_{f1}$ Perceived Damage of an SNS user is not informed by the Perceived Likelihood of an information privacy violation.

To test our hypothesis, we will check the correlation between the mean values derived for perceived damage and privacy concerns. After conducting the Pearson Rank correlation coefficient test (Refer to Section 3.8.4 in Chapter 3 – Research Methodology), significant correlation was observed between perceived damage and privacy concerns (0.23 correlation significant at .01 level). Hence we accept the null hypothesis $H0_f$ and $H0_{f1}$ and state that Privacy

concerns of an SNS user is not informed by the perceived damage resulting from an information privacy violation and Perceived Damage of an SNS user is informed by the perceived likelihood of an information privacy violation. (For details regarding the Pearson's Rank Correlation test, please refer to Appendix B11, Table B11.1). We accept the null hypotheses $H0_{f1}$ and state that Perceived Damage of an SNS user is informed by the perceived likelihood of an information privacy violation.

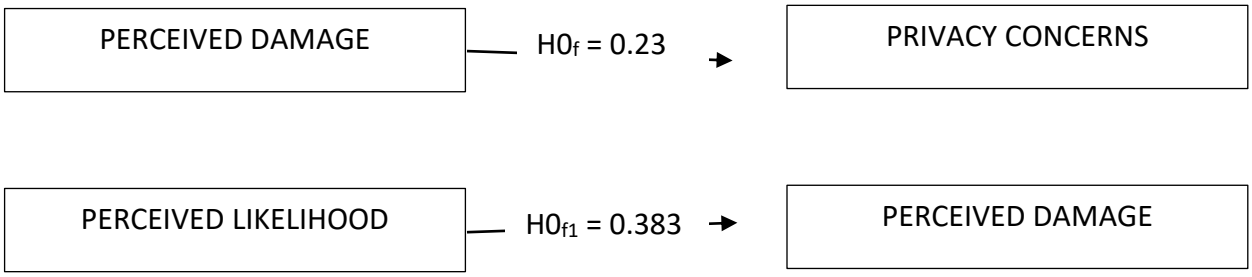


Figure 4.2: CORRELATION BETWEEN PERCEIVED DAMAGE vs PRIVACY CONCERNS, & PERCEIVED LIKELIHOOD vs PERCEIVED DAMAGE

In general, the respondents were observed to be less concerned if their information was used for genuine commercial purposes or shared with government agencies. Significantly more number of respondents were very concerned about the potential damage they may suffer if their personal information was shared without their knowledge and the potential use of this information against them. The theoretical model also argues that privacy concerns is informed by the perceived likelihood of a privacy violation we will check how the participants responded to question relating to the Perceived Likelihood of a privacy violation.

4.6 Perceived Likelihood

In this section, the respondents were asked to what extent they perceive that a privacy violation is likely to occur. The respondents were asked to rate on a scale of 1 to 7, with 1 indicating not likely at all and 7 indicating very likely, on the potential likelihood of certain events in the event of a potential privacy violation. A total of seven questions were asked under this section. In the theoretical model the privacy concerns or the cost of using an SNS is informed by the perceived

damage and the likelihood of such a violation. A negative correlation was observed between the length and frequency of Facebook use with the respondents' Perceived Likelihood of a privacy violation.). The number of respondents (24%) who think that they will never be subjected to a privacy violation is more when compared with the number of respondents (5.2%) who thinks that they are at high risk of being exposed to a privacy violation. Again the respondents from villages perceive that they are at more risk of being subjected to a privacy violation than the other groups, even though no significant difference could be noticed between the groups regarding perceived computer skills and years of using Facebook. Table 4.10 lists the mean values obtained for the individual questions posted under the "Perceived Likelihood" construct.

Table 4.10: PERCEIVED LIKELIHOOD (MEAN VALUES)

Please assess the likelihood of the following events: Information you provide on FB: (1=Not at all likely 4=Moderately likely; 7=Very likely)	Mean
Q1 … will be used for commercial purposes (e.g. market research, advertising).	3.49
Q2 … will be shared with other parties (e.g. employer, governmental agencies, etc.).	3.69
Q3 … will become available to unknown individuals or companies without your knowledge.	3.88
Q4 … will be accessed by someone you don't want (e.g. "ex", parents, teacher, employer, unknown person, etc.).	4.04
Q5 … will be used against you by someone.	3.53
Q6 ..will be used to embarrass you by someone.	3.46
Q7 ..will be continuously spied on (by someone to whom it was not intended).	3.85

* - Mean difference significant at 0.05 level.

To check whether there is any significant difference between the mean values obtained for the individual questions under the Perceived Likelihood construct, we hypothesise that

$H0_g$ - There is no significant difference between the mean values obtained for the individual questions under the Perceived Likelihood construct.

$H1_g$ – There is a significant difference between at least one of mean values for the individual questions under the Perceived Likelihood construct.

The mean values obtained for the individual questions under the "perceived likelihood" construct was tested using Repeated Measures One Way ANOVA Test. A significant difference was observed between the mean values derived for individual questions under the "perceived likelihood" construct ($F(5.085, 1215.231) = 6.007$, $p = 0.000$, $\dot{\eta}_p^2 = 0.025$). Therefore, we reject the null hypotheses $H0_g$ and state that there is a significant difference between the mean values obtained for at least one of the individual questions under the "Perceived Likelihood" construct and a Bonferoni post Hoc test was conducted. Refer Table 4.11 for a brief information regarding the mean differences between individual questions posted under Perceived Likelihood Construct. (For detailed information Refer Appendix B6, Table B6.1 and Table B6.2). Significant differences were observed between Q1 and Q4, Q3 and Q5, Q3 and Q6, Q4 and Q5, and Q4 and Q6. (For questions related to Q1 to Q7 see Table 4.10 and Table 4.11)

Table 4.11: PERCEIVED LIKELIHOOD (MEAN DIFFERENCES)

Perceived Likelihood	Q1	Q2	Q3	Q4	Q5	Q6	Q7
Q1 … will be used for commercial purposes (e.g. market research, advertising).		-0.196	-0.392	-0.550*	-0.038	0.033	-0.362
Q2 … will be shared with other parties (e.g. employer, governmental agencies, etc.).	0.196		-0.196	-0.354	0.158	0.229	-0.167
Q3 … will become available to unknown individuals or companies without your knowledge.	0.392	0.196		-0.158	0.354	0.425*	0.029
Q4 … will be accessed by someone you don't want (e.g. "ex", parents, teacher, employer, unknown person, etc.).	0.550*	0.354	0.158		0.513*	0.583*	0.188
Q5 … will be used against you by someone.	0.038	-0.158	-0.354	-0.513*		0.071	0.325
Q6 ..will be used to embarrass you by someone.	-0.033	-0.229	0.425*	-0.583*	-0.071		-0.396
Q7 ..will be continuously spied on (by someone to whom it was not intended).	0.362	0.167	0.029	-0.188	-0.325	0.396	

* - Mean difference significant at 0.05 level.

The post hoc tests confirmed that the perceived likelihood of their information being accessed by someone whom they don't want is more when compared with the other scenarios presented before them.

Respondents think that it is more likely that the information that they submit on Facebook will be accessed by someone unintended and without their permission and it is less likely that it will be used for commercial purposes.

The theoretical model suggests that the privacy concerns of SNS users is informed by both perceived damage that they can suffer in the event of an information privacy violation and the perceived likelihood of such an event. As we have already seen that there is a positive correlation between perceived damage and privacy concerns, we will check if there is any relationship

between Perceived Likelihood and Privacy Concerns. To verify this relationship, we hypothesise that:

Hypothesis $H0_h$: Privacy concerns of an SNS user is informed by the Perceived Likelihood of an information privacy violation.

Hypothesis $H1_h$: Privacy concerns of an SNS user is not informed by the Perceived Likelihood of an information privacy violation.

After conducting the Pearson's Rank Correlation coefficient test, significant positive correlation was observed between perceived likelihood of a privacy violation and privacy concerns (0.238 significant at .01 level). Hence we accept the null hypotheses $H0_h$ and state that the privacy concerns of an SNS user is informed by the perceived likelihood of an information privacy violation (Refer to Appendix B11, Table B11.2).

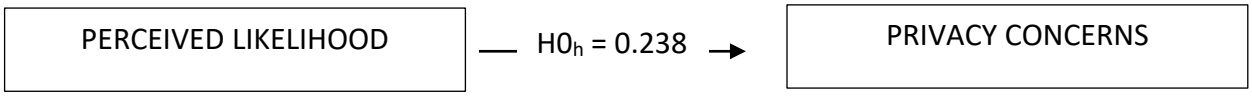


Figure 4.3: CORRELATION BETWEEN PERCEIVED LIKELIHOOD vs PRIVACY CONCERNS

The privacy concerns of the respondents were informed by the perceived damage and the perceived likelihood of such a violation, as shown in the theoretical framework. In the following sections we will discuss the trust factors which influence the disclosure behaviour of SNS users.

4.7 Trust Factors

In this section respondents were asked to rate how they trusted their service provider (Facebook), the other users on their network and the Legal System. It was determined that they trusted Facebook more than their Legal System, and the other users on the network.

4.7.1 Trust in Social Networking Services

In case of trusting the platform, or Facebook in this case, the respondents raised to our expectations. In this section the users trust in the service provider (Facebook) was measured by asking the participants to rate seven different questions on a 7 point Likert scale, with 1 indicating that they strongly disagree and a 7 indicating that they strongly agree. It has been revealed that in general the users trust the service provider. Table 4.12 lists the mean values obtained for the individual questions posted under the "Trust in Social Networking Services" construct.

Table 4.12: TRUST IN SOCIAL NETWORK SERVICES (MEAN VALUES)

In general, FB: Likert Scale (1=Strongly Disagree; 7=Strongly Agree)	Mean
Q1. ...is open and receptive to the needs of its members.	4.60
Q2. ...makes good-faith efforts to address most member concerns.	4.53
Q3. ...is honest in its dealings with me.	4.39
Q4. ...keeps its commitments to its members.	4.44
Q5. ...is trustworthy.	3.89
Q6. ...tells the truth related to the collection and use of the personal information.	4.07
Q7. ...is competent in protecting the information I provide.	4.30

A small percentage of the respondents have indicated that they do not trust Facebook, while significantly more number of the participants indicated that they trust the service provider. To check whether there is any significant difference between the mean values obtained for the individual questions under the Trust in Service Provider construct, we hypothesise that

$H0_j$ - There is no significant difference between the mean values obtained for the individual questions under the Trust in Service Provider construct.

$H1_j$ – There is a significant difference between at least one of mean values for the individual questions under the Trust in Service Provider construct.

The mean values obtained for the individual questions under the "trust in service provider" construct was tested using Repeated Measures One Way ANOVA Test. A significant difference was observed between the mean values derived for individual questions under the "trust in service provider" construct ($F(4.908, 1172.970) = 10.098$, $p = 0.000$, $\dot{\eta}_p^2 = 0.041$). Therefore, we reject the null hypotheses $H0_j$ and state that there is significant difference between at least one of the mean values obtained for the individual questions under the "Trust in Service Provider" construct and a Bonfferoni post hoc test was conducted. Refer Table 4.13 for a brief information regarding the mean differences between individual questions posted under Trust in service provider Construct. (For detailed information Refer Appendix B7, Table B7.1 and Table B7.2). Significant differences were observed between Q1 and Q5, Q2 and Q5, Q2 and Q6, Q3 and Q5, Q3 and Q6. Q4 and Q5, Q4, and Q6 and Q5 and Q7. (For questions related to Q1 to Q7 see Table 4.12 and Table 4.13)

Table 4.13: TRUST IN SERVICE PROVIDER (MEAN DIFFERENCES)

	Q1	**Q2**	**Q3**	**Q4**	**Q5**	**Q6**	**Q7**
Q1. ...is open and receptive to the needs of its members.		0.050	0.192	0.142	0.688*	0.513*	0.275
Q2. ...makes good-faith efforts to address most member concerns.	-0.050		0.142	0.092	0.638*	0.463*	0.225
Q3. ...is honest in its dealings with me.	-0.192	-0.142		-0.050	0.496*	0.321	0.083
Q4. ...keeps its commitments to its members.	-0.142	-0.092	0.050		0.546*	0.371*	0.133
Q5. ...is trustworthy.	-0.688*	-0.638*	-0.496*	-0.546*		-0.175	-0.412*
Q6. ...tells the truth related to the collection and use of the personal information.	-0.513*	-0.463*	-0.321	-0.371*	0.175		-0.237
Q7. ...is competent in protecting the information I provide.	-0.275	-0.225	-0.083	-0.133	0.412*	0.237	

* - Mean difference significant at 0.05 level.

While the respondents believe that Facebook is receptive to the needs of its members, addresses their concerns, is honest and tries to keep its commitments, they do not trust Facebook. This paradox emerges from the perception that the users believe that Facebook does not fully reveal the truth relating to the collection and further use of their personal information and that Facebook is not competent enough to protect their personal information.

Male respondents in general have indicated that Facebook makes efforts to address the users concerns, is trustworthy, keeps it commitments to the users, and tells the truth about the collection and use of their personal information than their female counterparts.

The theoretical framework suggests that trust in the service provider has a positive impact on the benefits that SNS users expect from the platform and self-disclosed more and a negative impact on the privacy concerns. To test the relationship between these constructs we hypothesise that:

Hypothesis $H0_k$: Users who trust the service provider tend to enjoy more benefits from the platform.

Hypothesis $H1_k$: Users who trust the service provider does not enjoy more benefits from the platform.

Hypothesis $H0_{k1}$: Users who trust the service provider has less privacy concerns.

Hypothesis $H1_{k1}$: Users who trust the service provider has more privacy concerns.

Hypothesis $H0_{k2}$: Users who trust the service provider tend to self-disclose more.

Hypothesis $H1_{k2}$: Users who trust the service provider negatively affects user self-disclosure.

After checking the relationship (using Pearson's Rank correlation coefficient) it was found that there was a strong correlation between trust in service provider and expected benefits (0.434 significant at 0.01 level) and self-disclosure (0.526 correlation significant at 0.01 level). Hence we accept hypothesis $H0_k$ & $H0_{k2}$ and state that those who trust the service provider tend to enjoy more benefits from the platform and self-disclosed more. No significant correlation was observed between Trust in Service Provider and Privacy Concerns (Refer to Appendix B11, Table B11.3 and Table B11.4)

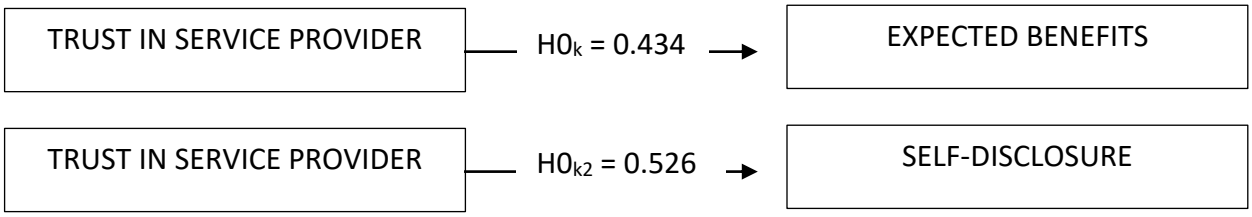


Figure 4.4: CORRELATION BETWEEN TRUST IN SERVICE PROVIDER vs EXPECTED BENEFITS & SELF-DISCLOSURE

4.7.2 Trust in SNS Members

A total of six questions were posted under this section and users were asked to rate each question on a seven point Likert scale with 1 indicating that they strongly disagree with the statement and a 7 indicating that they strongly agree. Even though the users were generally inclined towards trusting the service provider, they do not share the same sentiments for the other users on the network. Generally, the group of respondents do not trust the other members using the platform. They trust their ability to control information about them and the platform itself. Table 4.14 lists the mean values obtained for the individual questions posted under the "Trust in SNS Members" construct.

Table 4.14: TRUST IN SNS MEMBERS (MEAN VALUES)

Generally, I trust that Facebook users: (1 = Strongly Disagree, 4 = Neutral, 7 = Strongly Agree)	**Mean**
Q.1. ...will not to misuse my sincerity on FB.	3.80
Q.2. ...will not embarrass me for some information they learned about me through FB.	3.83
Q.3. ...will not use the information they found about me in FB against of me.	3.75
Q.4. ...will not use the information about me in a wrong way.	3.81
Q.5. ...are trustworthy	3.38
Q.6. ...are open and delicate to each other.	3.45

Many users do not believe that the other users on the network are open and delicate to each other (48%), while only 37% of the respondents believe that the other users can be trusted. Many users believe that the other users on the network may embarrass them, use the information against them in a wrong way, and are not trustworthy.

To check whether there is any significant difference between the mean values obtained for the individual questions under the Trust in SNS Members construct, we hypothesise that:

$H0_I$ - There is no significant difference between the mean values obtained for the individual questions under the Trust in SNS Members construct.

$H1_I$ – There is a significant difference between at least one of mean values for the individual questions under the Trust in SNS Members construct.

The mean values obtained for the individual questions under the "trust in other users" construct was tested using Repeated Measures One Way ANOVA Test. A significant difference was observed between the mean values derived for individual questions under the "Trust in SNS Members" construct ($F(3.979, 960.869) = 8.499$, $p = 0.000$, $\dot{\eta}_p^2 = 0.034$). Therefore, we reject the null hypotheses $H0_I$ and state that there is significant difference between the mean values obtained for the individual questions under the "Trust in SNS Members" construct. Bonferroni post hoc tests indicated that users in general think that the other users on the network are not trustworthy. Refer to Table 4.15 for a brief information regarding the mean differences between individual questions posted under "Trust in SNS Members" Construct (Refer to Appendix B8, Table B8.1 and Table B8.2). Significant differences were observed between Q1 and Q5, Q1 and Q6, Q2 and Q5, Q2 and Q6, Q3 and Q5, Q3 and Q6, Q4 and Q5, and Q4 and Q6 (see Table 4.14 and Table 4.15)

Table 4.15: TRUST IN SNS MEMBERS (MEAN DIFFERENCES)

Trust in	Q1	Q2	Q3	Q4	Q5	Q6
Q.1. ...will not to misuse my sincerity on FB.		-0.029	0.054	0.008	0.421*	0.354
Q.2. ...will not embarrass me for some information they learned about me through FB.	0.029		0.083	0.021	0.450*	0.383*
Q.3. ...will not use the information they found about me in FB against of me.	-0.054	-0.083		-0.063	-0.367*	0.300
Q.4. ...will not use the information about me in a wrong way.	0.008	-0.021	0.063		0.429*	0.362*
Q.5. ...are trustworthy	-0.421*	-0.450*	-0.367*	-0.429*		-0.067
Q.6. ...are open and delicate to each other.	-0.354	-0.383*	-0.300	-0.362*	0.067	

* - Mean difference significant at 0.05 level.

The overall mean score obtained for "Trust in SNS members" construct indicates a general mistrust towards the other users of the network, it is interesting to note that the mean values obtained for Q5 and Q6 is significantly low when compared with the other questions (Refer to Table 4.15). While most of the users perceive that the other members of the network will not misuse the personal information they disclose on the platform to embarrass them, misinterpret or use against them, they do not trust each other and believe that the others are not "open and delicate to each other".

The theoretical framework suggests that those who trusts the other members of the network had less privacy concerns and enjoyed more benefits and self-disclosed more. To test this relationship, we hypothesise that:

Hypothesis $H0_m$: Users who trust the other users of the Network tend to enjoy more benefits from the platform.
Hypothesis $H1_m$: Users who trust the other users of the Network does not enjoy more benefits from the platform.
Hypothesis $H0_{m1}$: Users who trust the other users of the Network has less privacy concerns.
Hypothesis $H1_{m1}$: Users who trust the other users of the Network has more privacy concerns.
Hypothesis $H0_{m2}$: Users who trust the other users of the Network tend to self-disclose more.
Hypothesis $H1_{m2}$: Users who trust the other users of the Network negatively affects user self-disclosure.

After checking for any significant correlation between the above mentioned constructs using Pearson's Rank correlation coefficient, it was observed that those who trust the other members of the network expected more benefits from the network (0.337 correlation significant at 0.01 level) and self-disclosed more (0.395 correlation significant at 0.01 level). Hence we accept the null hypothesis $H0_m$ and $H0_{m2}$ and state that users who trust the other users of the Network tend to enjoy more benefits from the platform and users who trust the other users of the Network tend to self-disclose more. A slight negative correlation (even though not significant) was

observed between trust in SNS members and privacy concerns (Refer to Appendix B11, Table B11.5 & Table B11.6).

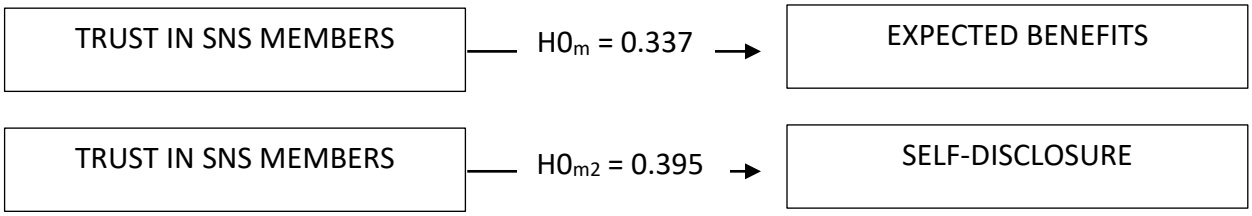


Figure 4.5: CORRELATION BETWEEN TRUST IN SNS MEMBERS vs EXPECTED BENEFITS, & SELF-DISCLOSURE

Even though the users in general do not trust the other users on the network, female respondents think that the other users are open and delicate to each other than the male respondents.

In general, the Facebook users do not trust each other. They believe that the other users on the network can use the information they disclose on the network against them and are not trustworthy. In the next section, we will analyse the data obtained for trust in legal assurance.

4.7.3 Trust in Legal Assurance

This section measured the users trust in the existing legal framework. Three questions were included in this section and the respondents were asked to rate the questions on a seven point Likert scale, with 1 indicating that they strongly disagree and 7 indicating that they strongly agree. In general, the mean obtained for the three statements under this section, indicated that the users were neutral towards trusting the legal framework. Table 4.16 lists the mean values obtained for the individual questions posted under the "Trust in Legal Assurance" construct.

Table 4.16: TRUST IN LEGAL ASSUARANCE (MEAN VALUES)

Question: Indicate to what extend you agree or disagree with the following statements (1 = Strongly Disagree, 4 = Neutral, 7 = Strongly Agree)	**Mean**
Q1. I feel confident that existing laws protect me against abuse of my information on FB.	4.12
Q2. Existing laws adequately protect my information on FB.	3.99
Q3. The existing legal framework is good enough to make me feel comfortable using FB.	4.05

To check whether there is any significant difference between the mean values obtained for the individual questions under the Trust in Legal Assurance construct, we hypothesise that

$H0_n$ - There is no significant difference between the mean values obtained for the individual questions under the Trust in Legal Assurance construct.

$H1_n$ – There is a significant difference between at least one of mean values for the individual questions under the Trust in Legal Assurance construct.

The mean values obtained for the individual questions under the "Trust in Legal Assurance" construct was tested using Repeated Measures One Way ANOVA Test. Bonferroni post hoc tests indicated that there is no significant difference was observed between the mean values derived for individual questions under the "Trust in Legal Assurance" construct ($F (1.994, 476.594) = 1.277$, $p = 0.28$, $\dot{\eta}_p^2 = 0.005$). Therefore, we accept the null hypothesis $H8_a$ and state that there is no significant differences between the mean values for the different questions posted under this construct. The mean differences for the different questions posted under the Trust in Legal Assurance construct is listed in Table 4.17. (As stated above there is no significant differences between the mean values obtained for the individual questions posted under the Trust in Legal Assurance construct)

Table 4.17: TRUST IN LEGAL ASSURANCE (MEAN DIFFERENCES)

Trust in Legal Assurance	**Q1**	**Q2**	**Q3**
Q1. I feel confident that existing laws protect me against abuse of my information on FB.		0.125	0.067
Q2. Existing laws adequately protect my information on FB.	-0.125		-0.058
Q3. The existing legal framework is good enough to make me feel comfortable using FB.	-0.067	0.058	

To check is there is any significant correlation between "Trust in Legal Assurance", "Awareness" and "Privacy Concerns" construct, we hypothesise that

Hypothesis $H0_o$: Users who have Trust in Legal Assurance tends to have more Awareness.

Hypothesis $H1_o$: Users who have Trust in Legal Assurance tends to have less Awareness.

Hypothesis $H0_{o1}$: Users who have Trust in Legal Assurance has less Privacy Concerns.

Hypothesis $H1_{o1}$: Users who have Trust in Legal Assurance has more Privacy Concerns.

After checking for any significant correlation using Pearson's Rank Correlation coefficient, it was determined that there is significant positive correlation between Trust in Legal Assurance and Awareness (0.489 correlation significant at 0.01 level). Hence we accept the null hypotheses $H0_o$ and state that users who have trust in Legal Assurance tends to have more awareness. However, no significant correlation was observed between Trust in Legal Assurance and Privacy concerns (Refer to Appendix B11, Table B11.7).

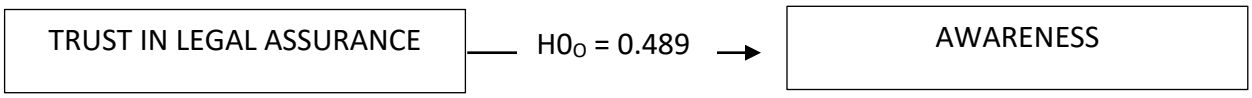


Figure 4.6: TRUST IN LEGAL ASSURANCE vs AWARENESS

Now that we have checked the relationships between the trust factors and the other constructs included in the theoretical model, in the next section we will concentrate on the constructs included in the control factors included in our theoretical model.

4.8 Control Factors

In this section, respondents were asked about the methods at their disposal to control their personal information, and if they were aware of Facebook practices and/or privacy policy.

4.8.1 Awareness

This section measured the user's perceived awareness regarding Facebook's transparency and openness with the users. In this section, the respondents were only asked whether they are aware of how and what information about them can be collected by Facebook. They generally agreed that they are aware of Facebook's information gathering policy and the further use of

that information. Table 4.18 lists the mean values obtained for the individual questions posted under the Awareness construct.

Table 4.18: AWARENESS (MEAN VALUES)

Question: Indicate to what extend you agree or disagree with the following statements: (1 = Strongly Disagree, 4 = Neutral, 7 = Strongly Agree)	**Mean**
Q1. Generally, I find FB transparent in how the personal information I provide can be used.	4.23
Q2. FB clearly communicates what information it can collect about me.	4.33

To check whether there is any significant difference between the mean values obtained for the individual questions under the Awareness construct, we hypothesise that

$H0_p$ - There is no significant difference between the mean values obtained for the individual questions under the Awareness construct.

$H1_p$ – There is a significant difference between at least one of mean values for the individual questions under the Awareness construct.

The values obtained under the "Awareness" construct was tested using Repeated Measures One Way ANOVA Test. Bonferroni post hoc tests indicated that confirmed that there is no significant difference between the values obtained under the individual questions posted under this construct ($F(1.000, 239.000) = 1.259$, $p = 0.263$, $\dot{\eta}_p^2 = 0.005$). Therefore, we accept the null hypotheses $H0_p$ and state that there is no significant difference between the values obtained for the individual questions under the "Awareness" construct. Table 4.19 lists the mean differences between the different questions under the Awareness construct As stated above the mean differences are not significant.

Table 4.19: AWARENESS (MEAN DIFFERENCES)

Awareness	**Q1**	**Q2**
Q1. Generally, I find FB transparent in how the personal information I provide can be used.		0.100
Q2. FB clearly communicates what information it can collect about me.	-0.100	

The theoretical model proposes that users who are aware of the information privacy policy of Facebook had more trust in the platform, tended to have more trust in the other users of the network and perceive to have more control over the personal information they reveal on Facebook. To test these relationships, we hypothesise that:

Hypothesis $H0_q$: Users who are aware of the information privacy policy of Facebook has more trust in the Platform.
Hypothesis $H1_q$: Users who are aware of the information privacy policy of Facebook does not trust the Platform.
Hypothesis $H0_{q1}$: Users who are aware of the information privacy policy of Facebook has more trust the other users of the Network.
Hypothesis $H1_{q1}$: Users who are aware of the information privacy policy of Facebook does not trust the other users of the Network.
Hypothesis $H0_{q2}$: Users who are aware of the information privacy policy of Facebook perceive more control over their personal information.
Hypothesis $H1_{q2}$: Users who are aware of the information privacy policy of Facebook does not perceive more control over their personal information.

After conducting the correlation between the various constructs using the Pearson's Rank correlation coefficient, it was found that users who are aware of the privacy policy of Facebook trusted the platform (0.586 correlation significant at 0.01 level), the other users of the network (0.310 correlation significant at 0.01 level) and perceive more control over their personal information (0.527 significant at .05 level). Hence we accept the null hypothesis $H0_q$, $H0_{q1}$ and $H0_{q2}$ and state that users who are aware of the information privacy policy of Facebook has more trust in the platform, has more trust in the other users of the network and perceive to have more control over the personal information they reveal on Facebook. Table 4.19 lists the mean differences between the different questions under the Awareness construct (Refer to Appendix B11, Table B11.8, B11.9, B11.10).

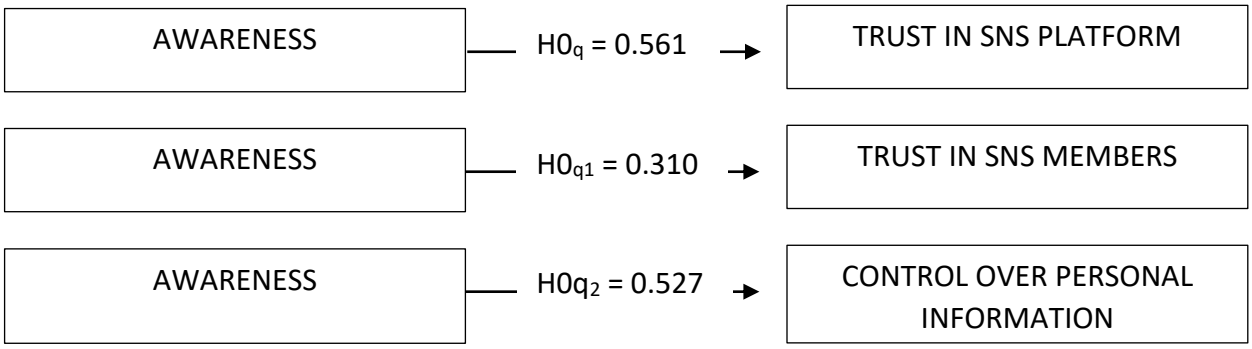


Figure 4.7: CORRELATION BETWEEN AWARENESS vs TRUST IN SNS PLATFORM, TRUST IN SNS MEMBERS, & CONTROL OVER PERSONAL INFORMATION

Awareness was also observed to be influenced by years of Facebook use, and years of tertiary experience. However, it was also observed that perceived computer skills had little or no effect on awareness. As it was determined that those who are aware of the features and policies of Facebook, perceive to have more control over their personal information, in the next section we will check how the "control over personal information" construct influences the other constructs included in our theoretical model.

4.8.2 Control over Personal Information

This section measured the users perceived control given to them from by Facebook through functionality, policies etc. The respondents were asked to rate a total of five questions on a 7-point Likert scale, with 1 indicating "no control" and 7 indicating "maximum control". Generally, the users agree that they have control over the information they reveal on Facebook. Table 4.20 lists the mean values obtained for the individual questions under the "Control over Personal Information" construct.

Table 4.20: CONTROL OVER PERSONAL INFORMATION (MEAN VALUES)

How much control is given to you by Facebook (e.g. through functionality, privacy policies) over: (1= No control at all; 4=Moderate control; 7=Considerable control)	**Mean**
Q.1. …the information you provide on Facebook (e.g. in my profile, on the Wall etc.)	4.76
Q.2. …how and in what case the information you provide can be used.	4.65
Q.3. …who can collect and use the information you provide.	4.40
Q.4. …who can view your information on Facebook?	4.52
Q.5. …the actions of other users (e.g. tagging you in pictures, writing on the Wall).	4.23

To check whether there is any significant difference between the mean values obtained for the individual questions under the Control over Personal Information construct, we hypothesise that

$H0_r$ - There is no significant difference between the mean values obtained for the individual questions under the Control over Personal Information construct.

$H1_r$ – There is a significant difference between at least one of mean values for the individual questions under the Control over Personal Information construct.

The mean values obtained for the individual questions under the "Control over Personal Information" construct was tested using Repeated Measures One-Way ANOVA. A significant difference was observed between the mean values derived for individual questions under the "Control Over Personal Information" construct ($F(3.419, 817.233) = 8.680$, $p = 0.000$, $\dot{\eta}_p^2 = 0.035$). Therefore, we reject the null hypothesis $H0_r$ and state that there is a significant difference between at least one of mean values for the individual questions under the "Control over Personal Information" construct. Bonferroni post hoc tests was conducted to test the differences between the individual questions. Table 4.21 lists the mean differences between the different questions under the Control over Personal Information construct (Refer to Appendix B9, Table B9.1 and Table B9.2). Significant differences were observed between Q1 and Q3, Q1 and Q5, Q2 and Q3, Q2 and Q5, and Q4 and Q5 (Refer to Table 4.20 and Table 4.21).

Table 4.21: CONTROL OVER PERSONAL INFORMATION (MEAN DIFFERENCES)

Control over Personal Information	Q1	Q2	Q3	Q4	Q5
Q1. …the information you provide on Facebook (e.g. in my profile, on the Wall etc.)		0.112	0.362*	0.246	0.533*
Q2. …how and in what case the information you provide can be used.	-0.112		0.250*	0.133	0.421*
Q3. …who can collect and use the information you provide.	-0.362*	-0.250*		-0.117	0.171
Q4. …who can view your information on Facebook?	-0.246	-0.133	0.117		0.287*
Q5. …the actions of other users (e.g. tagging you in pictures, writing on the Wall).	-0.533*	-0.421*	-0.171	-0.287*	

* - Mean difference significant at 0.05 level.

Users perceive little or no control over the actions of other users and who can collect the information they disclose on the platform. Only nineteen percentage of the respondents believe that they do not have control over their information disclosed on Facebook, while the majority (42%) believe otherwise.

The theoretical model postulates that those who perceive more control over their personal information has more trust in the platform and trusts the other users of the network. To check this relationship, we hypothesise that:

Hypothesis $H0_s$: Users who perceive to have more Control over their Personal Information has more Trust in the Platform.

Hypothesis $H1_s$: Users who perceive to have more Control over their Personal Information does not Trust the Platform.

Hypothesis $H0_{s1}$: Users who perceive to have more Control over their Personal Information has more trust the other Users of the Network.

Hypothesis $H1_{s1}$: Users who perceive to have more Control over their Personal Information does not trust the other Users of the Network.

Hypothesis $H0_{s2}$: Users who perceive to have more Control over their Personal Information has less Privacy Concerns.

Hypothesis $H1_{s2}$: Users who perceive to have more Control over their Personal Information has more Privacy Concerns.

After conducting the correlation between the various constructs using the Pearson's Rank correlation coefficient, it was observed that users who perceive more control over their personal information has more trust in the service provider (0.63 correlation significant at 0.01 level) and the other users of the network (0.444 correlation significant at 0.01 level). Hence we retain hypothesis $H0_s$ and $H0_{s2}$ and state that those who perceive to have more control over their personal information has more trust in the platform and the other users of the network. It was also revealed that awareness regarding the various control measures and the privacy policy of Facebook did not have any significant impact on the privacy concerns of the respondents (Refer to Appendix B11, Table B11.11, & B11.12).

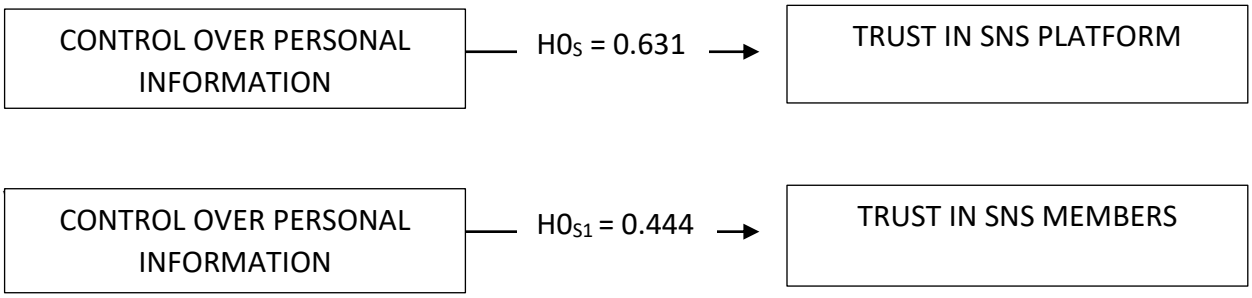


Figure 4.8: CORRELATION BETWEEN CONTROL OVER PERSONAL INFORMATION vs TRUST IN SNS PLATFORM, & TRUST IN SNS MEMBERS

4.9 Self-Disclosure

In this section, users were asked to rate how much personal information they reveal on Facebook. A total of six questions were provided and the users were asked to rate each question on a scale of 1 to 7, with 1 indicating that they "strongly disagree" and 7 indicating that they "strongly

agree". Table 4.22 lists the mean values obtained for the individual questions under the "Self-Disclosure" construct.

Table 4.22: SELF-DISCLOSURE (MEAN VALUES)

Indicate to what extend you agree or disagree with the following statements: (1 = Strongly Disagree, 4 = Neutral, 7 = Strongly Agree)	**Mean**
Q1. I have a comprehensive profile on FB.	4.31
Q2. I always find time to keep my profile up-to-date.	3.79
Q3. I have a detailed profile on FB.	4.06
Q4. My profile tells a lot about me.	3.92
Q5. From my FB profile it would be easy to find out my preferences in music, movies or books.	4.19
Q6. From my FB profile it would be easy to understand what person I am.	3.82

To check whether there is any significant difference between the mean values obtained for the individual questions under the Self-Disclosure construct, we hypothesise that:

$H0_t$ - There is no significant difference between the mean values obtained for the individual questions under the Self-Disclosure construct.

$H1_t$ – There is a significant difference between at least one of mean values for the individual questions under the Self-Disclosure construct.

The mean values obtained for the individual questions under the Self-Disclosure construct was tested using Repeated Measures one-way ANOVA. A significant difference was observed between the mean values derived for individual questions under the "Self-Disclosure" construct ($F(4.324, 1033.55) = 6.987$, $p = 0.000$, $\dot{\eta}_p^2 = 0.028$). Therefore, we reject the null hypothesis $H0_t$ and state that there is a significant difference between at least one of mean values for the individual questions under the "Self-Disclosure" construct (Refer to Appendix B10, Table B10.1 and Table B10.2). Bonferroni post hoc tests were conducted to test the differences in mean values between the individual questions. Significant differences were observed between Q1 and

Q2, Q1 and Q4, Q1 and Q6, Q2 and Q5, and Q5 and Q6. Table 4.23 list the mean differences between the various questions under "Self-Disclosure" construct (see Table 4.22 and Table 4.23).

Table 4.23: SELF-DISCLOSURE (MEAN DIFFERENCES)

Self-Disclosure	**Q1**	**Q2**	**Q3**	**Q4**	**Q5**	**Q6**
Q.1. I have a comprehensive profile on FB.		0.517*	0.250	0.388*	0.121	0.488*
Q.2. I always find time to keep my profile up-to-date.	-517*		-0.267	-0.129	-0.396*	-0.029
Q.3. I have a detailed profile on FB.	-0.250	0.267		0.138	-0.129	0.238
Q.4. My profile tells a lot about me.	-0.388	0.129	-0.138		-0.267	0.100
Q.5. From my FB profile it would be easy to find out my preferences in music, movies or books.	-0.121	0.396*	0.129	0.267		0.367*
Q.6. From my FB profile it would be easy to understand what person I am.	-0.488*	0.029	-0.238	-0.100	-0.367*	

* - Mean difference significant at 0.05 level.

The theoretical framework points towards the existence of privacy calculus, which suggests that users conduct a cost-benefit analysis before they decide to self-disclose. In the original research, the authors came to the conclusion that even with high privacy concerns SNS users self-disclosed more information. To test this theory, we will check the relationship between these constructs by hypothesising that

Hypothesis $H0_u$: Users who expect more benefits from the platform self-discloses more.
Hypothesis $H1_u$: Users who expect more benefits from the platform self-discloses less.
Hypothesis $H0_{u1}$: Users who have more privacy concerns self-discloses less.
Hypothesis $H1_{u1}$: Users who have more privacy concerns self-discloses more.

Correlation between expected benefits and Self-Disclosure was found to be significant (0.513 correlation significant at 0.01 level) after conducting a Pearson's Rank correlation coefficient test. Hence we will accept hypothesis $H0_u$, and state that users who expect more benefits from the platform self-discloses more. However, no significant correlation was observed between Privacy

concerns and Self-Disclosure, even though the test showed a slight positive correlation (refer to Appendix B11, Table B11.13).

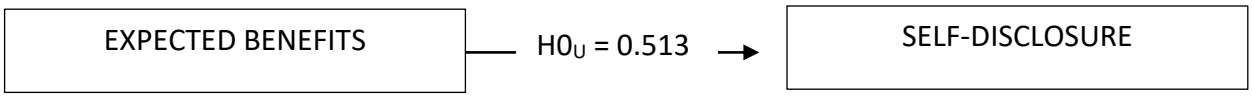


Figure 4.9: CORRELATION BETWEEN EXPECTED BENEFITS vs SELF-DISCLOSURE

Figure 4.10 provides a combined view of the theoretical framework and the connections between the various constructs included in the model.

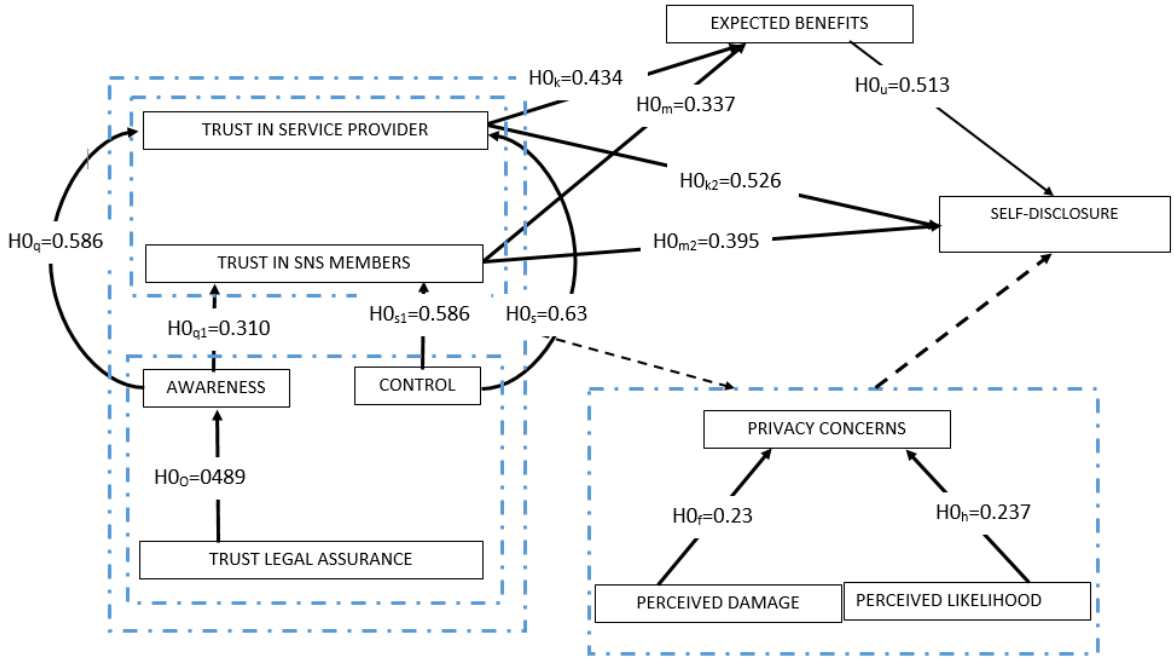


Figure 4.10: THEORETICAL FRAMEWORK BASED ON THIS STUDY

Dotted arrow indicates that connection is not significant.

4.10 Conclusion

This study is a replication of another study conducted in Germany and the US to understand the perceptions of German and US students when using Facebook. The results of this study will further our understandings on the South African SNS users self-disclosure behaviour in terms of the privacy calculus. Facebook has already reached maturity in the Western world and is looking to expand its footprint in Africa and Asia. Understanding the user's requirements is essential to maintain their market dominance. Our study was conducted among students mainly from the

province of the Eastern Cape, South Africa. The average age group of the participants was 22 years, with the maximum representation from the students aged 18 to 25 years. Many of the students have been using Facebook for more than 3 years, with 83% of them responding that they use their phone to access Facebook. They use Facebook for various activates including uploading contents, communicating with their friends, accessing news feeds (job adverts) etc. However, 5.2% of the respondents have indicated that they are just passive followers of their friend's activities.

Entertainment has been identified as the primary objective of using Facebook. It is interesting to note that only one fourth of them try to make new friends on the network, while most of them are interested in staying connected with existing friends. The respondents did not see self-presentation or enhancing one's image as a benefit they can derive from Facebook.

Many of them have indicated that they are very concerned about a possible information privacy violation. Even though they understand the implications of a privacy violation, they think that it is less likely to happen. We have observed that the privacy concerns of the participants slightly increases with the length and frequency of using Facebook. Most respondents did not have a problem with using their personal information for legitimate commercial purposes or it being shared with Government agencies.

Even though they trusted Facebook in not misusing their personal information, they do not share the same sentiments when it comes to the other users sharing the platform. They have also indicated that they trust Facebook more than the legal framework. Those who tended to trust the SNS platform and the other members tend to enjoy the benefits of using the platform more. They participants generally agree that they are aware of how and what information about them can be collected by Facebook.

Those who perceived more control over their personal information and had trust in the Facebook platform, the other users of the platform, and had trust in the legal assurance, tend to enjoy more benefits and self-disclosed more personal information. The perceived benefits the respondents enjoyed from the platform, was strongly correlated with self-disclosure as well. In the next chapter we will discuss these findings and report the results.

Chapter 5: Discussion of Results

5.1 Introduction

In the last chapter we have analysed the data obtained for finding the relationships between various constructs included in the theoretical model for this study. We have also tested whether there is any significant difference between the mean values obtained under various situations within the main construct themselves. In this chapter we will have a detailed discussion on the analysed data and finally report the results obtained.

The majority of the participants were from Walter Sisulu University (85%), with the ratio of male students to female students were evenly distributed (roughly 47% females and 53% males). An analysis of the participant's activities on Facebook revealed that many of them use it for entertainment and relationship maintenance. Of the 239 students who responded, 141 (58%) of them upload contents, 176 (72%) of them like, tag or comment on their friends contents, 151 (62%) of them are interested in news feeds, mainly job adverts, 154 (63%) of them use it for communicating with friends, 68 (28%) of them try to make new friends and contacts on the network, 62 (25%) of them share links and other interesting things on the network, while 13 (5%) of them are not interested in any of the above activities and they are just passive followers of their friends activities. It is interesting to note that only around one fourth of them (28%) try to make new friends on the network, while most of them are interested in staying connected with existing friends and obtaining news feeds.

In this chapter deals with the discussion of the results obtained by analysing the data. The expected benefits construct will be discussed first, followed by taking a closer look at the privacy concerns construct. The moderating factors and contributing factors which influences these two constructs will also be discussed in detail. We will conclude by presenting the results obtained from this study.

5.2 Expected Benefits

The theoretical model which forms the basis of this study postulates that users conduct a cost-benefit analysis before deciding to reveal their personal information on Social Networking

Services (SNS) like Facebook. It further states that the cost-benefit analysis is further influenced by other moderating factors. Benefits that the users expect from Facebook include Relationship Maintenance, Entertainment and Self Presentation. After analysing the data obtained under this construct, it was revealed that the main benefits that users expect from Facebook is Entertainment followed by Relationship Maintenance (Refer to Chapter 4, Section 4.3, Table 4.1, Table 4.2 and Table 4.3). It was further revealed that users wish to maintain existing relationships than to try and develop new relationships. It could be possible that the SNS users are using other SNS platforms or other means for developing new Relationships and Self Presentation (Drolet, 2013). A recent research conducted in the US, revealed that though older people are signing up increasingly on Facebook, the younger generation is more inclined towards platforms like Snapchat (Utz, Muscanell, & Khalid, 2015). A study from the Pew Research Center has also revealed that teenagers have abandoned Facebook in favour of other social media platforms such as Snapchat and Instagram (Anderson & Jiang, 2018). As most of the participants are between the ages of 18 and 22, it could be possible that the low level of perceived benefits the targeted population derived from using Facebook, especially on the self-presentation area, could indicate that the targeted population is slowly migrating to other social platforms, which is more "small-screen" friendly (As 86% of the population use their cell-phones as their primary device to access Facebook) and which does not store their personal information.

Taking a closer look at the mean values obtained for the individual questions (Refer to Section 4.3, Table 4.3, in Chapter 4) under Relationship Maintenance respondents perceive that Facebook is useful in staying in touch with their friends, than supporting relationships and developing new relationships. Under the Entertainment category (Refer to Section 4.3, Table 4.4, in Chapter 4) the respondents perceive that having fun is the primary benefit of using Facebook than spending a relaxing time when using Facebook.

Entertainment is the primary benefit that users derive from using Facebook, followed by Relationship Maintenance across all categories. Facebook does not seem to be the primary SNS platform when it comes to self-presentation. However, users still perceive that they derive

significant benefits from using SNS like Facebook. The theoretical framework postulates that the users conduct a cost-benefit analysis before taking the decision to disclose information on social media like Facebook. The cost of revealing personal information on Facebook is the loss of personal information privacy. The next section deals with the costs of revealing personal information on social media.

5.3 Privacy Concerns

Privacy Concerns of the users is considered as the cost of revealing personal information on Facebook. It is highly likely that the user's personal information can be used against them under various circumstances that have been described in detail in the Background chapter (Chapter 2). As the mean score for the individual questions posted under this construct vary between 4.65 and 5.03, it can be concluded that the participants in general believe that the private information they reveal on Facebook can be misused. The participants were more concerned about their data being accessed by someone without their knowledge, than the other scenarios presented before them (can be misinterpreted, spied on or to be used in a way they did not foresee) (Refer to Table 4.5 in Chapter 4).

All respondents in general have very high privacy concerns, with many indicating that their personal information will be shared without their knowledge and will be continuously spied on by others. Our data revealed that (116 participants) 48% of the respondents are concerned or very concerned about the loss of personal information privacy on SNS like Facebook. It is also interesting to note that around (28 participants) 12% of the respondents were not concerned about their privacy (Refer to Chapter 4, Section 4.4, Table 4.5).

5.4 Perceived Damage

This construct was used to measure the measure the participant's perceived damage, in the event of a personal information privacy breach, and a total of 7 scenarios were presented before them. It was surprising to note that even though the participants in general had very high privacy concerns they perceive relatively low damage from it (Refer to Chapter 4, Section 4.4.2, Table 4.9). The mean values derived for perceived damage and privacy concerns differed significantly.

It could be possible that the respondents believe that it is not likely to happen to them (Krasnova, Kolesnikova, & Guenther, 2009). The respondents were willing to transfer their information to a third party like companies and government organizations, if their information was used for genuine purposes and if it is done with their knowledge. However, they perceive that they may suffer damages if the information is used against them, if they are continuously spied on, is used against them or embarrass them or if it ends up in the wrong hands (like parents, teachers, ex-employers etc.). As most of the respondents have reported that one of the main uses of Facebook was News feeds, it could be possible that if the information is used for genuine purposes, they may have access to more information and opportunities (Hoadley, Xu, Lee, & Rosson, 2010).

Respondents in general did not think they would be subjected to a potential damage, if their information was used for commercial purposes or if their personal information was shared with third party companies or Government agencies. However, the respondents have indicated that they will be subjected to a potential damage if it is not done with their knowledge. This is evident from the rating that they have provided for Questions 3 and 4 (Refer to Chapter 4, Section 4.4.1, Table 4.8 and Table 4.9). They also do not want their personal information to be accessed by someone for whom that information was originally intended for, and then that very same personal information being used against them. Being continuously spied on is also one of the potential damage that they perceive.

The significant positive correlation that was observed between Perceived Damage and Privacy Concerns (Refer to Chapter 4, Section 4.4.1, Figure 4.2) and Perceived Damage and Perceived likelihood (Refer to Chapter 4, Section 4.4.2, Figure 4.3), support the theoretical framework used for this study, which postulates that Privacy Concerns is informed by Perceived Damage and Perceived Damage in turn is informed by the Perceived Likelihood of an information privacy violation. The next section concentrates on the perceived likelihood construct, *ie* the respondent's perception of an information privacy violation.

5.5 Perceived Likelihood

This construct was used to measure the measure the participant's Perceived Likelihood of an information privacy violation, and a total of 7 scenarios were presented before them. It was surprising to note that even though the participants in general had very high privacy concerns they perceive that it is not likely to happen (Refer to Chapter 4, Section 4.5, Table 4.10). The mean values derived for Perceived Likelihood and Privacy Concerns differed significantly. It was also surprising to note that the mean values for Perceived Damage and Perceived Likelihood also differed significantly. It is also interesting to note that the Privacy Concerns of a user is more informed by the Perceived Damage that they can suffer than by the Perceived Likelihood of such a violation. In other words, even though they perceive more damage from an information privacy violation, they perceive that it is not likely to happen. After analysing the data, it was revealed that they believe that it is more likely that the information they reveal on Facebook will be accessed by someone whom they don't want or the information will be used against them. It was also interesting to note that the respondents perceive that the information they reveal will neither be used for commercial purposes nor will be used to embarrass them.

The significant positive correlation that was observed between Perceived Likelihood and Privacy Concerns, support the theoretical framework used for this study, which postulates that Privacy Concerns of an SNS user is informed by the Perceived Damage and the Perceived Likelihood of an information privacy violation.

The benefits and costs that a user considers before deciding to reveal personal information on social media is influenced by moderating factors like Trust, Awareness and Control. These moderating factors has been incorporated into the theoretical model and the user's perception regarding these constructs were measured and analysed to find how these moderating factors influenced the cost-benefit analysis. In the following sections the impact of these moderating factors on the cost-benefit analysis will be discussed, starting with the trust factors, *ie* whether the respondents Trust the Platform (Facebook), the Other Users of the Network and their Trust in Legal Assurance.

5.6 Trust in the SNS Provider

This construct was used to measure the measure the participant's Trust in the Service Provider, and a total of 7 scenarios were presented before them. The participants in general think that Facebook is not trustworthy and does not tell the truth when it comes to the collection and further use of their personal information (Refer to Chapter 4, Section 4.7.1, Table 4.12). However, they believe that Facebook makes good faith efforts to address most of the members concerns, is open and receptive to their needs, is honest and tries to keep their commitments. This contradiction could be possibly due to two particular situations (a) Many users believe that the policy of Facebook regarding collection, storing, analysis and sharing is too complicated for them to understand (Govani & Pashley, 2005; Hoadley et al., 2010), and (b) And the interface provided by Facebook which creates an atmosphere, where the users are led to disclose more (Fogg & Iizawa, 2008).

The theoretical framework suggests that Trust in the Service Provider has a positive impact on the benefits that SNS users expect from the platform and Self Disclosed more and a negative impact on the Privacy Concerns. A strong positive correlation was observed between Trust in the SNS Provider and Expected Benefits), and Self-Disclosure (Refer to Chapter 4, Section 4.7.1, Figure 4.4). The above observation confirms the arguments stated in the theoretical framework used for this study. However, no significant correlation was noticed between Trust in the Service Provider and Privacy Concerns.

While the respondents believe that Facebook is receptive to the needs of its members, addresses their concerns, is honest and tries to keep its commitments, they do not trust Facebook. This paradox emerges from the perception that the users believe that Facebook does not fully reveal the truth relating to the collection and further use of their personal information and that Facebook is not competent enough to protect their personal information. In the next section, we will concentrate on Trust in the Other Users of the Network construct included in the theoretical framework.

5.7 Trust in SNS Users

This construct was used to measure the measure the participant's trust in the other users of the network and a total of 6 scenarios were presented before them. Even though they are relatively happy about Facebook's attitude towards its users (Refer to Chapter 4, Section 4.7.2, Table 4.14), they do not share the same sentiments when it comes to the other users of the network (Refer to Chapter 4, Section 4.7.2, Table 4.15). In general, they think that the other users of the network is not trustworthy. This may be due to some bad experiences they had, or due to the increased awareness about disclosing information on SNS like Facebook (Christofides, Muise, & Desmarais, 2012; Wang et al., 2011). The overall mean score obtained for Trust in SNS members construct indicates a general mistrust towards the other users of the network, it is interesting to note that the mean values obtained for Q5 and Q6 is significantly low when compared with the other questions (Refer to Chapter 4, Section 4.7.2, Table 4.15). While most of the users perceive that the other members of the network will not misuse the personal information they disclose on the platform to embarrass them, misinterpret or use against them, they do not trust each other and believe that the others are not "open and delicate to each other".

The theoretical model suggests that Trust in SNS Members will have a positive impact on Expected Benefits and Self-Disclosure and a negative impact on Privacy Concerns. A significant positive correlation was observed between Trust in SNS Members and Expected-Benefits construct (Refer to Chapter 4, Section 4.7.2, Figure 4.5), and between Trust in SNS Members and Self-Disclosure construct. This proves the argument in the theoretical model adopted for this study and establishes the link between the above mentioned constructs.

In general, the Facebook users do not trust each other. They believe that the other users on the network can use the information they disclose on the network against them and are not trustworthy. In the next section we will discuss about the next trust construct included in the theoretical framework.

5.8 Trust in Legal Assurance

This construct measured the users Trust in the existing Legal Framework regarding protection of personal information that they disclose on SNS like Facebook. Three questions were posted under this section and in general the mean obtained for the three statements under this section, indicated that the users were neutral towards trusting the legal framework. The mean values obtained for the three questions were also tested for any significant mean differences. However, as no significant differences were observed, it is possible that South African SNS users are generally unaware of the rules governing protection of personal information. Those who had trust in legal assurance also tended to have more awareness about the legal framework and the privacy policy of Facebook (Refer to Chapter 4, Section 4.7.3, Figure 4.6). In the next two sections we will discuss about the Awareness and Control over Personal Information constructs.

5.9 Awareness

In this section, the respondents were only asked whether they are aware of how and what information about them can be collected by Facebook. They generally agreed that they are aware of Facebook's information gathering policy and the further use of that information. The mean values obtained for those two questions were tested to check for any significant differences. It was observed that there is no significant difference between the mean values obtained for the two questions included under the awareness construct. The theoretical framework postulates that the Awareness construct positively influences the Perceived Control over Personal Information construct and together they have a positive impact on the Trust in SNS Platform and Trust in SNS members construct. In other words, those who are aware of the features and policies of Facebook and the legal framework will have more Trust in the Platform and the Other Users of the Network. After checking for correlation between these constructs it was observed that there is a significant positive correlation between Awareness and Control over Personal Information (Refer to Chapter 4, Section 4.6.1, Figure 4.7), Awareness and Trust in SNS, and Awareness and Trust in SNS Members constructs. In the next section we will discuss about the Control over Personal Information construct.

5.10 Control over Personal Information

A total of five questions were included in this section and, generally the users agreed that they have control over the information they reveal on Facebook. However, the users were not that confident when it comes to the actions of other users and who and what information others can collect, and use the information that a person reveals on Facebook. The overall mean value suggests that the respondents agree that they have control over their personal information. Having a closer look at the individual questions, they seem to be fairly confidant when it comes to the control that Facebook provides, but it fades a little when it comes to the actions of other users. It was also revealed that Awareness regarding the various Control Measures and the privacy policy of Facebook did not have any significant impact on the Privacy Concerns of the respondents.

The theoretical model postulates that those who perceive more Control over their Personal Information has more Trust in the Platform, Trusts the other Users of the Network and has less Privacy Concerns. Even though no significant correlation was observed between Control over Personal Information and Privacy Concerns, it was revealed that those who perceive more Control over their Personal Information had more Trust in the Platform and Trust in the other Users of the Network (Refer to Chapter 4, Section 4.8.2, Figure 4.8).

Privacy Concerns of the respondents, as indicated in the theoretical model, is informed by the Perceived Likelihood of a privacy violation and the Perceived Damage resulting from such a privacy violation. However, those who perceived to have more awareness feared a slight likelihood and damage from a potential information privacy violation (correlation not significant). Those who perceived to have more control over their information tend to enjoy the benefits of using the platform more and also tend to Self-Disclose more personal information.

5.11 Self-Disclosure

A total of six questions were provided and the users were asked to rate each question on a scale of 1 to 7, with 1 indicating that they “strongly disagree” and 7 indicating that they “strongly agree”. In general, the users perceive that they do not reveal much personal information on

Facebook. Those who perceived more Control over their Personal Information and had Trust in the Facebook platform, the Other Users of the platform, and had Trust in the Legal Assurance, tend to enjoy more benefits and Self Disclosed more personal information. Even though generally the population was concerned with privacy, they tended to self-disclose more personal information.

The post hoc tests confirms that even though the users have a comprehensive profile on Facebook, they do not update it regularly and they perceive that it will be difficult to find out their preferences in music, movies or books, from the information they self-disclose on the platform. Nineteen respondents believe that they do not have a comprehensive profile on Facebook, while forty one respondents believe that it will be very difficult to understand their personality from their profile. Thirty five respondents indicated that they do not update their profiles and an average of 30 respondents have indicated that they do not communicate their likes or preferences on Facebook. Only around Thirty Three of the respondents believe that they regularly update their information and reveal all their personal information on Facebook.

5.12 Conclusion

This study is a replication of another study conducted in Germany and the US to understand the perceptions of German and US students when using Facebook. The results of this study will further our understandings on the South African SNS users self-disclosure behaviour in terms of the privacy calculus. Facebook has already reached maturity in the Western world and is looking to expand its footprint in Africa and Asia. Understanding the user's requirements is essential to maintain their market dominance.

Entertainment has been identified as the primary objective of using Facebook. It is interesting to note that only one fourth of them try to make new friends on the network, while most of them are interested in staying connected with existing friends. The respondents did not see self-presentation or enhancing ones image as a benefit they can derive from Facebook. It is also interesting to note that as the number of years of using Facebook increases, they derive less benefits.

Many of them have indicated that they are very concerned about a possible information privacy violation. Even though they understand the implications of a privacy violation, they think that it is less likely to happen. Most respondents did not have a problem with using their personal information for legitimate commercial purposes or it being shared with Government agencies.

Even though they trusted Facebook in not misusing their personal information, they do not share the same sentiments when it comes to the other users sharing the platform. They have also indicated that they trust Facebook more than the legal framework. Those who tended to trust the SNS platform and the other members tend to enjoy the benefits of using the platform more. They participants generally agree that they are aware of how and what information about them can be collected by Facebook.

Those who perceived more control over their personal information and had trust in the Facebook platform, the other users of the platform, and had trust in the legal assurance, tend to enjoy more benefits and self-disclosed more personal information. The perceived benefits the respondents enjoyed from the platform, was strongly correlated with self-disclosure as well.

The findings of this study is similar to what the theoretical model postulates which forms the basis of this study. Even with high “Privacy Concerns” users “Self-Discloses” information. “Awareness” about the features of the platform and “Trust in Legal Assurance” gives users a perception of more “Control over their Personal Information”. “Trust in the SNS platform” and “Trust in other Users” of the network allow users to derive more benefits from the SNS platform. This makes the users to “Self-Disclose” more personal information. However, it was also observed that none of these constructs influences the “Privacy Concerns” of the users.

More benefits of using the platform makes the users self-disclose more. Self-Disclosure of personal information is a decision which the user takes after conducting a cost-benefit analysis, where the cost is the Privacy Concerns and the benefits are enjoyment, relationship maintenance and self-presentation. However, it was also revealed that the younger generation is moving away from Facebook as a platform for self-presentation. This cost benefit analysis is also influenced by

several moderating factors like Trust in the Platform, other Users and the Legal Framework, Awareness, and Control over Personal Information, which influences their decision. Another study conducted in US also revealed that attitude and hyperbolic discounting also plays a major part. In this study, it was revealed that even with high Privacy Concerns, which in turn is informed by Perceived Damage and Perceived Likelihood of an information privacy violation, the users of social media disclose their personal information on social media like Facebook. Privacy Concerns was neither negatively nor (significantly) positively correlated with Self-Disclosure. This confirms that a privacy paradox exists within the South African SNS user community. In the next chapter we will conclude by revisiting the objectives of this study and by checking whether the objectives have been met.

Chapter 6: Conclusion

6.1 Introduction

The findings of the study was presented in the Chapter 5. The findings indicate the existence of a privacy paradox amongst South African SNS users, meaning that, even with high privacy concerns, users are self-disclosing their personal information. The cost-benefit analysis and the influence of various control and moderating factors was also presented in detail in Chapter 5. This chapter concludes the by firstly providing a chapter review. This is followed by restating the research problem and research objectives by arguing how the objectives of the study have been met. Finally, this chapter concludes by stating the limitations of this study and directions for future research.

6.2 Chapter Review

Chapter 1 presented the road map for this study. A brief insight into the concept of information privacy and its significance was presented. An explanation of the concept of privacy concerns, benefits and self-disclosure in the context of SNS followed. The Privacy Calculus Theory was presented next, which states that SNS users conduct a cost-benefit analysis before deciding to self-disclose their personal information on SNSs. This was followed by stating the privacy paradox phenomenon which argues that even though SNS users have high privacy concerns, they still self-disclose their personal information on SNSs like Facebook. The problem statement and research problem were defined and research objectives were posed. A brief insight into the research approach and theoretical framework was also presented.

Chapter 2 dealt with related literature pertaining to this study. The concept of privacy, information privacy, privacy policy and legal frameworks in the context of SNS was explained in detail. A brief insight into the evolution of SNS in general and Facebook in particular was presented next. The privacy concerns and threats the SNS users are likely to face in the event of an information privacy violation on SNS was explained in detail. This was followed by stating the

concept of the privacy paradox phenomenon. The theoretical framework for this study, which is based on the Privacy Calculus Theory was presented next. All the constructs included in the theoretical framework were explained in detail, and sufficient motivation was provided as to why each of those constructs were included in the theoretical framework. As this study is a replication of another study conducted in Germany and USA, details of the original study was also presented.

Chapter 3 provides the detailed explanation of the methodology used for this study. This chapter starts by providing a motivation for replicating the original study. This is followed by explaining the instrument design, the changes that were made to the original instrument and the adapted isiXhosa version of the instrument. The reasons behind selecting convenience sampling was presented next. Finally, the data collection process, and the methods of analysing the data obtained was also explained in detail.

Chapter 4 deals with the analysis of the data obtained. The data was analysed in three phases. First the data was analysed to obtain the general demographic information of the respondents. Secondly, the mean values for each of the questions under the various constructs included in the theoretical framework was obtained using Repeated Measures one-way ANOVA. After obtaining the mean values, a post-hoc test was conducted to check if the mean differences between the individual questions posted under the various constructs included in the theoretical framework were significant or not. This helped us to find the situations or factors that influenced SNS users perceptions regarding a particular construct. Finally, the data was analysed to check for significant correlation (if any) between the constructs included in the theoretical framework.

In **Chapter 5**, the results of this study were presented. It discussed how the perceptions of SNS users regarding each of the constructs included in the theoretical framework was formed. It further presented how the cost-benefit analysis was conducted, and how the moderating and control factors affected the cost-benefit analysis, before the SNS user decides to self-disclose their personal information. It was determined that even with high privacy concerns, SNS users in SA still self-disclose their personal information.

6.3 Revisiting the Research Problem and Objectives

This section revisits the research problem and discusses how the objectives of the research were achieved by aligning each of the sub-objectives with the approach that was used.

This study was aimed at understanding South African SNS users Self-Disclosure behaviour. The initial problem was stated as "Currently we do not understand South African SNS users' self-disclosure behaviour in terms of the Privacy Calculus Theory". To address this problem, the primary research objective was stated as:

> *To understand the perceptions of South African SNS users regarding the perceived benefits, costs, moderating factors and self-disclosure, using the Privacy Calculus Theory.*

To achieve the primary objective of this study, the primary objective was divided into three sub-objectives:

Sub-Objective 1

> *To understand information privacy, privacy calculus, moderating factors and self-disclosure as they relate to SNS users*

To achieve this objective literature relating to privacy in general and information privacy in the context of SNS in particular was revisited and studied in detail. Though one universal definition for privacy could not be identified, for the scope of this study, **general privacy** was defined as the ability to control or selectively reveal one's own self, material possessions, and the information that defines a person, while **information privacy** was defined as a person's expectation of privacy in the collection and sharing of his or her personal information. This study is based on the **Privacy Calculus Theory** which in turn is based on Theory of Reasoned Action (TRA), Theory of Planned Behaviour (TPB), and Information Boundary Theory (IBT). According to the TRA and TPB, the adoption of some behaviours must be directly related to some benefit and IBT states that each individual forms an informational space (or territory) around him or her with clearly defined

boundaries. Such boundaries determine what information can be shared. Based on these theories, it was determined that a person conducts a cost-benefit analysis before he or she decides to self-disclose personal information. Keeping that in mind a theoretical framework was adopted which included constructs like the costs and benefits of using an SNS, the moderating factors which influence the cost-benefit analysis, and the actual self-disclosure. Related literature was revisited and each of these constructs was studied in detail. Enjoyment, Self-Presentation and Relationship Maintenance were identified as the benefits of using an SNS, while Privacy Concerns of the users, which in turn is informed by the Perceived Likelihood and Perceived Damage resulting from such a violation, were identified as the costs of using an SNS like Facebook. Control over Personal Information, Trust in the Platform and the other Users of the Platform were included as the moderating factors. Awareness regarding the various control features offered by the platform, privacy policy of the platform and the legal framework were also included and studied in detail.

Sub-Objective 2

> *To determine the value placed on the determinants of SNS user self-disclosure by South African Facebook users.*

As this is a replication of another study conducted in Germany and USA, the original instrument was adopted for this study, without any changes. isiXhosa translation of the questions and instructions were also provided next to the English version of the questions (Refer to Chapter 3, Section 3.3). A total of 56 questions were included under the various constructs included in the theoretical framework. The participants were asked to rate each of the questions on a scale of 1 to 7 and the data obtained was collated. The data was analysed in three phases using three different statistical tests, namely Mean, Repeated Measures One-Way-ANOVA, and Bonferonni post hoc analysis to determine the actual value placed by the participants on each of the constructs in general and each of the individual questions in particular (Refer to Chapter 3,

Section 3.7). The findings provided insights into the value placed on the determinants of SNS user Self-Disclosure by South African Facebook users (Refer to Chapter 4 and Chapter 5).

Sub-Objective 3

> *To establish whether the privacy paradox manifest in the use of SNS by South African Facebook users*

Repeated Measures One-Way-ANOVA and Bonferonni post hoc analysis revealed that many of the participants derived benefits from using a SNS platform like Facebook and that the moderating effects like Trust in the Platform and Users, Control Factors and Awareness regarding the privacy policy of the platform and the legal framework, positively influenced the SNS users to enjoy more benefits. Pearsons Rank Correlation Coefficient was conducted to determine how these constructs influenced each other, and to validate the theoretical framework. It was determined that even with high privacy concerns, South African SNS users self-disclose their personal information. The high privacy concerns of South African SNS users does not influence the South African SNS users decision to self-disclose. In other words, it was determined that privacy paradox manifests in the use of SNS by South African Facebook users.

6.4 Research Contributions

This is a replication of another study conducted in Germany and USA amongst university students titled “Privacy Calculus on Social Networking Sites: Explorative Evidence from Germany and USA”, undertaken by Krasnova and Veltri (2010). As user self-disclosure drives the sustainability of SNSs, it is important for the providers to understand the factors that affect self-disclosure. The original study was aimed at determining the factors that influence user self-disclosure and whether the national culture influences these factors. To achieve that a survey was conducted to explore the differences in perceptions of disclosure-relevant determinants between German and US Facebook users. The researchers came to the conclusion that privacy paradox exists among

German and US SNS users. It was also determined that National cultures of these countries greatly influenced the perceptions of the SNS users regarding the values they placed on the constructs included in the theoretical framework and how the cost-benefit analysis was conducted.

As discussed in the previous chapters, the main contributions of this study has to be viewed from two different angles, *ie* from the SNS user's side and from the SNS platform provider's side. SNS users are increasingly concerned about their personal information privacy. While they are not greatly concerned about their personal information being used for legitimate legal purposes and for services which ultimately turns out to their advantage, they do not want to sacrifice their privacy for things which may harm them at a later stage. Keeping this view in mind National Governments around the world are enacting strong information privacy laws to protect their citizen's information privacy. From the platform provider's side, to remain competitive in the market and to sustain the viability of their business model, SNSs like Facebook will have to encourage user self-disclosure. They also have to ensure that the platform remains attractive to the users while ensuring their personal information privacy. This study gives valuable insight into the perceptions of South African SNS users regarding their privacy concerns and how they conduct a cost-benefit analysis, before they decide to self-disclose their personal information. It also reveals how the moderating factors influence this cost-benefit analysis and the actual value placed by South African SNS users on these costs, benefits and moderating factors. The benefits, threats and privacy concerns of the SNS users is also discussed in detail. The literature review reveals the rights and privileges of SNS users regarding the privacy policy of Facebook and the legal framework (information privacy) of South Africa. This information and the results of this study can be utilised both by the SNS users and the platform provider to make the use of SNSs like Facebook as a positive experience for all.

6.5 Research Limitations

This study has certain limitations that I wish to acknowledge at this stage.

Firstly, though many researchers (Dienlin & Metzger, 2016; Krasnova, Veltri & Günther, 2012; Sun, Wang, Shen, & Zhang, 2015) have used the Privacy Calculus Theory to study the self-disclosure behaviour of SNS users, some of them have expressed their reservations about the use of this theory. They argue that users do not always conduct the cost-benefit analysis as a perfect calculus, due to factors like attitude, lack of all the information or data, hyperbolic discounting etc.

Secondly, the original researchers of the US and German study compared the results obtained from their research with the help of determinants of National culture derived by Hofstede for various national cultures. This could not be done for this study, as the original data from the original research was not made available for the use of this study.

Thirdly, Facebook was the only SNS that was considered for this study. As the young generation is considered to be moving away from Facebook as their preferred SNS platform, this can also be considered as a major limitation.

And finally, as convenience sampling was used, the sample size may not be a true reflection of the general South African SNS user demographic.

6.6 Future Research

The limitations that were identified above, holds immense future possibilities to further our understanding of SNS user behaviour.

Firstly, more research studies into TPB, TRA, Privacy Calculus and the attitudes that govern the SNS users while they self-disclose their personal information and the values that they place on the various determinants of self-disclosure should be undertaken. This may help future researchers to develop a new model or modify and strengthen the theoretical framework used for this study.

Secondly, researchers should try and replicate this study amongst different National cultures to determine whether National cultures influence the SNS user's perceptions regarding self-disclosure and the values placed on the determinants of self-disclosure.

Thirdly, future researchers should include more SNS platforms and the instrument should be modified accordingly to address the challenges faced.

And finally, the same research can be replicated in South Africa by selecting a sample size which is large and which reflects the true demographic representation of South African SNS users.

6.7 Conclusion

This research is a replication of another study conducted in Germany and USA. We started this study by providing a detailed road map detailing how this research will be conducted. An extensive research into related literature was conducted and existing views, opinions and results were presented. The methodology used for this study was explained next, including the data analysis process. The data was analysed, discussed and the results were presented in the following chapters. This study has revealed the existence of privacy paradox amongst the South African SNS users. It has also revealed how the different constructs included in the theoretical framework influences the cost-benefit analysis and the values that South African SNS users place on the various determinants of self-disclosure.

.

REFERENCES

Acquisti, A., Gross, R., & Stutzman, F. (2014). Face Recognition and Privacy in the Age of Augmented Reality. *Journal of Privacy and Confidentiality*, 6(2), 1.

Acquisti, A., & Grossklags, J. (2005). Privacy and Rational Decision Making. *IEEE Security & Privacy*, 26–33.

Ahmed, S. M. S., & Zulhuda, S. (2015). The concept of internet of things and its challenges to privacy. *South East Asia Journal of Contemporary Business, Economics and Law*, 8(4).

Alhabash, S., Park, H., Kononova, A., Chiang, Y.-h., & Wise, K. (2012). Exploring the motivations of Facebook use in Taiwan. *Cyberpsychology, Behavior, and Social Networking,* 15(6), 304-311.

Anderson, M., & Jiang, J. (2018). Teens, social media & technology 2018. Washington, DC: *Pew Internet & American Life Project*. Retrieved June, 3, 2018.

Bazarova, N. (2012). Contents and contexts: disclosure perceptions on facebook. In *Proceedings of the ACM 2012 Conference on Computer Supported Cooperative Work* (pp. 369–372). Seattle, Washington, USA: ACM.

Bidwell, N. (2010). Ubuntu in the network: humanness in social capital in rural Africa. *interactions*, 17(2), 68-71.

Booysen, L. (2001). The duality in South African leadership: Afrocentric or Eurocentric. *South African Journal of Labour Relations*, 25(3 & 4), p. 36-64.

Boyd, D. M., & Ellison, N. B. (2010). Social network sites: definition, history, and scholarship. *IEEE Engineering Management Review*, 38(3), 16-31.

Brandtzæg P.B., & Heim J. (2009) Why People Use Social Networking Sites. In: Ozok A.A., Zaphiris P. (eds) *Online Communities and Social Computing*. OCSC 2009. Lecture Notes in Computer Science, vol 5621. Springer, Berlin, Heidelberg

Brandtzaeg, P. B., & Heim, J. (2011). A typology of social networking sites users. *International Journal of Web Based Communities*, 7(1), 28-51.

Carifio, J., & Perla, R. J. (2007). Ten common misunderstandings, misconceptions, persistent myths and urban legends about Likert scales and Likert response formats and their antidotes. *Journal of Social Sciences*, 3(3), 106-116.

Cătoiu, I., Orzan, M., Macovei, O.-I., & Iconaru, C. (2014). Modelling users' trust in online social networks. *Amfiteatru Economic Journal*, 16(35), 289-302

Christofides, E., Muise, A., & Desmarais, S. (2009). Information disclosure and control on Facebook: are they two sides of the same coin or two different processes? *CyberPsychology & Behavior*, 12(3), 341-345.

Christofides, E., Muise, A., & Desmarais, S. (2012). Risky disclosures on Facebook: The effect of having a bad experience on online behavior. *Journal of Adolescent Research*, 27(6), 714-731.

Cullen, R. (2009). Culture, identity and information privacy in the age of digital government. *Online Information Review*, 33(3), 405-421.

Derlaga, V. J., & Berg, J. H. (2013). Self-disclosure: Theory, research, and therapy: Springer Science & Business Media.

Dienlin, T. and Metzger, M.J. (2016), An Extended Privacy Calculus Model for SNSs: Analyzing Self-Disclosure and Self-Withdrawal in a Representative U.S. Sample. *Journal of Computer-Mediated Communication*, 21: 368-383.

Diggelmann, O., & Cleis, M. N. (2014). How the right to privacy became a Human Right. *Human Rights Law Review*, 14(3), 441-458.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17(1), 61-80.

Drolet, D. (2013). Millennials Migrate to Niche Social Networks. Interview from http://totalaccess.emarketer.com/

Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. Journal of Computer-Mediated Communication, 13(1), 210-230.

Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The benefits of Facebook "friends:" Social capital and college students' use of online social network sites. Journal of Computer-Mediated Communication, 12(4), 1143-1168.

Ellison, N. B., Vitak, J., Gray, R., & Lampe, C. (2014). Cultivating social resources on social network sites: Facebook relationship maintenance behaviors and their role in social capital processes. Journal of Computer-Mediated Communication, 19(4), 855-870.

Elmi, A. H., Iahad, N. A., & Ahmed, A. A. (2012). Factors Influence Self-Disclosure Amount in Social Networking Sites (SNSs). Journal of Information Systems Research and Innovation, 1(1), 43 - 50.

European-Commission. (2012). Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (Vol. 11). ec.europa.eu/justice/dataprotection/document/review2012/com_2012_11_en.pdf.

Falk, S., & Riel, N. (2013). Cultural Differences in User Privacy Behavior on Social Networking Sites : An Empirical Study comparing German and Swedish Facebook Users (Dissertation). Retrieved from http://urn.kb.se/resolve?urn=urn:nbn:se:hj:diva-21648

Fishbein, M. (1979). A theory of reasoned action: Some applications and implications. *Nebraska Symposium on Motivation, 27,* 65–116.

Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior*, 25(1), 153-160.

Fogg B.J., & Iizawa D. (2008) Online Persuasion in Facebook and Mixi: A Cross-Cultural Comparison. In: Oinas-Kukkonen H., Hasle P., Harjumaa M., Segerståhl K., Øhrstrøm P. (eds) Persuasive Technology. PERSUASIVE 2008. Lecture Notes in Computer Science, vol 5033. Springer, Berlin, Heidelberg

Fourli, I. (2010). Business model for mobile social network.

Gangadharbatla, H. (2008). Facebook me: Collective self-esteem, need to belong, and internet self-efficacy as predictors of the iGeneration's attitudes toward social networking sites. *Journal of Interactive Advertising*, 8(2), 5-15.

Gavison, R. (1980). Privacy and the Limits of Law. *The Yale Law Journal*, 89(3), 421-471.

Glass, G. V., Peckham, P. D., & Sanders, J. R. (1972). Consequences of failure to meet assumptions underlying the fixed effects analyses of variance and covariance. *Review of Educational Research*, 42(3), 237-288.

Gonzalez, C. (2010). Social media best practices for communication professionals through the lens of the fashion industry. Unpublished dissertation. University of Southern California.

Govani, T., & Pashley, H. (2005). Student awareness of the privacy implications when using Facebook. *Unpublished paper presented at the "Privacy Poster Fair" at the Carnegie Mellon University School of Library and Information Science*, 9, 1-17.

Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. In *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society (WPES'05)* (pp. 71–81). https://doi.org/10.1145/1102199.1102214

Hoadley, C. M., Xu, H., Lee, J. J., & Rosson, M. B. (2010). Privacy as information access and illusory control: The case of the Facebook News Feed privacy outcry. *Electronic Commerce Research and Applications*, 9(1), 50-60.

Hofstede, G. (1984). Culture's consequences: International differences in work-related values. *Volume 5 of Cross-Cultural Research and Methodology Series, Sage Library of Social Research; V. 101*

Hofstede, G. (2001). Culture's consequences: Comparing values, behaviors, institutions and organizations across nations. Second Edition. Sage.

Introna, L. D. (1997). Privacy and the computer: why we need privacy in the information society. *Metaphilosophy*, 28(3), 259-275.

Jensen, C., Potts, C., & Jensen, C. (2005). Privacy practices of Internet users: self-reports versus observed behavior. *International Journal of Human-Computer Studies*, 63(1), 203-227.

Jiang, Z., Heng, C. S., & Choi, B. C. (2013). Research Note—Privacy Concerns and Privacy-Protective Behavior in Synchronous Online Social Interactions. *Information Systems Research*, 24(3), 579-595.

Joinson, A. N. (2001). Self-disclosure in computer-mediated communication: The role of self-awareness and visual anonymity. *European Journal of Social Psychology*, 31(2), 177-192.

Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal*. 25(6), 607-635.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, 64, 122-134.

Krasnova, H., Kolesnikova, E., & Guenther, O. (2009). " It Won't Happen To Me!": Self-Disclosure in Online Social Networks. AMCIS 2009 Proceedings, 343.

Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. *Journal of information Technology* 25(2), 109-125.

Krasnova, H. & Veltri, N.F. (2010) Privacy Calculus on Social Networking Sites: Explorative Evidence from Germany and USA. *2010 43rd Hawaii International Conference on System Sciences*, Honolulu, HI, 2010, pp. 1-10.

Krasnova, H., Veltri, N. F., & Günther, O. (2012). Self-disclosure and privacy calculus on social networking sites: The role of culture. *Business & Information Systems Engineering*, 4(3), 127-135.

Krasnova, H., Wenninger, H., Widjaja, T., & Buxmann, P. (2013). Envy on Facebook: A Hidden Threat to Users' Life Satisfaction? *Wirtschaftsinformatik*, 92.

Krombholz, K., Merkl, D., & Weippl, E. (2012). Fake identities in social media: A case study on the sustainability of the facebook business model. *Journal of Service Science Research*, 4(2), 175.

Kwak, K. T., Choi, S. K., & Lee, B. G. (2014). SNS flow, SNS self-disclosure and post hoc interpersonal relations change: Focused on Korean Facebook user. *Computers in Human Behavior*, 31, 294-304.

Kwan, G. C. E., & Skoric, M. M. (2013). Facebook bullying: An extension of battles in school. *Computers in Human Behavior*, 29(1), 16-25.

Lange, P. G. (2007). Publicly private and privately public: Social networking on YouTube. *Journal of Computer-Mediated Communication*, 13(1), 361-380.

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues*, 33(3), 22-42.

Lehikoinen, J. T., Olsson, T., & Toivola, H. (2008). Privacy regulation in online social interaction. *Proceedings of IADIS International Conference, ICT, Society and Human Beings*, 22-24 July, 2008, Amsterdam, the Netherlands.

Lewis, K., Kaufman, J., & 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), 79-100.

Li-Barber, K. T. (2012). Self-disclosure and student satisfaction with Facebook. *Computers in Human Behavior*, 28(2), 624-630.

Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems*, 54(1), 471-481.

Li, X., & Chen, X. (2010), Factors Affecting Privacy Disclosure on Social Network Sites: An Integrated Model, In *Proceedings of 2010 International Conference on Multimedia Information Networking and Security*, Nanjing, Jiangsu, 4-6 Nov., pp. 315-319.

Liu, C., Marchewka, J. T., & Ku, C. (2004). American and Taiwanese perceptions concerning privacy, trust, and behavioral intentions in electronic commerce. *Journal of Global Information Management (JGIM)*, 12(1), 18-40.

Livingstone, S. (2008). Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression. *New Media & Society*, 10(3), 393-411.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, 15(4), 336-355.

Nagy, J., & Pecho, P. (2009). Social networks security. Paper presented at the Emerging Security Information, Systems and Technologies, *Proceedings of Third International Conference on Emerging Security Information, Systems and Technologies: SECURWARE'09*.

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, 41(1), 100-126.

Nosko, A., Wood, E., & Molema, S. (2010). All about me: Disclosure in online social networking profiles: The case of FACEBOOK. *Computers in Human Behavior*, 26(3), 406-418.

Pavlou, P. A. (2011). State of the information privacy literature: Where are we now and where should we go?, *MIS Quarterly*, 35(4), 977-988.

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy and Marketing*, 19(1), 27-41.

Phelps, J. E., D'Souza, G., & Nowak, G. J. (2001). Antecedents and consequences of consumer privacy concerns: An empirical investigation. *Journal of Interactive Marketing*, 15(4), 2-17.

Sagioglou, C., & Greitemeyer, T. (2014). Facebook's emotional consequences: Why Facebook causes a decrease in mood and why people still use it. *Computers in Human Behavior*, 35, 359-363.

Seidman, G. (2013). Self-presentation and belonging on Facebook: How personality influences social media use and motivations. *Personality and Individual Differences*, 54(3), 402-407.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS Quarterly*, 35(4), 989-1016.

Solove, D. J. (2012). Introduction: Privacy self-management and the consent dilemma. *Harvard Law Review*, 126, 1880.

Stutzman, F., Capra, R., & Thompson, J. (2011). Factors mediating disclosure in social network sites. *Computers in Human Behavior*, 27(1), 590-598.

Stutzman, F., & Hartzog, W. (2012). Boundary regulation in social media. *Proceedings of the ACM 2012 conference on Computer Supported Cooperative Work*. Seattle, WA, USA, February 11-15

Sun, Y., Wang, N., Shen, X.-L., & Zhang, J. (2015). Location information disclosure in location-based social network services: Privacy calculus, benefit structure, and gender differences. *Computers in Human Behavior*. 52, 278-292.

Tagtmeier, C. (2010). Facebook vs. Twitter: Battle of the social network stars. *Computers in Libraries*, 30(7), 6.

Trepte, S., & Reinecke, L. (2013). The reciprocal effects of social network site use and the disposition for self-disclosure: A longitudinal study. *Computers in Human Behavior*, 29(3), 1102-1112.

Tschersich, M., & Botha, R.A. (2014). Exploring the Impact of Restrictive Default Privacy Settings on the Privacy Calculus on Social Network sites. *Proceedings of 22nd European Conference on Information Systems (ECIS 2014)*.

Tucker, C. E. (2014). Social networks, personalized advertising, and privacy controls. *Journal of Marketing Research.* 51(5), 546-562.

United States National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. 1979. *The Belmont Report: ethical principles and guidelines for the protection of human subjects of research*, Washington, DC: US Department of Health, Education, and Welfare.

Utz, S., Muscanell, N., & Khalid, C. (2015). Snapchat elicits more jealousy than Facebook: A comparison of Snapchat and Facebook use. *Cyberpsychology, Behavior, and Social Networking*, 18(3), 141-146.

Van Zoonen, L. (2016). Privacy concerns in smart cities. *Government Information Quarterly*, 33(3), 472-480.

Vasalou, A., Joinson, A. N., & Courvoisier, D. (2010). Cultural differences, experience with social networks and the nature of "true commitment" in Facebook. *International Journal of Human-Computer Studies*, 68(10), 719-728.

Wang, Y., Norcie, G., Komanduri, S., Acquisti, A., Leon, P. G., & Cranor, L. F. (2011). I regretted the minute I pressed share: A qualitative study of regrets on Facebook. In *Proceedings of the Seventh Symposium on Usable Privacy and Security (SOUPS '11)*. Association for Computing Machinery, New York, NY, USA, Article 10, 1–16.

Warren, C. and Laslett, B. (1977), Privacy and Secrecy: A Conceptual Comparison. *Journal of Social Issues*, 33(3): 43-51.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, 4(5), 193-220.

Westin, A. F. (1968). Privacy and freedom. *Washington and Lee Law Review*, 25(1), 166.

Wheeless, L. R. (1978). A follow-up study of the relationships among trust, disclosure, and interpersonal solidarity. *Human Communication Research*, 4(2), 143-157.

Wheeless, L. R., & Grotz, J. (1976). Conceptualization and measurement of reported self-disclosure. *Human Communication Research*, 2(4), 338-346.

Willard, N. (2006). Cyberbullying and cyberthreats: Responding to the Challenge of online social aggression, threats, and distress. Research press, Champaign, IL

Wu, K.-W., Huang, S. Y., Yen, D. C., & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. *Computers in Human Behavior*, 28(3), 889-897.

Xu, F., M, K., & Chen, X. (2013). Factors affecting privacy disclosure on social network sites: an integrated model. *Electronic Commerce Research*, 13(2), 151-168.

Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2008). Examining the formation of individual's privacy concerns: Toward an integrative view. In *Proceedings of the 2008 International Conferences on Information Systems (ICIS 2008)*, Paper 6.

Xu, Y. C., Yang, Y., Cheng, Z., & Lim, J. (2014). Retaining and attracting users in social networking services: An empirical investigation of cyber migration. *The Journal of Strategic Information Systems*, 23(3), 239-253.

Young, A. L., & Quan-Haase, A. (2009). Information revelation and internet privacy concerns on social network sites: a case study of facebook. In *C&T '09: Proceedings of the Fourth International Conference on Communities and Technologies*, 265–274

Youyou, W., Kosinski, M., & Stillwell, D. (2015). Computer-based personality judgments are more accurate than those made by humans. *Proceedings of the National Academy of Sciences*, 112(4), 1036-1040.

Yu, J., Hu, P. J.-H., & Cheng, T.-H. (2015). Role of affect in self-disclosure on social network websites: A test of two competing models. *Journal of Management Information Systems*, 32(2), 239-277.

Zhao, S., Grasmuck, S., & Martin, J. (2008). Identity construction on Facebook: Digital empowerment in anchored relationships. *Computers in Human Behavior*, 24(5), 1816-1836.

Zukowski, T., & Brown, I. (2007). Examining the influence of demographic factors on internet users' information privacy concerns. In *Proceedings of the 2007 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on IT Research in Developing Countries (SAICSIT'07)*. 2-3 Oct, Port Elizabeth, South Africa, 197-204

APPENDIX A
QUESTIONNAIRE

1.1.	**Please enter your age.** In years (whole numbers)
	Nceda ufake iminyaka yakho yobudala. Ngeminyaka (ebhalwe ngamanani apheleleyo)
1.2.	**Gender** ○ Male ○ Female
	Isini Indoda Umfazi
1.3.	**The institution in which you are currently registered.** ○ WSU ○ NMU
	Iziko lemfundo ephakamieyo ofunda kulo ngoku WSU NMU
1.4.	**Name & Location of the School where you have completed your Matric.** You can provide the name of the school & indicate whether the school was located in a town, village, location, city, etc.
	Igama nendawo yeSikolo ophumelele kuso iMatrikhi yakho. Unganika igama lesikolo uze ubonise ukuba esi sikolo sisedolophini, elalini, elokishini, esixekweni, njalo njalo.
1.5.	**Race** ○ Black ○ White ○ Coloured ○ Indian ○ Asian ◉ Other:

	Uhlanga Ontsundu Omhlophe Owebala Indiya UmAsia Olunye uhlanga
1.6.	**How many years of tertiary experience do you have?** Years of studying in a tertiary institution like FET, University etc. ○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ More than five years
	Mingaphi iminyaka ukwiziko lemfundo ephakamileyo? Imiminyaka ufunda kwiziko lemfundo ephakamileyo elinje ngeFET, iYunivesithi njalo njalo. 1 2 3 4 5 Ngaphezu kweminyaka emihlanu
1.7.	**On a scale of 1 to 5, how would you grade your computer skills?** 1 = No skills at all & 5 = Highly skilled.
	Ngokomlinganiselo ka-1 ukuya ku-5, ungazibeka ndawoni izakhono zakho zekhompyutha? 1 = Andinazakhono tu 5 = Ndinezakhono kakhulu
1.8.	**Are you a registered user of Facebook?** ○ Yes ○ No
	Ungumsebenzisi obhalisiweyo kaFacebook? Ewe Hayi
2	General questions about your Facebook use & activities.
	Imibuzo gabalala malunga nendlela omsebenzisa ngayo uFacebook kunye nezinto ozenza kuye.

2.1	**How do you access Facebook?** Select all the correct answers. For example, if you use your phone, tablet and PC for accessing Facebook, select all three. ☐ Phone ☐ Tablet ☐ Personal Computer ☐ Other
	Ungena njani kuFacebook? Khetha zonke iimpendulo ezichanekileyo. Umzekelo, ukuba usebenzisa ifowuni, ithablethi nePC yakho ukungena kuFacebook, zikhethe zontathu. Ifowuni IThablethi Ikhompyutha yakho Enye
2.2.	**How long have you been using Facebook?** ○ Less than One year ○ Around 2 years ○ Around 3 years ○ Around 4 years ○ Around 5 years ○ Greater than Five years
	Lingakanani ixesha usebenzisa uFacebook? Ngaphantsi konyaka omNye Malunga neminyaka emi-2 Malunga neminyaka emi-3 Malunga neminyaka emi-4 Malunga neminyaka emi-5 Ngaphezu kweminyaka emiHlanu
2.3.	**On a scale of 1 to 5, indicate how frequently do you use Facebook?** Select the best possible scenario. Select 1 if you rarely use it and 5 if you use it regularly. 1 2 3 4 5 I visit Facebook very rarely. ○ ○ ○ ○ ○ I visit Facebook regularly.

	Kumlinganiso ophakathi ko-1 no-5, chaza ukuba umsebenzisa kangakanani na uFacebook. Khetha eyona meko ingcono. Khetha u-1 ukuba awufane umsebenzise, uze ukhethe u-5 ukuba umsebenzisa kakhulu. 1 2 3 4 5 Ndingena manqaphanqapha kakhulu kuFacebook. ○ ○ ○ ○ ○ Ndingena rhoqo kuFacebook.
2.4.	**Describe your activities on Facebook.** Select the best possible scenario. You can select more than one activities. ☐ Upload contents (text, images, videos, music etc) ☐ Like, Tag etc. ☐ News Feeds ☐ Communicate with friends ☐ Try to make new friends on Facebook ☐ Share links or other interesting things. ☐ I do not do any of the above. I am just a passive follower of my friends activities. ☐ Other:
	Chaza ezona zinto uzenzayo kuFacebook. Khetha eyona meko ichanekileyo. Ungakhetha ngaphezu kwento enye kwezi zilandelayo. Ukukhuphela iikhontenti (izinto ezibhaliweyo, imifanekiso, iividiyo, umculo, njalo njalo) Ukuthanda, ukuthega, njalo njalo Iindaba eziFakiweyo Ukuncokola nabahlobo Ukuzama ukwenza abahlobo abantsha kuFacebook Ndidlulisa iilinki okanye ezinye izinto ezinika umdla. Andenzi nenye kwezi zingentla. Ndilandela nje izinto ezenziwa ngabahlobo bam
3	Expected Benefits: Questions in this Section relates to the benefits that you expect from using Facebook. Indicate to what extend you agree or disagree with the following statements. 1=Strongly Disagree; 2=Disagree; 3=Slightly Disagree; 4=Neutral; 5=Slightly Agree; 6=Agree; 7=Strongly Agree.

	Izinto olindele ukuzifumana ngokusebenzisa uFacebook: Imibuzo ekweli Candelo inxulumene nezinto olindele ukuzifumana ngokusebenzisa uFacebook. Chaza ukuba uvumelana okanye awuvumelani kangakanani nezi ntetho zilandelayo. 1=Andivumelana tu; 2=Andivumelani; 3=Andivumelani Kancinci; 4= Ndiphakathi; 5=Ndivumelana Kancinci; 6=Ndiyavumelana; 7= Ndivumelana Ngamandla.
3.1.	**Facebook is useful in supporting relationships with my friends....**
	UFacebook uluncedo ekuxhaseni ubuhlobo bam nabahlobo bam....
3.2.	**Facebook is convenient to stay in touch with my friends....**
	UFacebook yindlela elula yokuhlala ndinxibelelana nabahlobo bam....
3.3.	**Facebook is useful for developing relationships to people (business or private)....**
	UFacebook uluncedo ekwakheni ubuhlobo nabantu (nokuba bobomsebenzi okanye obumalunga nawe)....
3.4.	**I have fun on Facebook.**
	Ndiyamonwabela uFacebook.
3.5.	**I spend enjoyable and relaxing time on Facebook.**
	Ndichitha ixesha elimnandi nelipholileyo kuFacebook.
3.6.	**Facebook allows me to make a better impression on others.....**
	UFacebook undenza ndikwazi ukuziveza ngendlela engcono kwabanye abantu.....
3.7.	**Facebook allows me to present myself in a favourable way with others.**
	UFacebook undinceda ekubeni ndizibonakalise ngohlobo olulungileyo kwabanye abantu.
4	Privacy Concerns: The questions in this section deals with your privacy concerns on Facebook.
	How much are you concerned that the information submitted on Facebook: …… (1= Not concerned at all; 4= Moderately concerned; 7=Very much concerned)
	Iinkxalabo malunga nobufmihlo: Le mibuzo ikweli candelo ijongene neenkxalabo zobumfihlo bemiba yakho kuFacebook.
	Uxhalabe kangakanani malunga nokuba iinkcukacha ezifakwe kuFacebook: ..... (1 = Andixhalabanga tu; = 4 Ndixhalabe ngokuphakathi; 7 = Ndixhalabe kakhulu)
4.1.	**How much are you concerned that the information submitted on Facebook can be used in a way you did not foresee?**
	Ikuxhalabisa kangakanani into yokuba iinkcukacha ezifakwe kuFacebook zingasetyenziswa ngendlela obungayilindelanga?
4.2.	**How much are you concerned that the information submitted on Facebook can become available to someone without your knowledge?**
	Ikuxhalabisa kangakanani into yokuba iinkcukacha ezifakwe kuFacebook zingafunyanwa ngomnye umntu ungayazi wena loo nto?
4.3.	**How much are you concerned that the information submitted on Facebook can be misinterpreted?**
	Ikuxhalabisa kangakanani into yokuba iinkcukacha ezifakwe kuFacebook zinokutolikwa ngenye indlela?

4.4.	**How much are you concerned that the information submitted on Facebook can be continuously spied on (by someone unintended).?**
	Ikuxhalabisa kangakanani into yokuba iinkcukacha ezifakwe kuFacebook zingasoloko zikrotywa (ngumntu ebezingafakelwanga yena)?
5	**Perceived Damage: The questions in this section deals with the damage that you think can be caused if any privacy violations occur.**
	Please assess the amount of the resulting damage to you (financial, to your reputation, social, psychological) if the following events took place? (1=Very low Damage; 4=Moderate Damage; 7=Very high Damage)
	Ubungozi obuqikelelelekayo: Imibuzo ekweli candelo ijongene nomonakalo ocinga ukuba unokubangelwa kuko nakuphi ukungalandelwa kobumfihlo
	Nceda uhlole ubungakanani bomonakalo kuwe (ngokwezemali, ngokwesidima sakho, entlalweni, ngokwasengqondweni) xa kunokwenzeka oku kulandelayo? (1 = Ngumonakalo omncinci kakhulu; 4 = Ngumonakalo ophakathi; 7 = Ngumonakalo omkhulu kakhulu)
5.1.	**If your personal information on Facebook was used for commercial purposes (e.g. market research, advertising).**
	Ukuba iinkukacha zakho zobuqu ezikuFacebook zakha zasetyenziselwa ezoshishino (umz. uphando lwezeentengiso, izibhengezo).
5.2.	**If your personal information on Facebook was shared with other parties (e.g. employer, governmental agencies, etc.).**
	Ukuba iinkcukacha zakho zobuqu ezikuFacebook zakha zadluliselwa kwabanye abantu (umz. umqeshi, iiarhente zikarhulumente, njalo njalo).
5.3.	**If your personal information on Facebook became available to unknown individuals or companies without your knowledge.**
	Ukuba iinkcukacha zakho zobuqu ezikuFacebook zakha zafunyanwa ngabantu ongabaziyo okanye iinkampani ongazaziyo wabe wena ungayazi loo nto.
5.4.	**If your personal information on Facebook was accessed by someone unintended (e.g. "ex", parents, teacher, employer, unknown person, etc.).**
	Ukuba iinkcukacha zakho zobuqu ezikuFacebook zakha zajongwa ngumntu ebezingafakelwanga yena (umz. owayesakuba sisithandwa sakho, abazali bakho, utitshala, umqeshi, umntu ongamaziyo, njalo njalo).
5.5.	**If your personal information on Facebook was used against you by someone.**
	Ukuba kukho umntu okhe wasebenzisa iinkcukacha zakho zobuqu ezikuFacebook ukulwa nawe.
5.6.	**If your personal information on Facebook was used to embarrass you by someone.**
	Ukuba iinkcukacha zakho zobuqu ezikuFacebook zakha zasetyenziswa ngomnye umntu ekukuhlazeni.
5.7.	**If your personal information on Facebook was continuously spied on (by someone to whom it was not intended).**
	Ukuba inkcukacha zakho zobuqu ezikuFacebook zakha zamana zikrotywa (ngumntu ezazingafakelwanga yena).

6	**Perceived likelihood: The questions in this section deals with the possible likelihood (in your opinion) of a privacy violation and damage.**
	Please assess the likelihood of the following events: (1=Not at all likely; 4=Moderately likely; 7=Very likely)
	Ukuqikelelwa kokuba kunokwenzeka: Le mibuzo ikweli candelo ijongene nokuqikelelwa kokuba kunokwenzeka kangakanani (ngokucinga kwakho) kokungalandelwa kobumfihlo kunye nomonakalo.
	Nceda uhlole ukuba zinokwenzeka kangakanani ezi zehlo zilandelayo: [(1=Akunakwenzeka tu; 4=Kunokwenzeka ngokuphakathi; 7=Kungenzeka kakhulu)
6.1.	**Information you provide on Facebook will be used for commercial purposes (e.g. market research, advertising).**
	Inkcukacha ozifaka kuFacebook ziza kusetyenziselwa ezoshishino (umz. uphando lweentengiso, izibhengezo).
6.2.	**Information you provide on Facebook will be shared with other parties (e.g. employer, governmental agencies, etc.).**
	Iinkcukacha ozifaka kuFacebook ziza kudluliselwa kwabanye abantu (umz. umqeshi, iiarhente zikarhulumente, njalo njalo).
6.3.	**Information you provide on Facebook will become available to unknown individuals or companies without your knowledge.**
	Iinkcukacha ozifaka kuFacebook ziza kufumaneka kubantu ongabaziyo okanye iinkampani ongazaziyo ube wena ungayazi loo nto.
6.4.	**Information you provide on Facebook will be accessed by someone you don't want (e.g. "ex", parents, teacher, employer, unknown person, etc.).**
	Iinkcukacha ozifaka kuFacebook ziza kufunyanwa ngumntu ongafuniyo ukuba azifumane (umz. owayesakuba sisithandwa sakho, abazali, utitshala, umqeshi, umntu ongamaziyo, njalo njalo).
6.5.	**Information you provide on Facebook will be used against you by someone.**
	Iinkcukacha ozifaka kuFacebook ziza kusetyenziswa ngumntu othile ukulwa nawe.
6.6.	**Information you provide on Facebook will be used to embarrass you by someone.**
	Iinkcukacha ozifaka kuFacebook ziza kusetyenziswa ngomnye umntu ekukuhlazeni.
6.7.	**Information you provide on Facebook will be continuously spied on (by someone to whom it was not intended).**
	Iinkcukacha ozifaka kuFacebook ziza kumana zikrotywa (ngumntu ebezingafakelwanga yena).
7	**Trust in Social Networking Service (SNS) provider: Do you trust Facebook?**
	Indicate to what extend you agree or disagree with the following statements? (1=Strongly Disagree; 2=Disagree; 3=Slightly Disagree; 4=Neutral; 5=Slightly Agree; 6=Agree; 7=Strongly Agree.)
	Ukuthemba umniki weNkonzo yamaQonga oNxibelelwano (iSNS): Uyamthemba uFacebook?
	Chaza ukuba uvumelana okanye awuvumelani kangakanani nezi ntetho zilandelayo? (1=Andivumelana tu; 2=Andivumelani; 3=Andivumelani Kancinci; 4= Ndiphakathi; 5=Ndivumelana Kancinci; 6=Ndiyavumelana; 7= Ndivumelana Ngamandla.)

7.1.	**In general, Facebook is open and receptive to the needs of its members.**
	Xa sithetha gabalala, uFacebook uvulelekile yaye uyazamkela iimfuno zamalungu akhe.
7.2.	**In general, Facebook makes good-faith efforts to address most member concerns.**
	Xa sithetha gabalala, uFacebook wenza iinzame ezithembekileyo zokufezekisa uninzi lweenkxalabo zamalungu akhe.
7.3.	**In general, Facebook is honest in its dealings with me.**
	Xa sithetha gabalala, inyanisekile indlela uFacebook aqhuba ngayo nam.
7.4.	**In general, Facebook keeps its commitments to its members.**
	Xa sithetha gabalala, uFacebook uyazigcina izithembiso zakhe kumalungu akhe.
7.5.	**In general, Facebook is trustworthy.**
	Xa sithetha gabalala, uFacebook uthembekile.
7.6.	**In general, Facebook tells the truth related to the collection and use of the personal information.**
	Xa sithetha gabalala, uFacebook uthetha inyani ngokunxulumene nokuqokelelwa kunye nokusetyenziswa kweenkcukacha zobuqu.
7.7.	**In general, Facebook is competent in protecting the information I provide.**
	Xa sithetha gabalala uFacebook uyakwazi ukuzikhusela iinkcukacha endizifaka kuye.
8	**Trust in SNS members: Do you trust the other members in your Facebook network?**
	Indicate to what extend you agree or disagree with the following statements? (1=Strongly Disagree; 2=Disagree; 3=Slightly Disagree; 4=Neutral; 5=Slightly Agree; 6=Agree; 7=Strongly Agree.)
	Ukuthemba amalungu iSNS: Uyawathemba amanye amalungu akwinethiwekhi yakho kaFacebook?
	Chaza ukuba uvumelana okanye awuvumelani kangakanani nezi ntetho zilandelayo? (1=Andivumelana tu; 2=Andivumelani; 3=Andivumelani Kancinci; 4= Ndiphakathi; 5=Ndivumelana Kancinci; 6=Ndiyavumelana; 7= Ndivumelana Ngamandla.)
8.1.	**Generally, I trust that Facebook users will not to misuse my sincerity on Facebook.**
	Xa sithetha gabalala, ndinethemba lokuba abasebenzisi bakaFacebook abazi kukuxhaphaza ukunyaniseka kwam kuFacebook.
8.2.	**Generally, I trust that Facebook users will not embarrass me for some information they learned about me through Facebook.**
	Xa sithetha gabalala, ndiyathemba ukuba abasebenzisi bakaFacebook abazi kundihlaza ngeenkcukacha ezithile abazifundileyo ngam kuFacebook.
8.3.	**Generally, I trust that Facebook users will not use the information they found about me in Facebook against me.**
	Xa sithetha gabalala, ndiyathemba ukuba abasebenzisi bakaFacebook abazi kusebenzisa iinkcukacha abazifumene kuFacebook ukulwa nam.
8.4.	**Generally, I trust that Facebook users will not use the information about me in a wrong way.**
	Xa sithetha gabalala, ndiyathemba ukuba abasebenzisi bakaFacebook abazi kusebenzisa iinkcukacha zam kakubi.

8.5.	**Generally, I trust that Facebook users are trustworthy.**
	Xa sithetha gabalala, ndiyathemba ukuba abasebenzisi bakaFacebook bathembekile.
8.6.	**Generally, I trust that Facebook users are open and delicate to each other.**
	Xa sithetha gabalala, Ndiyakuthemba ukuba abasebenzisi bakaFacebook bancokolelana ngokukhululekileyo yaye becingelana.
9	**Trust in Legal assurance:**
	Indicate to what extend you agree or disagree with the following statements? (1=Strongly Disagree; 2=Disagree; 3=Slightly Disagree; 4=Neutral; 5=Slightly Agree; 6=Agree; 7=Strongly Agree.)
	Ukuthemba isiqinisekiso sezoMthetho:
	Chaza ukuba uvumelana okanye awuvumelani kangakanani nezi ntetho zilandelayo? (1=Andivumelana tu; 2=Andivumelani; 3=Andivumelani Kancinci; 4= Ndiphakathi; 5=Ndivumelana Kancinci; 6=Ndiyavumelana; 7= Ndivumelana Ngamandla.)
9.1.	**I feel confident that existing laws protect me against abuse of my information on Facebook.**
	Ndiyithembile imithetho ekhoyo ukuba iyandikhusela ekuxhatshazweni kweenkcukacha zam ezikuFacebook.
9.2.	**Existing laws adequately protect my information on Facebook.**
	Imithetho ekhoyo iyazikhusela iinkcukacha zam ezikuFacebook.
9.3.	**The existing legal framework is good enough to make me feel comfortable using Facebook.**
	Le meko yezomthetho ikhoyo ilunge ngokwaneleyo ukundenza ndizive ndikhululekile ukuba ndingamsebenzisa uFacebook.
10.	**Awareness:**
	Indicate to what extend you agree or disagree with the following statements? (1=Strongly Disagree; 2=Disagree; 3=Slightly Disagree; 4=Neutral; 5=Slightly Agree; 6=Agree; 7=Strongly Agree.)
	Ulwazi lokuqonda:
	Chaza ukuba uvumelana okanye awuvumelani kangakanani nezi ntetho zilandelayo? (1=Andivumelana tu; 2=Andivumelani; 3=Andivumelani Kancinci; 4= Ndiphakathi; 5=Ndivumelana Kancinci; 6=Ndiyavumelana; 7= Ndivumelana Ngamandla.)
10.1.	**Generally, I find Facebook transparent in how the personal information I provide can be used.**
	Xa sithetha gabalala, ndimbona uFacebook eselubala malunga nokuba zingasetyenziswa njani iinkcukacha zam endizinikayo.
10.2.	**Facebook clearly communicates what information it can collect about me.**
	UFacebook ukucacisa gca ukuba zeziphi iinkcukacha angazithatha kum.
11	**Control over personal information**
	Ulawulo ngakwiinkcukacha zakho zobuqu
11.1.	**How much control is given to you by Facebook (e.g. through functionality, privacy policies) over the information you provide on Facebook (e.g. in my profile, on the Wall etc.)**

	Ukunika ulawulo olungakanani uFacebook (umz. ngokokumsebenzisa kwakho, ngokweepolisi zobumfihlo) malunga neenkcukacha ozinika kuFacebook (umz. kwiprofayile yam, endizixhoma kwiWall, njalo njalo.)
11.2.	**How much control is given to you by Facebook (e.g. through functionality, privacy policies) over how and in what case the information you provide can be used.**
	Ukunika ulawulo olungakanani uFacebook (umz. ngokokumsebenzisa kwakho, ngokweepolisi zobumfihlo) malunga nokuba iinkcukacha ozinikayo zingasetyenziswa njani, kweziphi iimeko.
11.3.	**How much control is given to you by Facebook (e.g. through functionality, privacy policies) over who can collect and use the information you provide.**
	Ukunika ulawulo olungakanani uFacebook (umz. ngokokumsebenzisa kwakho, ngokweepolisi zobumfihlo) malunga nokuba ngubani onokuziqokelela azisebenzise iinkcukacha ozinikayo.
11.4.	**How much control is given to you by Facebook (e.g. through functionality, privacy policies) over who can view your information on Facebook.**
	Lungakanani ulawulo akunika lona uFacebook (umz. ngokokusetyenziswa kweenkcukacha zakho, iipolisi zokuba sekhusini) malunga nokuba ngubani onokujonga iinkcukacha zakho ezikuFacebook.
11.5.	**How much control is given to you by Facebook (e.g. through functionality, privacy policies) over the actions of other users (e.g. tagging you in pictures, writing on your Wall).**
	Lungakanamni ulawula akunika lona uFacebook (umz. ngokokusetyenziswa kweenkcukacha zakho, iipolisi zokuba sekhusini) malunga nezenzo zabanye abasebenzisi (umz. ukukuthega ezifotweni, ukukubhala kwiWall).
12	**Self-disclosure:**
	Indicate to what extend you agree or disagree with the following statements? (1=Strongly Disagree; 2=Disagree; 3=Slightly Disagree; 4=Neutral; 5=Slightly Agree; 6=Agree; 7=Strongly Agree.)
	Ukuzixela:
	Chaza ukuba uvumelana okanye awuvumelani kangakanani nezi ntetho zilandelayo? (1=Andivumelana tu; 2=Andivumelani; 3=Andivumelani Kancinci; 4= Ndiphakathi; 5=Ndivumelana Kancinci; 6=Ndiyavumelana; 7= Ndivumelana Ngamandla.)
12.1.	**I have a comprehensive profile on Facebook. [Ndineprofayile kaFacebook exela konke.]**
	Indicate to what extend you have completed all sections in your profile page (personal details, work details etc.). [Bonisa ukuba uwagcwalise kangakanani na onke amacandelo epheyiji yeprofayile yakho (iinkcukacha zobuqu, iinkcukacha zomsebenzi, njalo njalo.)]
12.2.	**I always find time to keep my profile up-to-date.**
	Ndisoloko ndiyigcina iprofayile yam iineenkcukacha malunga nokuqhubekayo ebomini bam.
12.3.	**I have a detailed profile on Facebook.**
	Ndineprofayile kaFacebook ecacisa konke.

12.4.	**My profile tells a lot about me.**
	Iprofayile yam itsho okuninzi malunga nam.
12.5.	**From my Facebook profile it would be easy to find out my preferences in music, movies or books.**
	Kungalula ukufumana ukuba ndithanda wuphi umculo, iimuvi neencwadi ngokujonga iprofayile yam kaFacebook.
12.6.	**From my Facebook profile it would be easy to understand what person I am.**
	Kungalula ukundiqonda ukuba ndingumntu onjani ngokujonga iprofayile yam kaFacebook.

APPENDIX B1

Table B1.1: Mean Values Obtained for Relationship Maintenance (RM), Entertainment (EN), & Self-Presentation (SP)

Estimates

Measure: MEASURE_1

factor1	Mean	Std. Error	95% Confidence Interval	
			Lower Bound	Upper Bound
RM	4.835	.091	4.655	5.014
EN	4.927	.111	4.709	5.145
SP	4.000	.118	3.768	4.232

Table B1.2: Pairwise mean comparison between RM, EN, & SP

Pairwise Comparisons

Measure: MEASURE_1

(I) factor1	(J) factor1	Mean Difference (I-J)	Std. Error	Sig.[b]	95% Confidence Interval for Difference[b]	
					Lower Bound	Upper Bound
RM	EN	-.092	.083	.267	-.256	.071
	SP	.835*	.092	.000	.653	1.016
EN	RM	.092	.083	.267	-.071	.256
	SP	.927*	.101	.000	.727	1.127
SP	RM	-.835*	.092	.000	-1.016	-.653
	EN	-.927*	.101	.000	-1.127	-.727

Based on estimated marginal means

*. The mean difference is significant at the .05 level.

b. Adjustment for multiple comparisons: Least Significant Difference (equivalent to no adjustments).

APPENDIX B2

Table B2.1: Mean Values for individual questions posted under Relationship Maintenance

Estimates

Measure: MEASURE_1

factor1	Mean	Std. Error	95% Confidence Interval	
			Lower Bound	Upper Bound
Q1. FB is useful in supporting relationships with my friends. (RF)	4.700	.109	4.485	4.915
Q2. FB is convenient to stay in touch with my friends. (STF)	5.079	.107	4.869	5.289
Q3. FB is useful for developing Relationships to people (business or private). (DRP)	4.738	.109	4.523	4.952

Table B2.2: Differences in mean values for individual questions posted under Relationship Maintenance

Pairwise Comparisons

Measure: MEASURE_1

(I) factor1	(J) factor1	Mean Difference (I-J)	Std. Error	Sig.[b]	95% Confidence Interval for Difference[b]	
					Lower Bound	Upper Bound
Q1	Q2	-.379*	.093	.000	-.604	-.154
	Q3	-.037	.105	1.000	-.292	.217
Q2	Q1	.379*	.093	.000	.154	.604
	Q3	.342*	.102	.003	.097	.587
Q3	Q1	.037	.105	1.000	-.217	.292
	Q2	-.342*	.102	.003	-.587	-.097

Based on estimated marginal means

*. The mean difference is significant at the .05 level.

b. Adjustment for multiple comparisons: Bonferroni.

Q1, Q2, & Q3 refer to questions Q1 – Q3 listed in Table B2.1 (above).

APPENDIX B3

Table B3.1: Estimated mean values for individual questions under Entertainment

Estimates

Measure: MEASURE_1

Entertainment	Mean	Std. Error	95% Confidence Interval	
			Lower Bound	Upper Bound
Q4. I have fun on FB. (FFB)	5.092	.115	4.865	5.318
Q5. I spend enjoyable and relaxing time on FB. (ERFB)	4.763	.117	4.531	4.994

Table B3.2: Pairwise comparisons of mean values for individual questions under Entertainment

Pairwise Comparisons

Measure: MEASURE_1

(I) Entertainment	(J) Entertainment	Mean Difference (I-J)	Std. Error	Sig.[b]	95% Confidence Interval for Difference[b]	
					Lower Bound	Upper Bound
Q1	Q2	.329*	.070	.000	.190	.468
Q2	Q1	-.329*	.070	.000	-.468	-.190

Based on estimated marginal means

*. The mean difference is significant at the .05 level.

b. Adjustment for multiple comparisons: Bonferroni.

Q1, & Q2 refer to questions Q1 – Q2 listed in Table B3.1 (above).

APPENDIX B4

Table B4.1: Mean values derived for Privacy Concerns Construct Estimates

Measure: MEASURE_1

Privacy Concerns	Mean	Std. Error	95% Confidence Interval	
			Lower Bound	Upper Bound
Q.1…can be used in a way you did not foresee	4.638	.124	4.392	4.883
Q.2…can become available to someone without your knowledge.	5.013	.137	4.743	5.282
Q.3…can be misinterpreted.	4.804	.131	4.547	5.061
Q.4 …can be continuously spied on (by someone unintended).	4.838	.139	4.564	5.111

Table B4.2: Pairwise comparisons of individual questions posted under Privacy Concerns Construct

Pairwise Comparisons

Measure: MEASURE_1

(I) Privacy Concerns	(J) Privacy Concerns	Mean Difference (I-J)	Std. Error	Sig.[b]	95% Confidence Interval for Difference[b]	
					Lower Bound	Upper Bound
Q1	Q2	-.375*	.121	.013	-.697	-.053
	Q3	-.167	.141	1.000	-.543	.210
	Q4	-.200	.141	.951	-.576	.176
Q2	Q1	.375*	.121	.013	.053	.697
	Q3	.208	.133	.717	-.146	.563
	Q4	.175	.131	1.000	-.173	.523
Q3	Q1	.167	.141	1.000	-.210	.543
	Q2	-.208	.133	.717	-.563	.146
	Q4	-.033	.119	1.000	-.350	.283
Q4	Q1	.200	.141	.951	-.176	.576
	Q2	-.175	.131	1.000	-.523	.173
	Q3	.033	.119	1.000	-.283	.350

Based on estimated marginal means

*. The mean difference is significant at the .05 level.

b. Adjustment for multiple comparisons: Bonferroni.

Q1, Q2, Q3 & Q4 refer to questions Q1 – Q4 listed in Table B4.1 (above).

APPENDIX B5

Table B5.1: Mean Values for individual questions under Perceived Damage Construct

Estimates

Measure: MEASURE_1

Perceived Damage	Mean	Std. Error	95% Confidence Interval	
			Lower Bound	Upper Bound
Q1. …was used for commercial purposes (e.g. market research, advertising).	3.954	.143	3.673	4.235
Q2. …was shared with other parties (e.g. employer, governmental agencies, etc.).	4.067	.149	3.774	4.360
Q3. …became available to unknown individuals or companies without your knowledge.	4.633	.148	4.342	4.924
Q4. …was accessed by someone you don't want (e.g. "ex", parents, teacher, employer, unknown person, etc.).	4.488	.141	4.210	4.765
Q5. …was used against you by someone.	4.933	.152	4.634	5.233
Q6. .was used to embarrass you by someone.	4.621	.150	4.326	4.916
Q7. .was continuously spied on (by someone to whom it was not intended).	4.483	.146	4.196	4.770

Table B5.2: Comparison of Mean values for individual questions under Perceived Damage Construct

Pairwise Comparisons

Measure: MEASURE_1

(I) Perceived Damage	(J) Perceived Damage	Mean Difference (I-J)	Std. Error	Sig.[b]	95% Confidence Interval for Difference[b]	
					Lower Bound	Upper Bound
Q1	Q2	-.112	.125	1.000	-.498	.273
	Q3	-.679*	.151	.000	-1.144	-.215
	Q4	-.533*	.164	.027	-1.036	-.031
	Q5	-.979*	.160	.000	-1.471	-.488
	Q6	-.667*	.160	.001	-1.157	-.176
	Q7	-.529*	.162	.026	-1.026	-.033
Q2	Q1	.112	.125	1.000	-.273	.498
	Q3	-.567*	.136	.001	-.985	-.148
	Q4	-.421	.145	.084	-.865	.024
	Q5	-.867*	.155	.000	-1.342	-.391
	Q6	-.554*	.156	.009	-1.032	-.077
	Q7	-.417	.150	.124	-.877	.044

Q3	Q1	.679*	.151	.000	.215	1.144
	Q2	.567*	.136	.001	.148	.985
	Q4	.146	.125	1.000	-.238	.530
	Q5	-.300	.133	.534	-.710	.110
	Q6	.013	.132	1.000	-.394	.419
	Q7	.150	.122	1.000	-.226	.526
Q4	Q1	.533*	.164	.027	.031	1.036
	Q2	.421	.145	.084	-.024	.865
	Q3	-.146	.125	1.000	-.530	.238
	Q5	-.446*	.139	.031	-.871	-.020
	Q6	-.133	.129	1.000	-.529	.262
	Q7	.004	.123	1.000	-.372	.380
Q5	Q1	.979*	.160	.000	.488	1.471
	Q2	.867*	.155	.000	.391	1.342
	Q3	.300	.133	.534	-.110	.710
	Q4	.446*	.139	.031	.020	.871
	Q6	.313	.102	.051	.000	.625
	Q7	.450*	.110	.001	.111	.789
Q6	Q1	.667*	.160	.001	.176	1.157
	Q2	.554*	.156	.009	.077	1.032
	Q3	-.013	.132	1.000	-.419	.394
	Q4	.133	.129	1.000	-.262	.529
	Q5	-.313	.102	.051	-.625	.000
	Q7	.138	.099	1.000	-.168	.443
Q7	Q1	.529*	.162	.026	.033	1.026
	Q2	.417	.150	.124	-.044	.877
	Q3	-.150	.122	1.000	-.526	.226
	Q4	-.004	.123	1.000	-.380	.372
	Q5	-.450*	.110	.001	-.789	-.111
	Q6	-.138	.099	1.000	-.443	.168

Based on estimated marginal means

*. The mean difference is significant at the .05 level.

b. Adjustment for multiple comparisons: Bonferroni.

Q1, Q2, Q3, Q4, Q5, Q6 & Q3 refer to questions Q1 – Q7 listed in Table B5.1 (above).

APPENDIX B6

Table B6.1: Mean values for the individual questions posted under the Perceived Likelihood Construct

Estimates

Measure: MEASURE_1

Perceived Likelihood	Mean	Std. Error	95% Confidence Interval	
			Lower Bound	Upper Bound
Q1 … will be used for commercial purposes (e.g. market research, advertising).	3.492	.132	3.232	3.751
Q2 … will be shared with other parties (e.g. employer, governmental agencies, etc.).	3.688	.134	3.424	3.951
Q3 … will become available to unknown individuals or companies without your knowledge.	3.883	.143	3.601	4.166
Q4 … will be accessed by someone you don't want (e.g. "ex", parents, teacher, employer, unknown person, etc.).	4.042	.146	3.754	4.330
Q5 … will be used against you by someone.	3.529	.135	3.264	3.794
Q6 ..will be used to embarrass you by someone.	3.458	.137	3.188	3.728
Q7 ..will be continuously spied on (by someone to whom it was not intended).	3.854	.139	3.580	4.128

Table B6.2: Mean differences for the mean values for the individual questions posted under the Perceived Likelihood Construct

Pairwise Comparisons

Measure: MEASURE_1

(I) Perceived Likelihood	(J) Perceived Likelihood	Mean Difference (I-J)	Std. Error	Sig.[b]	95% Confidence Interval for Difference[b]	
					Lower Bound	Upper Bound
Q1	Q2	-.196	.126	1.000	-.582	.190
	Q3	-.392	.139	.110	-.818	.035
	Q4	-.550*	.153	.008	-1.021	-.079
	Q5	-.038	.140	1.000	-.468	.393
	Q6	.033	.142	1.000	-.401	.468
	Q7	-.362	.142	.237	-.798	.073
Q2	Q1	.196	.126	1.000	-.190	.582
	Q3	-.196	.118	1.000	-.559	.167
	Q4	-.354	.135	.197	-.769	.061
	Q5	.158	.143	1.000	-.281	.598
	Q6	.229	.136	1.000	-.188	.646
	7	-.167	.144	1.000	-.607	.274

3	Q1	.392	.139	.110	-.035	.818
	Q2	.196	.118	1.000	-.167	.559
	Q4	-.158	.119	1.000	-.523	.207
	Q5	.354	.124	.100	-.028	.736
	Q6	.425*	.133	.034	.016	.834
	Q7	.029	.124	1.000	-.353	.411
Q4	Q1	.550*	.153	.008	.079	1.021
	Q2	.354	.135	.197	-.061	.769
	Q3	.158	.119	1.000	-.207	.523
	Q5	.513*	.122	.001	.139	.886
	Q6	.583*	.131	.000	.180	.986
	Q7	.188	.119	1.000	-.177	.552
Q5	Q1	.038	.140	1.000	-.393	.468
	Q2	-.158	.143	1.000	-.598	.281
	Q3	-.354	.124	.100	-.736	.028
	Q4	-.513*	.122	.001	-.886	-.139
	Q6	.071	.099	1.000	-.233	.375
	Q7	-.325	.118	.129	-.686	.036
Q6	Q1	-.033	.142	1.000	-.468	.401
	Q2	-.229	.136	1.000	-.646	.188
	Q3	-.425*	.133	.034	-.834	-.016
	Q4	-.583*	.131	.000	-.986	-.180
	Q5	-.071	.099	1.000	-.375	.233
	Q7	-.396*	.112	.011	-.741	-.050
Q7	Q1	.362	.142	.237	-.073	.798
	Q2	.167	.144	1.000	-.274	.607
	Q3	-.029	.124	1.000	-.411	.353
	Q4	-.188	.119	1.000	-.552	.177
	Q5	.325	.118	.129	-.036	.686
	Q6	.396*	.112	.011	.050	.741

Based on estimated marginal means

*. The mean difference is significant at the .05 level.

b. Adjustment for multiple comparisons: Bonferroni.

Q1, Q2, Q3, Q4, Q5, Q6 & Q7 refer to questions Q1 – Q7 listed in Table B6.1 (above).

APPENDIX B7

Table B7.1: Mean values for Trust in Service Provider Construct

Estimates

Measure: MEASURE_1

TRUST IN SERVICE PROVIDER (TISP)	Mean	Std. Error	95% Confidence Interval	
			Lower Bound	Upper Bound
Q1. ...is open and receptive to the needs of its members.	4.579	.113	4.356	4.802
Q2. ...makes good-faith efforts to address most member concerns.	4.529	.104	4.325	4.734
Q3. ...is honest in its dealings with me.	4.388	.116	4.160	4.615
Q4. ...keeps its commitments to its members.	4.438	.113	4.216	4.659
Q5. ...is trustworthy.	3.892	.113	3.668	4.115
Q6. ...tells the truth related to the collection and use of the personal information.	4.067	.114	3.842	4.291
Q7. ...is competent in protecting the information I provide.	4.304	.117	4.075	4.534

Table B7.2: Difference in mean values for Trust in Service Provider Construct

Pairwise Comparisons

Measure: MEASURE_1

(I) TISP	(J) TISP	Mean Difference (I-J)	Std. Error	Sig.[b]	95% Confidence Interval for Difference[b]	
					Lower Bound	Upper Bound
Q1	Q2	.050	.087	1.000	-.218	.318
	Q3	.192	.109	1.000	-.143	.526
	Q4	.142	.112	1.000	-.204	.487
	Q5	.688*	.132	.000	.281	1.094
	Q6	.513*	.125	.001	.130	.895
	Q7	.275	.131	.789	-.129	.679
Q2	Q1	-.050	.087	1.000	-.318	.218
	Q3	.142	.099	1.000	-.162	.445
	Q4	.092	.094	1.000	-.196	.379
	Q5	.638*	.116	.000	.281	.994
	Q6	.463*	.115	.002	.108	.817
	Q7	.225	.124	1.000	-.155	.605
Q3	Q1	-.192	.109	1.000	-.526	.143
	Q2	-.142	.099	1.000	-.445	.162
	Q4	-.050	.086	1.000	-.313	.213

	Q5	.496*	.102	.000	.182	.809
	Q6	.321	.115	.122	-.033	.675
	Q7	.083	.115	1.000	-.271	.437
Q4	Q1	-.142	.112	1.000	-.487	.204
	Q2	-.092	.094	1.000	-.379	.196
	Q3	.050	.086	1.000	-.213	.313
	Q5	.546*	.099	.000	.243	.849
	Q6	.371*	.113	.026	.023	.719
	Q7	.133	.119	1.000	-.233	.500
Q5	Q1	-.688*	.132	.000	-1.094	-.281
	Q2	-.638*	.116	.000	-.994	-.281
	Q3	-.496*	.102	.000	-.809	-.182
	Q4	-.546*	.099	.000	-.849	-.243
	Q6	-.175	.111	1.000	-.517	.167
	Q7	-.412*	.116	.010	-.769	-.056
Q6	Q1	-.513*	.125	.001	-.895	-.130
	Q2	-.463*	.115	.002	-.817	-.108
	Q3	-.321	.115	.122	-.675	.033
	Q4	-.371*	.113	.026	-.719	-.023
	Q5	.175	.111	1.000	-.167	.517
	Q7	-.237	.106	.543	-.563	.088
Q7	Q1	-.275	.131	.789	-.679	.129
	Q2	-.225	.124	1.000	-.605	.155
	Q3	-.083	.115	1.000	-.437	.271
	Q4	-.133	.119	1.000	-.500	.233
	Q5	.412*	.116	.010	.056	.769
	Q6	.237	.106	.543	-.088	.563

Based on estimated marginal means

*. The mean difference is significant at the .05 level.

b. Adjustment for multiple comparisons: Bonferroni.

Q1, Q2, Q3, Q4, Q5, Q6 & Q7 refer to questions Q1 – Q7 listed in Table B7.1 (above).

APPENDIX B8

Table B8.1: Mean values obtained for the individual questions under the Trust in SNS Members construct

Estimates

Measure: MEASURE_1

Trust in SNS Members (TISM)	Mean	Std. Error	95% Confidence Interval	
			Lower Bound	Upper Bound
Q.1. ...will not to misuse my sincerity on FB.	3.804	.121	3.566	4.043
Q.2. ...will not embarrass me for some information they learned about me through FB.	3.833	.113	3.611	4.056
Q.3. ...will not use the information they found about me in FB against of me.	3.750	.114	3.526	3.974
Q.4. ...will not use the information about me in a wrong way.	3.813	.112	3.592	4.033
Q.5. ...are trustworthy	3.383	.111	3.164	3.603
Q.6. ...are open and delicate to each other.	3.450	.117	3.219	3.681

Table B8.2: Difference in mean values obtained for the individual questions under the Trust in SNS Members construct

Pairwise Comparisons

Measure: MEASURE_1

(I) TISM	(J) TISM	Mean Difference (I-J)	Std. Error	Sig.[b]	95% Confidence Interval for Difference[b]	
					Lower Bound	Upper Bound
Q1	Q2	-.029	.092	1.000	-.303	.245
	Q3	.054	.092	1.000	-.220	.328
	Q4	-.008	.094	1.000	-.286	.270
	Q5	.421*	.108	.002	.100	.741
	Q6	.354	.121	.058	-.006	.714
Q2	Q1	.029	.092	1.000	-.245	.303
	Q3	.083	.084	1.000	-.166	.332
	Q4	.021	.093	1.000	-.255	.297
	Q5	.450*	.102	.000	.147	.753
	Q6	.383*	.120	.024	.027	.739
Q3	Q1	-.054	.092	1.000	-.328	.220
	Q2	-.083	.084	1.000	-.332	.166
	Q4	-.063	.076	1.000	-.288	.163

	Q5	.367*	.090	.001	.099	.634
	Q6	.300	.107	.081	-.017	.617
Q4	Q1	.008	.094	1.000	-.270	.286
	Q2	-.021	.093	1.000	-.297	.255
	Q3	.063	.076	1.000	-.163	.288
	Q5	.429*	.086	.000	.173	.685
	Q6	.362*	.099	.005	.068	.657
Q5	Q1	-.421*	.108	.002	-.741	-.100
	Q2	-.450*	.102	.000	-.753	-.147
	Q3	-.367*	.090	.001	-.634	-.099
	Q4	-.429*	.086	.000	-.685	-.173
	Q6	-.067	.084	1.000	-.317	.184
Q6	Q1	-.354	.121	.058	-.714	.006
	Q2	-.383*	.120	.024	-.739	-.027
	Q3	-.300	.107	.081	-.617	.017
	Q4	-.362*	.099	.005	-.657	-.068
	Q5	.067	.084	1.000	-.184	.317

Based on estimated marginal means

*. The mean difference is significant at the .05 level.

b. Adjustment for multiple comparisons: Bonferroni.

Q1, Q2, Q3, Q4, Q5, & Q6 refer to questions Q1 – Q6 listed in Table B8.1 (above).

APPENDIX B9

Table B9.1: Mean values for individual questions under Control Over Personal Information Construct

Estimates

Measure: MEASURE_1

Control Over Personal Information (COPI)	Mean	Std. Error	95% Confidence Interval	
			Lower Bound	Upper Bound
Q.1. …the information you provide on Facebook (e.g. in my profile, on the Wall etc.)	4.767	.105	4.559	4.974
Q.2. …how and in what case the information you provide can be used.	4.654	.104	4.448	4.860
Q.3. …who can collect and use the information you provide.	4.404	.106	4.196	4.612
Q.4. …who can view your information on Facebook?	4.521	.113	4.298	4.744
Q.5. …the actions of other users (e.g. tagging you in pictures, writing on the Wall).	4.233	.115	4.007	4.459

Table B9.2: Difference in mean values for individual questions under Control Over Personal Information Construct

Pairwise Comparisons

Measure: MEASURE_1

(I) COPI	(J) COPI	Mean Difference (I-J)	Std. Error	Sig.[b]	95% Confidence Interval for Difference[b]	
					Lower Bound	Upper Bound
Q1	Q2	.112	.085	1.000	-.128	.353
	Q3	.362*	.095	.002	.094	.631
	Q4	.246	.115	.338	-.080	.572
	Q5	.533*	.114	.000	.210	.856
Q2	Q1	-.112	.085	1.000	-.353	.128
	Q3	.250*	.074	.008	.041	.459
	Q4	.133	.094	1.000	-.133	.399
	Q5	.421*	.107	.001	.118	.724
Q3	Q1	-.362*	.095	.002	-.631	-.094
	Q2	-.250*	.074	.008	-.459	-.041
	Q4	-.117	.098	1.000	-.395	.161
	Q5	.171	.111	1.000	-.145	.487

Q4	Q1	-.246	.115	.338	-.572	.080
	Q2	-.133	.094	1.000	-.399	.133
	Q3	.117	.098	1.000	-.161	.395
	Q5	.287*	.101	.049	.000	.575
Q5	Q1	-.533*	.114	.000	-.856	-.210
	Q2	-.421*	.107	.001	-.724	-.118
	Q3	-.171	.111	1.000	-.487	.145
	Q4	-.287*	.101	.049	-.575	.000

Based on estimated marginal means

*. The mean difference is significant at the .05 level.

b. Adjustment for multiple comparisons: Bonferroni.

Q1, Q2, Q3, Q4, & Q5 refer to questions Q1 – Q5 listed in Table B9.1 (above).

APPENDIX B10

Table B10.1: Mean values for the individual questions under the Self-Disclosure construct

Estimates

Measure: MEASURE_1

SELF-DISCLOSURE (SD)	Mean	Std. Error	95% Confidence Interval	
			Lower Bound	Upper Bound
Q.1. I have a comprehensive profile on FB.	4.308	.111	4.090	4.527
Q.2. I always find time to keep my profile up-to-date.	3.792	.124	3.548	4.035
Q.3. I have a detailed profile on FB.	4.058	.125	3.812	4.304
Q.4. My profile tells a lot about me.	3.921	.123	3.679	4.162
Q.5. From my FB profile it would be easy to find out my preferences in music, movies or books.	4.188	.128	3.936	4.439
Q.6. From my FB profile it would be easy to understand what person I am.	3.821	.128	3.568	4.073

Table B10.2: Differences between the mean values for the individual questions under the Self-Disclosure construct

Pairwise Comparisons

Measure: MEASURE_1

(I) SD	(J) SD	Mean Difference (I-J)	Std. Error	Sig.[b]	95% Confidence Interval for Difference[b]	
					Lower Bound	Upper Bound
Q1	Q2	.517*	.103	.000	.212	.821
	Q3	.250	.104	.256	-.059	.559
	Q4	.388*	.110	.008	.060	.715
	Q5	.121	.124	1.000	-.246	.488
	Q6	.488*	.127	.002	.111	.864
Q2	Q1	-.517*	.103	.000	-.821	-.212
	Q3	-.267	.090	.053	-.535	.001
	Q4	-.129	.104	1.000	-.438	.180
	Q5	-.396*	.124	.023	-.763	-.029
	Q6	-.029	.115	1.000	-.369	.311

Q3	Q1	-.250	.104	.256	-.559	.059
	Q2	.267	.090	.053	-.001	.535
	Q4	.138	.092	1.000	-.137	.412
	Q5	-.129	.121	1.000	-.487	.229
	Q6	.238	.116	.629	-.107	.582
Q4	Q1	-.388*	.110	.008	-.715	-.060
	Q2	.129	.104	1.000	-.180	.438
	Q3	-.138	.092	1.000	-.412	.137
	Q5	-.267	.117	.355	-.614	.081
	Q6	.100	.091	1.000	-.169	.369
Q5	Q1	-.121	.124	1.000	-.488	.246
	Q2	.396*	.124	.023	.029	.763
	Q3	.129	.121	1.000	-.229	.487
	Q4	.267	.117	.355	-.081	.614
	Q6	.367*	.113	.021	.031	.702
Q6	Q1	-.488*	.127	.002	-.864	-.111
	Q2	.029	.115	1.000	-.311	.369
	Q3	-.238	.116	.629	-.582	.107
	Q4	-.100	.091	1.000	-.369	.169
	Q5	-.367*	.113	.021	-.702	-.031

Based on estimated marginal means

*. The mean difference is significant at the .05 level.

b. Adjustment for multiple comparisons: Bonferroni.

Q1, Q2, Q3, Q4, Q5, & Q6 refer to questions Q1 – Q6 listed in Table B10.1 (above).

APPENDIX B11

Table B11.1: PERCEIVED DAMAGE (PRD) vs PRIVACY CONCERNS (PRC)

Correlations

		PRD	PRC
PRD	Pearson Correlation	1	.230**
	Sig. (2-tailed)		.001
	N	239	239
PRC	Pearson Correlation	.230**	1
	Sig. (2-tailed)	.001	
	N	239	239

**. Correlation is significant at the 0.01 level (2-tailed).

Table B11.2: PERCEIVED LIKELIHOOD (PRL) vs PRIVACY CONCERNS (PRC)

Correlations

		PRC	PRL
PRC	Pearson Correlation	1	.237**
	Sig. (2-tailed)		.000
	N	239	239
PRL	Pearson Correlation	.237**	1
	Sig. (2-tailed)	.000	
	N	239	239

**. Correlation is significant at the 0.01 level (2-tailed).

Table B11.3: TRUST IN SERVICE PROVIDER (TSP) vs EXPECTED BENEFITS (EXB)

Correlations

		TSP	EXB
TSP	Pearson Correlation	1	.434**
	Sig. (2-tailed)		.000
	N	239	239
EXB	Pearson Correlation	.434**	1
	Sig. (2-tailed)	.000	
	N	239	239

**. Correlation is significant at the 0.01 level (2-tailed).

Table B11.4: TRUST IN SERVICE PROVIDER (TSP) vs SELF-DISCLOSURE (SD)

Correlations

		TSP	SD
TSP	Pearson Correlation	1	.526**
	Sig. (2-tailed)		.000
	N	239	239
SD	Pearson Correlation	.526**	1
	Sig. (2-tailed)	.000	
	N	239	239

**. Correlation is significant at the 0.01 level (2-tailed).

Table B11.5: TRUST IN SNS MEMBERS (TSM) vs EXPECTED BENEFITS (EXB)

Correlations

		EXB	TSM
EXB	Pearson Correlation	1	.337**
	Sig. (2-tailed)		.000
	N	239	239
TSM	Pearson Correlation	.337**	1
	Sig. (2-tailed)	.000	
	N	239	239

**. Correlation is significant at the 0.01 level (2-tailed).

Table B11.6: TRUST IN SNS MEMBERS (TSM) vs SELF-DISCLOSURE (SD)

Correlations

		TSM	SD
TSM	Pearson Correlation	1	.395**
	Sig. (2-tailed)		.000
	N	239	239
SD	Pearson Correlation	.395**	1
	Sig. (2-tailed)	.000	
	N	239	239

**. Correlation is significant at the 0.01 level (2-tailed).

Table B11.7: TRUST IN LEGAL ASSURANCE (TLA) vs AWARENESS (AWR)

Correlations

		TLA	AWR
TLA	Pearson Correlation	1	.489**
	Sig. (2-tailed)		.000
	N	239	239
AWR	Pearson Correlation	.489**	1
	Sig. (2-tailed)	.000	
	N	239	239

**. Correlation is significant at the 0.01 level (2-tailed).

Table B11.8: AWARENESS (AWR) vs TRUST IN SERVICE PROVIDER (TSP)

Correlations

		AWR	TSP
AWR	Pearson Correlation	1	.586**
	Sig. (2-tailed)		.000
	N	239	239
TSP	Pearson Correlation	.586**	1
	Sig. (2-tailed)	.000	
	N	239	239

**. Correlation is significant at the 0.01 level (2-tailed).

Table B11.9: AWARENESS (AWR) vs TRUST IN SNS MEMBERS (TSM)

Correlations

		AWR	TSM
AWR	Pearson Correlation	1	.310**
	Sig. (2-tailed)		.000
	N	239	239
TSM	Pearson Correlation	.310**	1
	Sig. (2-tailed)	.000	
	N	239	239

**. Correlation is significant at the 0.01 level (2-tailed).

Table B11.10: AWARENESS (AWR) vs CONTROL OVER PERSONAL INFORMATION (CPI)

Correlations

		AWR	CPI
AWR	Pearson Correlation	1	.527**
	Sig. (2-tailed)		.000
	N	239	239
CPI	Pearson Correlation	.527**	1
	Sig. (2-tailed)	.000	
	N	239	239

**. Correlation is significant at the 0.01 level (2-tailed).

Table B11.11: CONTROL OVER PERSONAL INFORMATION (CPI) vs TRUST IN SERVICE PROVIDER (TSP)

Correlations

		CPI	TSP
CPI	Pearson Correlation	1	.63**
	Sig. (2-tailed)		.000
	N	239	239
TSP	Pearson Correlation	.63**	1
	Sig. (2-tailed)	.000	
	N	239	239

**. Correlation is significant at the 0.01 level (2-tailed).

Table B11.12: CONTROL OVER PERSONAL INFORMATION (CPI) vs TRUST IN SNS MEMBERS (TSM)

Correlations

		CPI	TSM
CPI	Pearson Correlation	1	.444**
	Sig. (2-tailed)		.000
	N	239	239
TSM	Pearson Correlation	.444**	1
	Sig. (2-tailed)	.000	
	N	239	239

**. Correlation is significant at the 0.01 level (2-tailed).

Table B11.13: EXPECTED BENEFITS (EXB) vs SELF-DISCLOSURE (SD)

Correlations

		EXB	SD
EXB	Pearson Correlation	1	.513**
	Sig. (2-tailed)		.000
	N	239	239
SD	Pearson Correlation	.513**	1
	Sig. (2-tailed)	.000	
	N	239	239

**. Correlation is significant at the 0.01 level (2-tailed).