University of Southern Queensland

Understanding the impact of privacy concerns and trust on social networking sites: Analysing user intentions towards willingness to share digital identities

A Dissertation submitted by
Sanjib Tiwari, MIT, B.Tech (IT)
For the award of
Master of Business Research

2012

Certificate of Dissertation

I certify that the ideas, investigations, analysis, results, discussions, and conclusions reported in this dissertation are entirely my own work, except where otherwise acknowledged. I also certify that the work is original and has not been previously submitted for any other award, except where otherwise acknowledged.

--   Date:…../……/… …

Signature of Candidate – Sanjib Tiwari

Endorsement

--   Date:…../……/… …

Signature of Principal Supervisor – Dr Jianming Yong

--   Date:…../……/… …

Signature of Associate Supervisor – Dr Michael Lane

Abstract

Participation in social networking sites (SNS) has dramatically increased in recent years. SNS focus on building online communities of people who share interests and/or activities, or who are interested in exploring the interests and activities of others. This study examines the experiences of SNS users, and explores how the depth of their experience and knowledge of the Internet, trust and privacy concerns impact upon their individual willingness to share information about their own identity with other users on social networking websites. An acceptance model is proposed that incorporates cognitive, as well as affective, attitudes as primary influencing factors on user attitudes and behaviour which, in turn, are driven by underlying beliefs, perceived levels of privacy and trust, attitudinal experiences and knowledge, as well as a willingness to share.

The proposed conceptual model for this study is derived from the literature review and Theory of Planned Behaviour. This model explains how people experience different levels of motivation about sharing knowledge and seeking information from other members which, in turn, leads to a divergence in both intentions and behaviours within virtual communities. The model shows excellent measurement properties and establishes two distinct constructs—specifically, the need for perceived levels of privacy, and the need for established levels of trust within SNS.

This study is based on quantitative methodology and uses a structural equation model to test the construction of the model and its hypothesis. The data for this study were collected from a Facebook forum, with a sample size of 155 SNS users.

The main theoretical contribution of this study is to provide greater understanding and new insights into privacy concerns and trust, in so far as these factors impact upon SNS users' willingness to readily share information regarding their digital identities. Secondly, this study will enrich the existing literature regarding the inter-relationship between the extent of SNS users' length and depth of experience as Internet users, as this impact upon their willingness to share identity-based information.

List of publications during the MBSR study period

Tiwari, S, & Yong, J 2011, 'Understanding Impact of Privacy Concerns and Trust in Social Networking Sites', paper presented to 5th International Conference on ICT for Development and Education, Kathmandu, Nepal, November 16-17, 2011.

Yong, J, **Tiwari, S**, Xiaodi, H & Qun, J 2011, 'Constructing Robust Digital Identity Infrastructure For Future Networked Society', paper presented to 15th International Conference on Computer Supported Cooperative Work in Design (CSCWD), Lausanne, Switzerland, 8-10 June, 2011.

Acknowledgements

Table of Contents

List of Tables

List of Figures

List of Appendices

List of Acronyms

Acronyms	Description
C.R.	Critical Ratio
CFA	Confirmatory Factor Analysis
CFI	Comparative Fit Index
CR	Construct Reliability
DI	Digital Identities
GFI	Goodness of Fit Index
IFI	Incremental Fit Index
IS	Information System
IT	Information Technology
IUIPC	Internet Users' Information Privacy Concerns
NFI	Normed Fit Index
PC	Privacy Concerns
RMSEA	Root Mean Square Error of Approximation
RSS	Rich Site Summary
SEM	Structural Equation Model
SNS	Social Networking Site
SPSS	Statistical Package for the Social Sciences
T	Trust
TAM	Technology Acceptance Model
TLI	Tucker-Lewis coefficient
TPB	Theory of Planned Behavior
TRA	Theory of Reasoned Action
VE	Variance Extracted

Chapter I: Introduction

1.1 Background to the Study

Since the introduction of Social Networking Sites (SNS), the growth of social networks online has been both rapid and dramatic, changing the purpose and the functionality of the Internet. SNS such as Facebook, Myspace, Linkedin and others are types of online virtual communities that have grown in popularity in recent years (Hu & Ma 2010). Lo and Riemenschneider (2010) argued that the growing popularity of social networking sites has created a new stream of inquiry for academics and practitioners alike, as indicated by the number of papers appearing in proceedings of conferences and workshops relating to online social networks. Increasingly, SNS users have integrated these sites into their daily routines for the purpose of sharing their interests, and communicating with friends and contacts by posting and exchanging information about themselves (Shin 2010a). For example, Facebook alone has over 500 million active users (users who have returned to the site in the last 30 days), with the average user spending more than 55 minutes per day and each having 130 friends on Facebook (Facebook 2011).

Most SNS have the common goal of connecting users and building new relationships using the 'network effect'. To build these network connections, users must be willing to provide information by populating their profile with personal information so that their friends and acquaintances can search for, identify, and reach them, and then interact (Fuchs 2010). According to Thelwall (2009), a user profile is a list of identifying information that can include a person's real name, or a pseudonym. It also can include photographs, birthdays, and the location of their hometown, their

religion, ethnicity, political views and personal interests.

Valenzuela, Park and Kee (2009) argued that sharing authentic and genuine details about a user's real identity in this way encourages users to establish trust in order to develop new relationships. For example, Ellison, Steinfield and Lampe (2007b) found that Facebook users who shared their profiles on SNS had gained more friendship connections in their network.

As online social networking sites are considered personal spaces, their usage is often driven by friendship and relationships, in addition to providing an outlet for creative and personal expression. Many of these sites are classified as private, which suggests to the users that they exercise control over who has access to the information on their site, and gives the illusion of privacy. This study explores whether or not this expectation of privacy over a user's personal space influences how online social network users perceive their willingness to share information.

Lo (2010) argued that privacy concerns pose a problem, since past research has consistently revealed that online users are generally concerned about the privacy of their personal information. Moreover, Dwyer, Hiltz and Passerini (2007) have shown that, in contexts related to information, privacy and trust are two of the most salient beliefs affecting people's intentions to release information. Further, Luo (2002) built a trust-privacy framework which suggests that knowledge plays an important role in determining behaviour in situations in which potential privacy concerns are involved. He also found that users exhibit individual trust regarding SNS themselves and trust beliefs about other SNS users. Lo and Riemenschneider (2010) found that a model

involving trust and privacy concerns would be an appropriate lens through which to examine the phenomenon of personal information disclosure on SNS.

Dinev and Hart (2006) observed that users with Internet literacy have differing perspectives on privacy concerns and trust. Previous research studies found that privacy concerns exist in electronic commerce sites, but only a few studies have focused on how concerns about privacy and trust influence users' willingness to share aspects of their identities within SNS. Thus the main objective of this study is to determine:

To what extent do privacy concerns and trust influence users' willingness to share digital identities (information) on social networking sites?

1.2 Focus and Motivation

Interest among SNS researchers has been wide-ranging, with prior research focused on such topics as social capital (Ellison et al. 2007b), privacy concerns (Gross & Acquisti 2005), trust (Fogel & Nehmad 2009) the differences between users and non-users (Hargittai 2008), and identity management (DiMicco, Millen, Geyer, Dugan, Brownholtz & Muller 2008).

Recent research by Lo (2010) found that many users have major concerns about privacy and trust as they relate to the use of SNS. However, a number of studies found similar concerns about trust and privacy had effected the willingness of some individuals to use electronic commerce, particularly regarding online transactions (Pavlou & Fygenson 2006; Peter 2001; Rosenblum 2007; Xu 2009); but only a few studies have explored the privacy-trust issue in relation to people's willingness to

share personal information within SNS (Fogel et al. 2009; Shin 2010a). Luan, Fung, Nawawi and Hong (2005) found that users with more internet experience and knowledge were more willing to communicate and exchange information online. Fogel and Nehmad (2009) pointed out that users with more experience were positively disposed towards trusting the existing levels of security within SNS sufficiently to enable their participation. Moreover, Shin (2010a) found that once a user trusted SNS, they uploaded their personal data—seemingly without any concern—and shared this information among their friends without limits. DiMicco, Millen, Geyer, Dugan, Brownholtz and Muller (2008) established that users with less Internet knowledge were more likely to place the most trust in SNS sites as they believe that only friends could view the information that they uploaded. Additionally, Kim, Steinfield and Lai (2008) found that users with less Internet knowledge were primarily concerned with using SNS when they did access the internet, and were more likely to share information than were more experienced users. However, they also found that once users are equipped with better knowledge of security and privacy issues, they will be better able to assess the trustworthiness of websites.

Similarly, Lo (2010) determined that users with high levels of SNS literacy were more likely to exhibit concerns about privacy. However, Dwyer, Hiltz and Passerini (2007) argued that, in practice, users often ignored privacy issues as they related to SNS. From the above study it was found that users with substantial SNS experience and knowledge had different attitudes about their willingness to share aspects of their identity with other SNS participants than did users with only limited Internet and SNS experience.

Finally, Lo (2010) suggested, according to the study of Fogel and Nehamad (2009), that the majority of SNS users were university students. Students with the highest levels of computer literacy were more likely to be concerned about privacy, whereas students with less-developed computer literacy were less concerned about privacy. Hence, this study suggested that user SNS knowledge does, in fact, influence concerns about privacy. However, these researchers did not study how the users' experience with SNS influenced their willingness to share information with other users. Hence, this study is important in order to understand the influence of privacy concerns and trust upon SNS users' willingness to share personal information on SNS sites. In practice, it has been found that users are sharing their digital identities in SNS, despite media reporting about breaches in SNS security.

This indicates either that users were unaware of the importance of maintaining privacy in SNS, or that the users were willing to share their digital identities, regardless of privacy concerns. This particular issue motivates the proposed research.

1.3 Statement of Problem

As the use of the Internet increases, and as most people's time schedules become busier, many software companies have developed SNS in order facilitate the sharing of information in a virtual world. This helps people to reach and connect with their friends and family, with whom they might not have the time or opportunity to connect by other means. Most SNS are based upon open platforms within which anyone can join and create a profile. However, in order to use SNS, it is not necessary that everyone has an extensive knowledge of SNS and how they work. Boyd (2008) found that some users frequently updated their daily routines and future

plans in their SNS profile. Fogel and Nehamad (2009) discovered that most university students were intentionally sharing their daily routine in order to impress their colleagues. Also, they found that some users were unknowingly or unintentionally sharing their personal information on SNS sites.

Dwyer, Hiltz and Passerini (2007) found that privacy concerns and trust were major issues for users of SNS. As the world has become more digitised, the protection of the privacy of the user has become more complicated. Nysveen and Pedersen (2004) found that privacy concerns in SNS were similar to those found for users of electronic commerce in terms of concerns by users about providing personal information. Pavlou and Fygenson (2006) found that customers who were using both SNS and online transactions had more privacy concerns regarding online transactions than they did about SNS. Furthermore, they found that despite their concerns about security, users were still willing to share their personal information within SNS. However, they were unable to identify the reasons why users were more willing to share their personal information within SNS.

Previous studies conducted by Lo (2010) concerning privacy concerns in SNS suggest that knowledge and experience may affect the perception of users regarding privacy issues as they relate to the sharing of personal information. But his study did not justify whether users' SNS knowledge and experience play critical role to influence users' privacy concerns and trust to share personal information in SNS.

Dwyer, Hiltz and Passerini (2007) found that trust was another factor that determined users' willingness to share personal information in SNS. Debatin, Lovejoy, Horn and

Hughes (2009) contend that the issue of trust in SNS could be separated into two distinct aspects: trust about SNS itself; and trust of other SNS users. According to Boyd (2011), users with Internet experience might easily trust SNS because they have knowledge of security and privacy settings within the Internet which, in turn, make users feel more secure when using SNS. Furthermore, Binder, Howes and Sutcliffe (2009) also found that frequent users of SNS tend to build trust in the SNS itself, rather than with their friends. However, Lo (2010) found that users had more trust in their SNS friends than SNS themselves because of levels of knowledge and belief in their network of friends.

However, few studies have outlined the important of users' trust on using new systems, and none of the above studies investigated the impact of trust and a willingness to share their personal identity in SNS. Thus, this study focuses on user behaviours and attitudes towards privacy concerns and trust issues, as these factors influence user willingness to share information about users' own digital identities.

1.4 Goal and Research Objectives

Based on the previously-outlined research problem, the main research question of this study is:

To what extent do privacy concerns and trust influence users' willingness to share information about their digital identity within Social Networking Sites?

Therefore, the main research objectives that underpin the general research question of this study are:

❖ To examine the impact of users' experience with SNS upon their willingness to

share their digital identities.

❖ To examine the influences of privacy concerns as they relate to the trust needed for users to share their digital identities within SNS.

❖ To examine the influence of trust of SNS upon users' willingness to share their digital identities.

❖ To examine the impact of privacy concerns upon the willingness of users of SNS to share their digital identities.

1.5 Methodology

Chapter Four provides details of the methodology used in this study and provides justification for its use and implementation. An online questionnaire was used to collect data and a survey link was posted in the SNS forum. The instrument was adopted from previous study, so validity and reliability for this study purpose are assured. The exploratory and confirmatory factor analyses using SPSS 19.0, Structural Equation Modeling using AMOS 19.0 was performed to examine the goodness-of-fit indices of the various measurement and structural models.

1.6 Outline of Report

This thesis consists of six chapters. The first chapter (Introduction) provides background to the research, and briefly outlines the gaps in the research that this study seeks to explore. It introduces the research question and the research objectives and outlines the methodology chosen to explore the research question.

Chapter Two (Literature review) reviews the literature in the areas of SNS, digital identity, privacy concerns and trust. This study also explores the background, history

and development of SNS. Finally, this study investigates the demographic data that users are willing to share in SNS.

Chapter Three (Theoretical support and conceptual model) lays out the research framework for this study. This chapter reviews the relative theories used in information systems that relate to this study. Emerging from the literature review and theoretical support, a research conceptual model is presented and four hypotheses identified for further research.

Chapter Four (Research design and methodology) provides an outline and justification behind the methodology and collection of data for this study. It presents the methods, a description of the sample and an outline of the research process.

Chapter Five (Results and analysis) summarises and presents the findings of the study, using four hypotheses as the organising structure for analysis, and the key findings are identified and summarised.

Chapter Six (Findings, recommendations and conclusion) discusses the key findings from the data and provides conclusions to the study. The motivations behind social networking users are discussed and outlined, the perceptions of SNS are detailed, and issues such as users and their perceptions relating to trust and privacy in SNS are outlined. Users' willingness to share information regarding their identity within SNS is discussed and a new model is presented. The findings of this study reveal that the willingness by users of SNS to share their digital identities is determined by their individual perceptions about of privacy and trust within SNS. This chapter also

discusses the implications of theory and practice that arise from the results of this study. The limitations of this study are also addressed, and recommendations are made for areas of future research.

1.7 Conclusion

This chapter outlines the background to the research question by introducing social networking sites and describing their rapid growth in the Internet market place. Owing to the relative newness of social networking, there is little published research on the topic of privacy concerns and trust as they relate to user intentions and actions. Hence, this research breaks important new ground by exploring exactly how users' willingness to share digital identities is impacted upon by their own issues of privacy and trust as they relate to the use of SNS. The research problem that guides this study and its research is presented, and an overview of the study methodology is described. The outline of the report is detailed and the limitations of the study acknowledged. A review of the literature begins in Chapter Two.

Chapter II: Literature Review

2.1 Introduction

This section contains a review of the existing literature that is related to this project, beginning with a description of the concept of Web 2.0, and provides a background about Social Networking Sites beginning with the very first Social Networking Site, sixDegrees (www.sixdegree.com), up to the creation of the most popular current SNS, namely, Facebook. The focus of the literature review was to understand SNS, its usage, and to explain the public's increased participation in SNS and the impact of privacy and trust upon users' participation in social online networks. The literature review also shows how users can create their public profiles and share their digital identities with other users.

Gradually-increasing numbers of Internet users and social networking sites has created the issue of privacy concerns and trust. So the main objective of this research is to review users' privacy concerns and trust that effect users' willingness to share digital identities on SNS.

2.2 Social Networking Sites

2.2.1 Web 2.0 and Social Networking

The creation of Web 2.0 has facilitated an entirely new type of communication that became increasingly important to society. Web 2.0 is the popular term for advanced internet and applications and includes blogs, Wiki, RSS, and Social Networking Sites (Lai & Turban 2008). According to Anderson (2007) and Madden and Fox (2006), the concept of Web 2.0 was created by Dale Dougherty and O'Reilly Media Inc in 2004, and the term has become more popular and its use continued following 'dot

com' in recent years. Sir Tim Berner-Lee, the creator of the World Wide Web, criticised the term Web 2.0 as he believed it was nothing more than a fully-implemented version of the original Web. To support his view, he reportedly argued that Web 2.0 was based on Web 1.0 standards, and the purpose of both Web 1.0 and Web 2.0 was to create connections between people (Paul et al. 2007). However, Trembath (2011) argues that what differentiates Web 2.0 from more traditional IT, including the Web, is not just one attribute but, rather, a set of characteristics that together give shape to this new class of technologies, and at the same time provides the field of IT research and practise with some interesting challenges.

In practice, it is generally accepted that many standards that underpin Web 2.0 have been derived from the traditional Web, and that Web 2.0 has a much more social orientation than Web 1.0. Lai and Turban (2008), for instance, argued that the combination of user-generated content, its collaborative nature and the significant emphasis on Social Networking Sites make Web 2.0 more advanced than the traditional Web. Rather than being defined with reference to a list of specific applications and services, Web 2.0 is usually described as embodying a set of principles and practices. The associated applications and services usually have defining characteristics that enable users to create online content, access collective intelligence and access network-enabled interactive services (Madden et al. 2006). At the core of Web 2.0 is a sense of participation and 'collaborations, contributions and communities' (Paul et al. 2007, p. 14) and there are a range of websites (e.g. Wikipedia, YouTube and Blogger) that support Web 2.0 activities such as collaboration, media sharing and blogging. The focus of this study, however, is on

social networks.

The most popular types of Web 2.0 applications that have developed in recent years are online Social Networking Sites (SNS) or virtual communities, in which membership continues to grow exponentially (Lai et al. 2008). SNS such as Facebook, MySpace, Twitter, LinkedIn, Google Plus, Hi5, and Friendster are new forms of self-representation and communication, and imply a social behaviour that is different to the real world (Bonhard & Sasse 2006). Since their introduction, these SNS have not only attracted millions of users, but have become an essential part of the users' everyday activities—a parallel universe that, in the virtual world, satisfies the human need for sociability (Ganley & Lampe 2009). Social networking sites generate billions of dollars in revenue and are being increasingly used in marketing and advertising campaigns. However, very little research has been carried out to investigate the factors that influence the usage of SNS, as suggested by Gangadharbatla (2010).

The Pew Internet Project defined online social networks as 'spaces on the Internet where users can create a profile and connect that profile to others (individuals or entities) to create a personal network' (Lenhart 2009, p. 1). Social networking sites enable individuals to connect with their friends and colleagues, as well as to form new associations through participation in online groups. Yahoo! Groups (Yahoo 2011), for instance, is promoted as a place 'where people get to know each other and stay informed'. Alternatively, Facebook (2012) declares that it is their mission to 'give people the power to share and make the world more open and connected'. Group members typically have online access to group features such as forum

postings, photo albums, shared links and group birthday calendars, as well as individual features such as personal profiles. Plant (2004) argued that memberships of online communities satisfied two basic human needs: the need to be connected to others; and the need to acquire knowledge. Supporting this argument, a recently-completed study by Fox and Purcell (2010) found that individuals seeking health information benefited significantly from tapping into the pool of user-generated information and the emotional support provided within online social networks (Fox & Purcell 2010).

The amount and scope of information that SNS users freely reveal is stunning and constitutes a highly attractive database and profiling source for different interest groups, ranging from marketers to recruiters, private detectives, public authorities, and hackers. Information technology experts characterise Web 2.0 social networks as 'attractive targets for those with malicious intent', because each site offers a huge user base, sharing a common infrastructure, and the information that users willingly supply is highly valuable (Mansfield-Devine 2008). The average user's profile contains information about their home address, their pet's name, where they went to school, their mother's maiden name, their likes and/or dislikes, interests, hobbies and other family details just the kind of information used for security or 'lost password' questions that are required routinely, for example, by online banking services. Many participants also provided detailed information about their interests, sometimes including their political and sexual orientations or intimate portraits of their social or inner lives (Gross et al. 2005). Every now and then, problems related to privacy, trust or security issues on social network sites are reported in the media. For instance, in May 2008 the social networking website Bebo admitted that a 'bug' in its systems

enabled users to view other people's private information. Phone numbers and addresses were made available as some of Bebo's 40 million users found themselves randomly switched to other people's accounts (Eriksen 2008). Evidence from many other online social networks indicate that despite these reported breaches of security in the past, nevertheless, millions of social network users do not hesitate to share their thoughts, experiences, images, files, videos, and links in an environment that is largely devoid of security standards and practices.

It has also been argued that social networking sites are well-suited to meet information and connection needs because they foster the development of sparse, unbounded networks that encourage the formation of weak ties (Wellman 1997). 'Sparseness' refers to the number of contacts that members have with each other, while 'boundedness' refers to the percentage of members' ties that stay within the boundaries of the network. 'Tie strength' describes frequency of contact, social closeness, reciprocity and the degree of voluntary involvement (Granovetter 1973; Wellman 1997). Weak ties typically help individuals reach out to various information sources and resources, and are more likely to exist between acquaintances. Within this context, the social aspects of online networking are becoming increasingly important (Paul et al. 2007). Strong ties, on the other hand, typically provide companionship and emotional support, and are most likely to exist between family and close friends. They are founded on considerable trust and support. While it is generally accepted that it is the more traditional communities, such as those described by Tonnies (1887) and Durkheim (1893), that typically foster the development of strong ties, a recent study conducted by the Pew Research Centre in 2009 found that a high percentage of people surveyed (85%) used online social

networking applications to interact with people whom they already knew offline (Lenhart 2009). On that basis, it could be argued that strong ties, as well as weak ties, can be maintained online. Lai and Turban (2008) argued that online social networking sites have experienced a significant increase in popularity since the emergence of Web 2.0 applications and services. Moreover, the Pew Research Centre reported that the number of American adult internet users who had reported using a social networking site had quadrupled within the preceding four years, from 2005 (8%) to 2008 (35%), and had almost doubled from 2008 to 2011 (65%) (Lenhart 2009).

Disclosing personal information on the Internet presupposes trust, because the user does not know whether their personal information may be used in ways that the user is not able to foresee, and as a result may cause potential harm to the user, or lead to unwanted future solicitations or hijacking of one's online identity for personal use (Milne & Culnan 2004). Obviously, social networking takes place within a (largely unwarranted) context of trust. Consequently, the question arises why social network users are being so trusting, despite their concerns about privacy. Scant research has considered the interrelationships between privacy concerns, trust, social networks, and the Web 2.0 environment. In this study, analysis is conducted on the role that privacy concerns and issues of trust play vis-a-vis SNS from an Internet network governance perspective that integrates concepts of behavior intention theories such as the Theory of Planned Behavior.

2.2.2 Background of Social Networking Sites

Online social networks are a fast-growing phenomenon and are emerging as the Web's top application (Chiu, Cheung & Lee 2008). SNS have become a computer-

mediated communication medium in the Internet world (Ahn, Han, Kwak, Moon & Jeong 2007). At the most basic level, SNS are online communities based on a social-circle network model, in which people build their own profile and create a network of connections with other participants. Boyd and Ellison (2008, p. 211) defined SNS as web-based services that allow individuals to construct a public or semi-public profile within a bounded system, to articulate a list of other users with whom they share a connection, and then to view and traverse their list of connections and those made by others within the system. The visibility of a user's profile on different SNS determines to what extent SNS users can view other users' profiles and, normally, a SNS like Facebook has default settings, although these can be configured by individual users (Hoy & Milne 2010; Staksrud & Lobe 2010).

At the time of writing, there are hundreds of SNS offering different types of services to individuals and groups with shared interests. These SNS display great diversity in user bases across genders, age groups and specific geographical regions. The first wide-scale online social network 'sixdegrees.com' was created by Andrew Weinreich in 1997 (Albrechtslund 2008; Boyd et al. 2008; Livingstone 2008) and was closed in 2000 due to decreased popularity, although the site had features of profiles, friend circles and messaging (Boyd et al. 2008; Harrison & Thomas 2009; Shafie, Mansor, Osman, Nayan & Maesin 2011). It worked in such a way that a person who registered at the site could list up to ten friends only. Those friends were supposed to join and list ten friends each of their own, and so on. The site was used for apartment searches, job hunts, searches for medical specialists or lawyers, and even finding old high school colleagues (Boyd et al. 2008; Buote, Wood & Pratt 2009).

Boyd and Ellison (2008) present the history of SNS since 1997 when 'SixDegrees.com' was launched. They document the timeline up to late 2006, detailing the release dates of some of the major SNS, including online communities such as LunarStorm, AsianAvenue and QQ that have been re-invented and re-launched with SNS features (see Figure 2.1). Among the SNS found in the list, Facebook, MySpace, LinkedIn, Hi5, and Friendster are the most notable and well-known sites (Boyd et al. 2008). Also, taking a closer look at these SNS, it is not surprising that many of them resemble each other in their design and layout, as well as similarities in the features offered to users.

In 1999, LiveJournal integrated extra features such as guest books and diary pages (Harrison et al. 2009; Shafie et al. 2011); and in 2003, Linkedin was officially launched (LinkedIn 2011). By way of comparison, a relatively small Social Networking Site, My Connected Community (mc² 2011), had 17,049 registered members in 2002 and 81,851 registered members in 2010. However, Social Network Sites began to be popular with the general public with Friendster, MySpace and Facebook (Shafie et al. 2011). Alternatively, Facebook and MySpace are the two largest SNS in use today, as measured by the total number of registered users in 2010 and 2011 (Boyd 2011; Shin 2010b). In 2004, *The Times* newspaper predicted that Facebook would reach 55 million citizens in the near future. Now, Facebook has over 500 million active users, and approximately half of them log on to their Facebook account every day (Facebook 2011). On the other side, MySpace has over 100 million monthly active users worldwide and more than 68 million totally unique users in the USA (MySpace 2011). Other popular social networking sites in 2011 include Twitter, Flixster, Linkedin, and Orkut (Boyd 2011). According to Wu,

DiMicco and Millen (2010), there are a number of SNS created by individual organisations only for the use of their staff. Even though the number of members may vary, most Social Networking Sites have comparable features. Yahoo! (Yahoo 2011) and My Connected Community (mc² 2011), for instance, provide access to forums, photo albums, group event calendars, shared links and member polls. They also allow members to customise their profile pages.

Launch Dates of Major Social Network Sites

'97 — Six Degrees.com

'98

LiveJournal
AsianAvenue — '99
BlackPlanet

LunarStorm (SNS relaunch) —

'00
MiGente

(SixDegrees closes) —

'01 — Cyworld
Ryze —

Fotolog — '02
Friendster

Skyblog —

Couchsurfing
LinkedIn — '03 — MySpace
Tribe.net, Open BC/Xing — Last.FM
Orkut, Dogster — Hi5
Multiply, aSmallWorld — Flickr, Piczo, Mixi, Facebook (Harvard-only)
'04 Dodgeball, Care2 (SNS relaunch)
Catster —
Hyves

Yahoo! 360 — YouTube, Xanga (SNS relaunch)
Cyworld (China) — '05 Bebo (SNS relaunch)
Facebook (high school networks)
Ning — AsianAvenue, BlackPlanet (relaunch)

QQ (relaunch) — Facebook (corporate networks)
Windows Live Spaces — '06 Cyworld (U.S.)
Twitter — MyChurch, Facebook (everyone)

Figure 2. 1 Timeline of the many major SNS

(Source: Boyd and Ellison (2008))

20

2.2.3 Defining Social Networking Sites

Broadly, a social network can be defined as a set of actors and a set of ties representing some relationship, or lack of relationship, between the actors (Brass, Butterfield & Skaggs 1998). Actors in a social network (people, organisations, or other social entities) are connected by a set of relationships, such as friendship, affiliation, financial exchanges, trading relations, or information exchange. SNS uses computer support as the basis of communication between its members (Andrews, Preece & Turoff 2001; Andrews 2002). SNS are organised around users, and provide a basis for maintaining social relationships, for finding users with similar interests, and for locating content and knowledge that has been contributed or endorsed by other users (Mislove, Marcon, Gummadi, Druschel & Bhattacharjee 2007).

Web-based social networks provide different means for users to communicate, such as e-mail, instant messaging services, blogging, and photo/video-sharing. Since 1999, hundreds of online social networks have been launched, with similar technological features that support a wide range of interests and practices (Ellison & Boyd 2007a).

Social network sites provide different sets of services, and can be oriented around work or business related contexts (e.g., XING), romantic relationship initiations (the original goal of Friendster), or they could aim at connecting those with shared interests such as music (e.g., MySpace) or the college student population (e.g., StudiVZ, or the original launch of Facebook). On the other hand, LinkedIn provides a service that helps users exchange information and opportunities with broader networks of professionals. Most online social networks support the maintenance of

already-existing social ties, but there are also networking services that support the formation of new connections with strangers, based on shared interests, political views, or activities. Some online social networks are directed at diverse audiences, whereas others attract people based on common interests or shared racial, sexual, religious, or nationality-based identities (Boyd et al. 2008).

Drawing on Boyd and Ellison (2008) for the purposes of this study, online social networks are defined as web-based services that allow individuals to (1) create a public or semi-public profile for themselves within a bounded system, (2) indicate a list of other users with whom they are connected, and (3) view and traverse their list of connections and those made by other users within the system. The types and specific names of these connections may vary from network to network. However, for this study, SNS means any Social Networking Site that allows any public user to create their profile and share information. With the exponential growth of social networking, one may expect that users' experience on SNS is increasing.

2.2.4 SNS Knowledge and Experience

DiMicco, Millen, Geyer, Dugan, Brownholtz and Muller (2008) advocated that SNS Knowledge is a part of Internet knowledge or experience. Novaka, Hoffman and Yung (2000) argued that Internet experience is usually defined as general experience with web sites, and not as experience with one particular web site. Additionally, Chang and Chen (2008) found that by visiting several web sites and using various value-added services, users will increase their knowledge in general Internet experience. The length of internet experiences or knowledge for a user may play a critical role in their evaluation of their SNS experience, as suggested by Binder,

Howes and Sutcliffe (2009). Moreover, Gefen, Karahanna and Straub (2003) and Dahlen (2002) found that through repeated usage of a product or performance of a task, people became more experienced and gained knowledge. Therefore, for the user, the more experience of using the Internet they have, the greater is their ability to build more knowledge about the Internet.

Dinev and Hart (2006) suggested that an internet experience is similar to a SNS experience, which is measured in length of SNS usage and frequency of visits. A user's degree of Internet experience has some bearing upon how quickly the user might learn to navigate in an unfamiliar information space. Years of online experience have proven to be a significant predictor for users in relation to their adoption and effective use of online commerce in all forms and sharing information (Flicker 2004). Therefore, the more familiar a user is with the SNS website, the more likely it is that they will use the different applications available on a SNS web site, seemingly without any concerns.

A prior experience has been found to be an important determinant of behaviour (Ajzen & Fishbein 1980). According to Taylor and Todd (1995a) there are some significant differences in the relative influences of the determinants of usage depending on experience. However, there was a stronger link between behavioural intention and behaviour for the experienced users explained by Ajzen and Fishbein (1980). Moreover Ajzen and Fishbein (1980) found that experienced users employed the knowledge gained from their prior experience in order to inform their intentions (Ajzen et al. 1980). In addition, Eagly and Chaiken (1993) suggested that knowledge gained from past experiences would help to shape users' intention, in part because

experience makes knowledge more accessible in memory.

Novaka, Hoffman and Yung (2000) identified that experience with the Internet is among the most important factors that predict online shopping behaviour. Furthermore, Luan, Fung, Nawawi and Hong (2005) found that users with more experience and knowledge in using the Internet were more willing to experiment with online shopping. Their empirical findings reveal that regular visitors to the Internet were more knowledgeable and experienced and likely to perceive an absence of certainty in online relationships. They also found that this increased level of trust is positively related to the user's Internet knowledge and experience. Hence, this may imply that users with high levels of experience and knowledge in using the Internet and SNS are more willing to use SNS to share information about their digital identities.

2.3 Internet Privacy

Bandeis and Warren (1890) defined privacy in general terms as the right to be left alone. This definition has been the basis of the privacy debate that has taken place in industrialised nations since the beginning of the information era. Privacy in terms of the Internet is defined as personal information that an individual deems important and unattainable either by the general population or government surveillance or by any intrusion (Hodge 2006; Richards 2006; Timm & Duven 2008).

Lo (2010) argued that privacy has been considered to be the greatest issue facing Internet users today. A major reason people cite for not using the Internet is a fear about privacy and security (Metzger & Docter 2003; Paine, Reips, Stieger, Joinson & Buchanan 2007; Ramgovind, Eloff & Smith 2010). According to Lach's (1999)

survey, most of the online they studied thought that there should be laws to protect online privacy in Internet.

According to Hodge (2006), when contemplating issues of privacy there are two important things to keep in mind: the intent of the information shared and the expectation that it will remain private. A person who willingly posts or shares information on SNS for others to view cannot assume it is private, because the intent is to share that particular information (Meredith 2006). On the other hand, Hodge (2006) argued that when a user adjusts their privacy settings to prevent most users from viewing his or her information, the user has an expectation that this information will remain private.

Most Internet sites provide privacy statements, or terms and conditions that apply to users of the sites: for example both Facebook and MySpace provide a clear privacy statement and terms and conditions to inform users about the limits of protection that the site maintains for the information shared, as well as how the site will use the personal information provided. These privacy policies do not delineate who can access the information posted on the site, but outline the actions that are taken by the site's administrators. The focus of these privacy statements is to outline what information will be shared with a third party, but does not address the issue of who else might access the information that is posted therein. Little is known about whether individual users read or are aware of privacy settings. However, when Facebook created its news feed feature, users were outraged that 'friends' would be informed of their actions on the site. Facebook states that it will do everything possible to protect the information posted on the site but its creators 'cannot and do

not guarantee that User Content you post on the Site will not be viewed by unauthorised persons' (Facebook 2011). In addition to privacy policies that outline how Web sites will protect personal information provided to the company, the sites also outline who is responsible for the information posted in a profile. Facebook (2011) states, 'You may not want everyone in the world to have the information you share on Facebook; that is why we give you control of your information'. Both MySpace and Facebook provide advice to parents and users about how to keep the information shared in the profile protected. MySpace cautions users: 'Don't forget that your profile and MySpace forums are public spaces' (MySpace 2011).

According to Timm and Duven (2008), Chris Hughes, a co-founder of Facebook, stated that Facebook has provided ways for users to continue to connect online and that it is up to the user to protect his or her own information by using the tools provided on the site. The tools provided to social networking site users include a set of privacy controls that users can adjust to prevent others from viewing all information shared in a profile. On most sites, the default or automatic settings allow the profile to be seen by the maximum number of people. On Facebook, the default setting for a profile is set so that all members of the person's network can view the entire profile. On MySpace, the default setting for a profile is that all users on MySpace can view a user's profile (Timm et al. 2008). The privacy options that are available for users for other sites vary. On most sites, a user can restrict who can see their profile, and is given options to create a limited profile that makes parts of his or her information unavailable to all friends. Although these options are available, many users do not use these privacy settings (Barnes 2006).

2.3.1 Privacy Concerns

Dinev and Hart (2006) argued that an individual's Internet privacy concerns reflects his or her uneasiness about the potential opportunistic behaviour related to his or her personal information submitted over the Internet. Moreover, Dwyer, Hiltz and Widmeyer (2008) argued that privacy within social networking sites is often not expected or remains undefined. Additionally, Nooteboom (2007) and Son and Kim (2008) suggest that opportunistic behaviours may include a range of actions taken by others who use or misuse an individual's personal information, for example, identity theft, social engineering to extract one's financial information, and spam. Hence, users with SNS knowledge sometimes worry about the risks associated with sharing identity information on SNS.

Culnan and Bies (2003) and Xu (2009) argue that the privacy of information varies according to numerous factors, including industry sectors, culture and regulatory laws. Privacy concerns about information refer to an individual's subjective views of fairness within the context of information privacy (Davison, Clarke, Jeff, Langford & Kuo 2003; Malhotra, Kim & Agarwal 2004; Zarsky 2004).

Malhotra, Kim and Agarwal (2004) developed an Internet Users' Information Privacy Concerns (IUIPC) model to examine Internet privacy concerns. They conceptualised IUIPC as the degree to which an Internet user is concerned about collection by online marketers (vendors) of personal information; the users' control over the collected information; and the users' awareness of how the collected information is used.

With the proliferation of the Internet, Lo and Riemenschneider (2010) believe an important factor that contributes to shaping the individual's Internet privacy concerns is his or her level of Internet literacy. Further, Luan et al. (2005) argue that users with high levels of knowledge and experience with the Internet are more willing to become online shoppers and to place their trust in the sites. However, Hoffman, Novak and Peralta (1999) and George (2002) found that privacy concerns lead to a decreased likelihood of online purchases, and that the belief in the privacy of personal information was associated with negative attitudes towards internet purchasing.

Lo and Riemenschneider (2010) argued that the precise dynamics of how an individual's extent of Internet literacy influences his or her Internet privacy concerns was not straightforward. On the one hand, Bateman, Pike and Butler (2011) found that lower degrees of Internet literacy may elevate concerns about privacy, because although the individual may be vaguely aware of potential dangers, he or she may not know how to manage them. On the other hand, higher degrees of Internet literacy (Sheehan 2002) and increases in education levels (O'Neil 2001) can likewise raise concerns about privacy, because the individual is more aware of the dangers. However, Zhang and Tatipamula (2011) suggested that a more literate individual may have the knowledge to attempt to minimise the dangers by installing and updating operating system and browser security patches and fixes, anti-spyware software and alerts, and other prevention utilities.

Due to this perception of control (i.e. the ability to try to minimise potential dangers), individuals with higher levels of Internet literacy were expected to be less concerned

about their Internet privacy than individuals with lower Internet literacy. However, in a study of the behavioural intention to conduct online e-commerce transactions, Dinev and Hart (2006) found that Internet literacy was negatively related to Internet privacy concerns.

Khosrow-Pour (2007) suggested that willingness to provide personal information varied depending on the level of privacy offered by policy statements, and that respondents were most willing to provide information when given strong privacy statements by a SNS. Moreover, the Theory of Planned Behaviour, which is derived from the Theory of Reason Action, suggests that beliefs related to behaviour are prevailing determinants of a person's behavioural intentions (Ajzen 1991). As such, in the context of SNS, a person's beliefs about Internet privacy should also be a determinant of his or her intention to share personal information on a SNS.

However, in general, most consumers who participated in the e-commerce context were concerned about their online privacy. Findings from a recent study by the USC Center for the Digital Future indicate that 93% of online shoppers were concerned about the privacy of their personal information (USC 2011). Meinert, Peterson, Criswell and Crossland (2006a) suggested that this concern was among the chief factors discouraging users from shopping online. In line with this reasoning, Dinev and Hart (2006) found a negative relationship between Internet privacy concern and the user's general willingness to provide personal information in order to conduct transactions on the Internet. In the context of SNS, the relationship between Internet privacy concerns and users' willingness to submit personal information should be similar to those extant in the e-commerce context. That is, higher privacy concerns

should lead to a reduced willingness to submit personal information to a SNS, as well as a reluctance to share this information with other SNS users (i.e. friends and everyone). Hence, higher levels of privacy concerns will result in SNS users having less positively disposed intentions to share digital identities and trust.

2.4 Trust

Trust has become more important in a high tech environment (Fukuyama 1996). In the absence of trust, Web sites will most likely exist in an environment devoid of loyalty. Trust is also important for successful online interactions (Corritore, Kracher & Wiedenbeck 2003; Liu, Marchewka, Lu & Yu 2005). Mayer, Schoorman and Davis (2007, p. 712) define trust to mean that one believes in, and is willing to depend on, another party. Further, Liu, Marchewka, Lu and Yu (2005) define trust as a perceptual belief or level of confidence that someone respects the intentions, action and integrity of another party during an online transaction.

Lo and Riemenschneider (2010) suggested that trust for SNS can be compared with the observed purchasing behaviour of internet users. Hoffman, Novak and Peralta (1999) implied that the primary reason many people have yet to shop online or to provide personal information to a vendor is due to a fundamental lack of trust with online transactions that require the customer to provide credit card and personal information. However, Pavlou (2003) argued that trust creates positive feelings for users who partake of online transactions with web retailers, providing expectations for a satisfactory transaction and thus resulting in a positive attitude towards the transaction. Therefore, these studies suggest that users with Internet experience and trust are more willing to regard the sharing of their digital identity on SNS in a

positive light.

Liu et al. (2005) proposed a theoretical model that explains how trust influences consumer behavioural intentions vis-à-vis online transactions. They found strong support for the positive relationship between the levels or degrees of trust an individual has with an online business, and the individual's own behavioural intentions. Additionally, Gefen, Karahanna and Straub (2003) suggest that the higher the customers' trust in the web, the less effort customers will exert to scrutinise the details of the site to assess the authenticity of its services. Research in the field of electronic commerce has found that trust is strongly related to information disclosure and was reported as a significant precursor to the disclosure of information online (Hoffman et al. 1999; Metzger 2004).

Metzger (2004) found that sharing information on SNS with trust was a precondition for self-disclosure, because it reduced perceived risks involved in revealing personal identities. Malhotra, Kim and Agarwal (2004), in their IUIPC model, show that trusting beliefs have a positive effect on users' intention to willingly share personal information on SNS.

Mayer, Davis and Schoorman (1995, p. 474) define trust to mean a state in which 'one believes in, and is willing to depend on, another party'. According to McKnight, Cummings and Chervany (1998) two components of trust are *beliefs* (i.e. trust beliefs) and *willingness* (i.e. trust intentions). Trust beliefs, or 'factors of perceived trustworthiness' as Mayer et al. (1995) referred to them, are antecedents to trust intentions according to McKnight et al. (1998) and are comprised of three factors:

competence, benevolence, and integrity (Mayer et al. 1995; McKnight, Choudhury & Kacmar 2003). Specifically, competence refers to the ability of the trustee to perform the behaviours in the relevant domain expected by the truster. Benevolence refers to the extent to which the truster believes the trustee cares about and is motivated to act on behalf of the truster, rather than for the self-gain of the trustee. Finally, integrity refers to the extent to which the truster believes the trustee is honest and consistently keeps their promises.

Ajzen and Fishbein (1977), after a review of previous empirical studies about attitude-behaviour relations, concluded that stronger relationships exist between attitudes and behaviours when the attitudinal and behavioural entities have high correspondence. To support this statement, McKnight el al.(1998) explained that a person may have favourable attitudes toward football games, but unfavourable attitudes toward *attending* football games. Thus, measuring general attitudes toward football games should produce a weak relationship to attendance (the behaviour); however, measuring the person's attitude toward attending football games should generate a strong relationship with actual attendance. Moreover, Mayer el al. (2007) suggested that beliefs about an entity should also relate more highly with intention to behave toward that entity (in this study, with willingness to share identity information) when the belief and intention entities measured have higher correspondence.

Finally, Metzer (2004) and Liu et al. (2005) studied privacy, trust and disclosure in exploring barriers to electronic commerce and found that trust has a positive effect on users' intentions towards willingness to share information; however, these studies

did not mention how trust can influence user knowledge and their disposition towards sharing identity. Therefore, this study concludes that trusting beliefs have a positive effect on users' willingness to share personal information in SNS.

2.5 Digital Identities
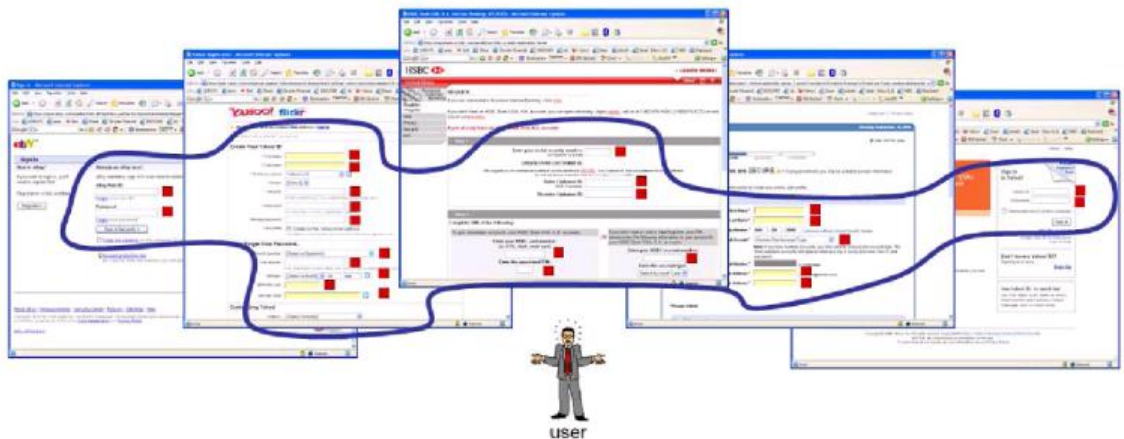
Figure 2. 2 Digital Identity: Global Set of Attributes of a User

(Source: Ahn, Ko and Shehab (2008))

There are various definitions of digital identity. The concept of digital identity varies depending upon its context of use. The term 'Digital Identity' used here describes a person's presence within the Internet as present in various applications, or, in other words, digital identity is a global set of attributes that make up an online representation of who and what a user is (Williams, Fleming, Lundqvist & Parslow 2010). It can include access credentials, personal attributes and references. An individual's Digital Identity, as perceived by other people, is made up of material that the individual manually posts (for example, photographs on Flickr and on one's own web page), but it also is made up of material other people publish to the Internet about individuals, such as blog posts that mention an individual, and photographs in which individuals are tagged (Williams et al. 2010). Over the Internet, a user has numerous access credentials that are issued from different sites; and different or duplicated personal attributes and references on each site. Identity is an elusive

concept: there is no single clear definition. The collective mass of all of the personal attributes when considered in totality can be judged to mean the users' digital identity as shown in Figure 2.2. In each site where users need to employ some authentication protocols in order to be active, a user can be represented by a subset of these attributes. For example, on an auction site such as eBay, a subset of a user's attributes such as username, password, purchase history and credit details represent the user's identity on this site, while for a university or college site, a user's identity may consist of their student ID number, password, class record and Grade Point Average or GPA (Ahn, Ko & Shehab 2008).

Identity is an important part of the formation of a self-concept. Self-concept is the totality of a person's thoughts and feelings in reference to oneself as an object (Gecas 1986; Zhao 2005; Zhao, Grasmuck & Martin 2008), and identity is that part of the self 'by which we are known to others' (Altheide 2000, p. 2). The construction of an identity is therefore a public process that involves both the 'identity announcement' made by the individual claiming an identity, and the 'identity placement' made by others who endorse the claimed identity, and an identity is established when there is a 'coincidence of placements and announcements' (Stone 2005). This definition indicates that the identity of a person is comprised of a set of attributes or properties, perceived both internally and verified externally, that together make the person unique (Ellison et al. 2007a).

Digital identity follows this same notion, however, within the context of the Social Web, the identity of users is bespoke and can be altered by the individual users (Kamel Boulos & Wheeler 2007; Rowe 2010). Such alterations are possible through

functionalities and feature sets on Social Web platforms such as profile pages (Robards 2010). On such pages users are able to create an identity profile consisting of their biographical information, which is an Identity for that user (Rowe 2010). Therefore, in this study, digital identity refers to personal information that makes users identifiable in SNS with their actual personas that exist in the real world.

Information relating to digital identity can be divided into three tiers (Weik & Wahle 2010; Windley 2005) as shown in Figure 2.3. The first tier is called 'my identity', which contains persistent identity information such as a person's name, date of birth and genealogical relations—information that is constant and unlikely to change (Rowe 2010; Weik et al. 2010).
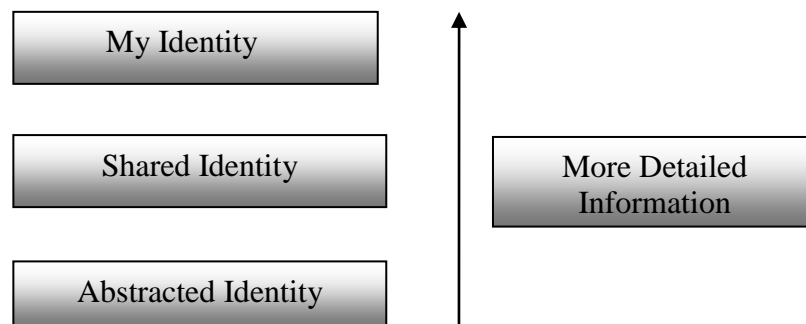
Figure 2. 3 Three tiers of digital identity

(Source: Rowe (2010))

The second tier is called 'shared identity', which contains attributes assigned to an individual by other people, such as the social network of a person. Shared identity contains information which is susceptible to change as a person makes friends with different people and loses contact with others (Rowe 2010; Weik et al. 2010).

The third tier is called 'abstracted identity' and contains identity information derived

from groupings and demographics. For example, identifying a person by a community of practice that they are involved in SNS. Identity information within this tier is very likely to alter as a person's interests evolve over time. As Figure 2.3 illustrates, when users move up the tiers, the information describing the digital identity of an individual becomes increasingly detailed and, therefore, deterministic in the sense of uniquely identifying the person (Rowe 2010; Weik et al. 2010). Thus, creating identities and sharing this personal information on SNS raises privacy concerns for users of SNS.

2.5.1 Willingness to Share Digital Identity

Human behaviours differ across individuals, as each one will possess differentiated intentions and interests as represented by their willingness to create and share personal identity that is true or authentic, rather than that which is fictitious. Behavioural intention is defined as 'the degree to which person has formulated a conscious plan to perform or not perform some specified future behaviour' (Warshaw & Davis 1985).

Our understanding of user behaviour is normally derived from studies within marketing disciplines, but many studies that can be readily applied to online SNS have also been conducted in relation to e-commerce. Some theories which are used to study the effect of behaviour intentions by users upon their interactions within SNS include the Theory of Reason Action (George 2002; Lo et al. 2010; Malhotra et al. 2004; Shin 2010a), the Theory of Planned Behaviour (Ellison et al. 2007b; Lo 2010), Technology Acceptance Model, and Social Contract Theory (Fogel et al. 2009).

According to Bateman, Pike and Butler (2011), user behaviour is affected by

emotional responses that rely on external surroundings and internal individual characteristics. In SNS, environmental characteristics involve creating groups, communities, entertainment, sharing applications and research interests (Park, Kee & Valenzuela 2009). Mori, Sugiyama and Matsuo (2005) suggest that individual characteristics involve making friends, developing new relationships, and updating personal identity and information. Moreover, DiMicco et al. (2008) suggested that users with a high profile have more friends. However, Ybarra and Mitchell (2008) argue that users who share more of their identity information may have different intentions, for example, they may want to impress their co-workers, colleagues and friends. Hence, they suggested that users have different intentions in terms of willingness to share identity information in SNS. According to Ajzen (1991), users' willingness to provide information can be seen as a behavioural intention, which according to Theory of Planned Behaviour (TPB) is a reliable predictor of actual behaviour. Information disclosure involves submitting personal information to the SNS. Regardless of whether or not the user chooses to, or is willing to share this information with other online users, once submitted, the information is in the possession of the SNS, and for the user this identifying information may be unknowingly shared on the SNS. Finally, Lo (2010), Shin (2010b), and Hu and Ma (2010) have studied the issues of privacy and trust relationship with users' different attitudes and found that TPB is the most suitable method to measure attitudes towards behaviour.

2.6 Gaps in the Literature

Academic literature on the subject indicates that information can be leaked through SNS (Rosenblum 2007). This is because information disclosed through SNS opens an opportunity for others to view the personal information and identity details for

that particular user (Molok, Chang & Ahmad 2010). Much research has been undertaken in terms of privacy concerns and trust in e-commerce (Dwyer et al. 2007; Lo 2010; Shin 2010b), but only a few studies have researched privacy concerns and trust in the context of SNS. Internet knowledge and experience influence a user to use the Internet for communication and to exchange information (Lo et al. 2010; Park, Konana, Gu & Man Leung 2010). However, Fogel and Nehmad (2009) have found that there is a risk of sharing information on the Internet due to privacy and trust issues. They also suggested that the extent of users' knowledge of the Internet knowledge might affect the degree to which they are willing to share identity information. Furthermore, Lo and Riemenschneider (2010) found that Internet literacy has a positive influence on sharing information, but they were unable to determine whether or not privacy and trust played an important role in influencing a user's willingness to share their digital identity on SNS. This study will focus on understanding the impact of user privacy concerns and trust upon a user's willingness to share their personal information on SNS.

2.7 Conclusion

This chapter has been concerned with the history and background of Social Networking Sites. It also provides background information about Internet privacy and user digital identity information sharing as it applies to the Internet. It was further discussed how user privacy concerns and trust impact upon a user's willingness to share information. However, despite privacy concerns, user experience, knowledge and trust all playing important roles in governing the extent of information sharing by users within SNS, there has been little empirical research which has focused on which factors influence users' behaviour towards use of SNS

for sharing personal information. This research seeks to address those gaps in knowledge in the field.

The next chapter explores theories related to behaviour, and the conceptual model used will show the relationship between SNS experience, privacy concerns, trust and their impact upon the user's willingness to share their digital identities. Finally, hypotheses are developed to support this study.

Chapter III: Theoretical Support and Conceptual Model

3.1 Introduction

This chapter describes in detail the concepts and theories drawn upon in support of this study. Different theoretical bases can help explain different motivations and intentions for users within Information Systems (IS), such as the Theory of Social Capital, Social Exchange Theory, Theory of Weak Ties, Theory of Reason Action (TRA), Technology Acceptance Models (TAM) and Theory of Planned Behaviour (TPB). This chapter also describes the conceptual model design for this study, which was developed from the literature review and supports the objective of this study. This chapter also explores the research question that guides this study and the hypotheses that arise out of it.

3.2 Related Social Theories

From previous study it has been established that a number of social theories have been extensively used to explain why community members share their knowledge with other users within the context of social networks. These theories suggest that users expect either economic or social reward from their participation (Constant, Sproull & Kiesler 1996; Nahapiet & Ghoshal 1998; Wasko & Faraj 2005). The Theory of Weak Ties provides valuable insights into why people seek information from virtual communities (Granovetter 1973; Granovetter 1983). Weak Ties refer to relationships between people with little familial or occupational connection. Consisting of members with diverse backgrounds, virtual communities can provide a

good platform within which people might diversify their sources of information. Psychology-based theories, on the other hand, propose that individuals' decision making-processes are often influenced by their perceived level of knowledge or confidence (e.g., illusion of knowledge or overconfidence), leading them to make decisions according to their prior beliefs, rather than by seeking advice from others (Barber & Odean 2001). Such factors may mitigate members' intentions to seek information from virtual communities, but cannot explain why they post information about themselves. Information systems (IS) theories and models such as the Theory of Reasoned Action (TRA) and Theory of Planned Behavior (TPB) can be extended to explain how people are motivated to either share their knowledge or to seek information from other members which, in turn, leads to different intentions and behaviours in virtual communities (Lin 2006). In particular, the information adoption model TPB that is extended from TRA posits that the usefulness of information, quality of information, and trust toward information sources are important factors that drive people to accept information from other sources (Bhattacherjee & Sanford 2006; Sussman & Siegal 2003).

This study draws upon the Theory of Reasoned Action (TRA) and Theory of Planned Behaviour (TPB) to explain the phenomenon of users' willingness to disclose personal information on SNS. The TRA (Ajzen et al. 1980) and its extension, the TPB (Ajzen 1991), have been well adopted and applied by information systems researchers for the last two decades in their examination of users' intentions to adopt technologies (e.g. Davis, 1989). TPB postulates three determinants of behavioural intentions: attitudes, subjective norms, and perceived behavioural control; however, underlying these determinants are the *beliefs* that are relevant to the behaviour

(Ajzen 1991). In this study, the focus is on investigating how individuals' beliefs about Internet privacy and their trust in different entities influence their willingness to provide personal information on SNS. In general terms, if an individual has positive beliefs regarding a certain behaviour, then he or she would be more willing to engage in that particular behaviour (Ajzen 1991).

3.2.1 Theory of Reasoned Action (TRA)

The Theory of Reasoned Action (TRA) describes 'intention' as the best predictor of whether or not behaviour is performed. According to TRA, direct determinants of behavioural intention are the pre-existing attitude towards the behaviour and the subjective norm associated with the behaviour. Attitude refers to personal beliefs about the positive or negative value associated with a particular behaviour and its outcomes. The term subjective norm refers to a person's positive or negative value associated with a given behaviour. One's attitude depends on whether or not the behaviour that is being considered is accepted by important referent individuals and their motivation to comply with those referents. Ultimately, interventions can be designed to change behavioural intentions by affecting one's attitude and subjective norm about a particular behaviour in order to promote that specific behaviour in a person.

TRA was drawn from social psychology. It is one of the fundamental theories of human behaviour and has been used to predict behaviour in a broad range of dimensions. Davis (1989) originally applied TRA to individual acceptance of technology and found that the variance explained was largely consistent with studies that had employed TRA in the context of other behaviour. Researchers in the domain

of information systems use this theory to understand the adoption of IT innovation (Han, 2003). TRA has been employed in education, automation in manufacturing and in Internet banking. Even though there is evidence that this theory can be used to understand the adoption behaviour for new technologies, there is limited evidence that this can be used to understand the determinants in understanding the human behavioural intention to use their own sensitive information to share with other systems.

3.2.2 Technology Acceptance Model (TAM)

The Technology Acceptance Model (TAM) (Davis 1989; Davis 1993) is an adaptation of the Theory of Reasoned Action (TRA) (Fishbein & Ajzen 1975) which specifies two beliefs—perceived usefulness and perceived ease of use—as determinants of attitude towards usage intentions and usage (Davis 1989). Usage intentions are, in turn, the sole direct determinants of usage (Taylor & Todd 1995b). Introducing intentions as a mediating variable in the model is important for both substantive and pragmatic reasons. Substantively, the formation of an intention to carry out behaviour is thought to be a necessary precursor to behaviour (Fishbein et al. 1975). Pragmatically, the inclusion of intention is found to increase the predictive power of models such as TAM and TRA, when compared to models that do not include intention (Fishbein et al. 1975; Taylor et al. 1995b).

3.2.3 Theory of Planned Behaviour (TPB)

In the development of theory, Theory of Planned Behaviour (TPB) is derived from the Theory of Reasoned Action (TRA). TPB mentions attitude, subjective norm and

perceived behaviour control intention. In this context, intention indicates people's desired effort to conduct an activity. Furthermore, attitude is an individual preference towards the object in question (Yu & Wu 2007). According to Crespo, Herrero and Bosque (2008) subjective norms reflect the degree of people's affection towards an object or behaviour, due to the perception of a significant referent/s. Moreover, they argue that perceived behavioural control reflects the perception of the availability of resources and opportunities for behaviour development.

Associated with intention to use SNS to share information using TPB, a study carried out by Peluchette and Karl (2008) found that attitudes and subjective norms positively affect an individual's intention to share information, whereas perceived behavioural control does not support this intention. This study includes personal innovativeness as a moderating effect. Another study conducted by Lin (2006) found that attitude and perceived behavioural control does positively affect willingness to share information, while subjective norms do not support this willingness. These studies were conducted with participants of varying backgrounds and antecedents.

TPB draws upon constructs taken from literature relating to characteristics, and more completely to account for conditions where individuals do not have complete control over their behaviour. The TPB asserts that behaviour is a direct function of behavioural intention and perceived behavioural control, and that behavioural intention is formed by one's attitude which, in turn, reflects a feeling of favourableness or unfavourableness towards performing a behaviour; and a subjective norm which reflects the perception that significant referents desire the individual to perform or not perform a behaviour; as well as perceived behavioural

control, which reflects an individual's perceptions of internal and external constraints on behaviour (Ajzen 1991).

Moreover, TPB contains an additional determinant, perceived behavioural control, to accommodate deficiency control and resources for a particular behaviour—which can be deliberate and planned. TPB is considered to be generic as well as assuming that individuals will use the information available logically with rational decision making. This assumption has been used to understand and explain behaviour across a wide range of domains, such as marketing and consumer behaviour and leisure behaviour. All this previous evidence asserts that this theory can be used to understand the adoption of human behaviour to control attitudes towards performing behaviour.

3.3 Research Question (RQ)

To what extent do privacy concerns and trust impact users' willingness to share digital identities within social networking sites?

To answer the main RQ the following sub-questions will be addressed:

RQ1 Does a user's experience of SNS have a positive impact upon their willingness to share digital identity?

RQ2 To what extent does users' privacy concerns impact on trust as a determinant in their willingness to share digital identities on SNS?

RQ3 To what extent does trust influence users to share their digital identities in SNS?

RQ4 To what extent do privacy concerns influence users to share digital identities in

SNS?

3.4 Conceptual Model

The conceptual model is developed for this research using the Theory of Planned

Behaviour by Ajzen (1991), and concepts of privacy and trust developed from

literature review and previous papers by Lo and Riemenschneider (2010), Dinev and

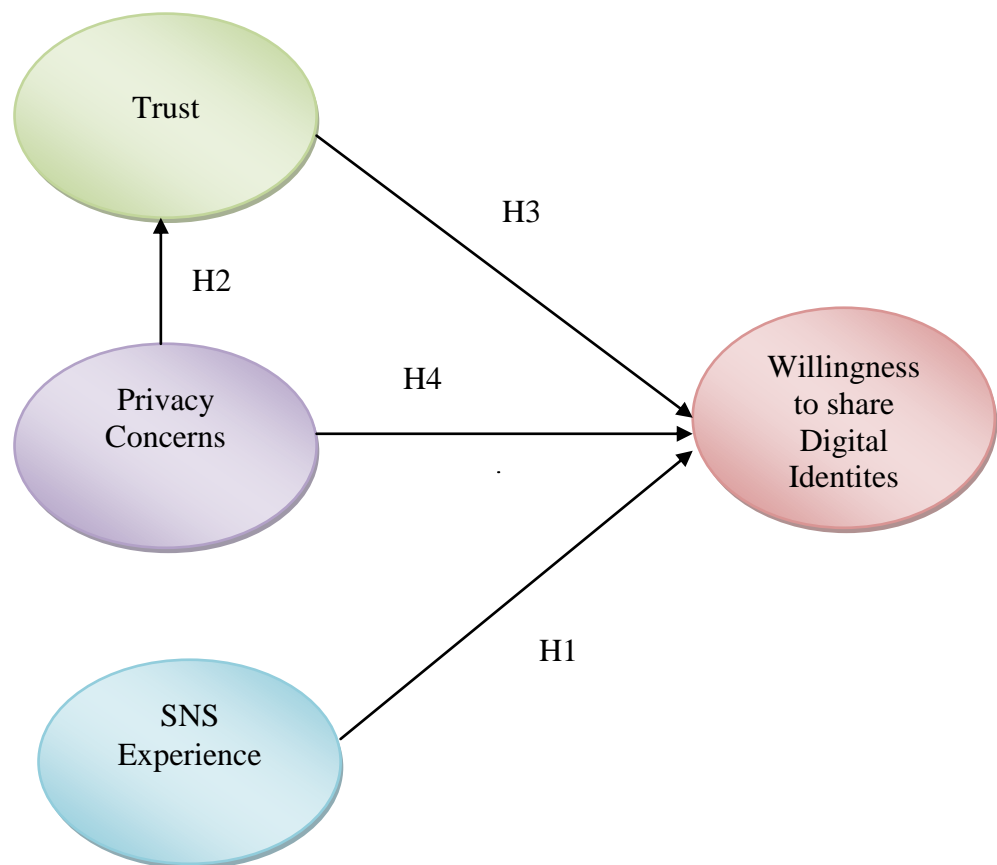Hart (2006), and Malhotra, Kim and Agarwal (2004).

Figure 3. 1 Conceptual model - Key factors of SNS that impact on willingness to share digital identity

(Source: The Author)

This model postulates that privacy concerns, trust and SNS experience do affect

users' willingness to share their digital identity. Privacy concerns and trust play an important role in influencing behaviour, therefore, this model applies the Theory of Planned Behaviour developed by Ajzen (1991). According to TPB (Ajzen 1991, p. 179), 'people's willingness to provide information can be seen as an individual behaviour driven by behavioural intensions where behavioural intentions are a function of an individual's attitude toward the behaviour, the subjective norms surrounding the performance of the behaviour and the individual's perception of the ease with which the behaviour can be performed (behavioural control)'. In this model privacy concerns and trust perceptions are behavioural controls of individuals that will determine a user's belief and willingness to share information. Thus, the model will test the effects of privacy, trust and SNS experiences upon users' willingness to share their digital identity.

In this study, the author was interested to know how privacy concerns and trust impacted on users' willingness to share personal information on SNS. People's willingness to provide information can be seen as a behavioural intention which, according to TRA/TPB, is a reliable predictor of actual behaviour (Ajzen 1991). Information disclosure involves submitting personal information to the SNS. Regardless of whether or not the user chooses to or is willing to share this information with other online users, once submitted, the information is in the possession of the SNS. While people can easily (and do) provide fictitious information to social networking sites, the focus of this study is on investigating why people are willing to provide authentic personal information. For the purposes of this study, personal information broadly encompasses any information that can help trace and confirm one's identity, such as name, birth date, address, phone number,

photograph, or the location of their home town. Prior studies about information sharing on SNS suggest that trust in a SNS is a driving force that increases a person's willingness to share information on that SNS (Dwyer et al. 2007; Fogel et al. 2009).

The Theory of Planned Behaviour suggests that beliefs related to a behaviour are prevailing determinants of a person's behavioural intentions (Ajzen 1991). As such, in the context of this study, a person's beliefs about their knowledge and experience are determinants of his or her intentions to share personal information on a SNS. On the one hand, lower degrees of Internet experience may elevate the user's concerns about privacy, because although the individual may be vaguely aware of potential dangers, he or she may not know how to manage them. On the other hand, higher degrees of Internet experience can likewise raise concerns about privacy, because the individual is more aware of the dangers. However, the more literate individual may have the knowledge to attempt to minimise the dangers by installing and updating operating system and browser security patches and fixes, anti-spyware software and alerts, and other prevention utilities. Due to this perception of control (the ability to try to minimise potential dangers), individuals with higher SNS knowledge and experiences are expected to be less concerned about their Internet privacy than individuals with lower levels of knowledge. For example, in a study of the behavioural intention to conduct online e-commerce transactions, Dinev and Hart (2005-6) found that higher Internet literacy was a positive intention on willingness to carry out transactions online. Hence, the first hypothesis is derived:

H1: Users with high levels of SNS experience will be more willing to share digital identities.

Drawing upon the TRA/TPB (Ajzen 1991; Ajzen et al. 1980), it is argued here that a person's privacy concerns and trust beliefs will tend to significantly influence his or her willingness to provide personal information to a SNS. The TPB postulates three determinants of behavioural intention: attitudes, subjective norms, and perceived behavioural control; however, underlying these determinants are the *beliefs* relevant to the behaviour (Ajzen 1991). In general, if an individual evaluates beliefs regarding a behaviour in a positive light, then he or she would be more willing to perform the particular behaviour (Ajzen 1991). Conversely, a person who evaluates beliefs regarding a particular behaviour negatively will be less likely to perform the behaviour. In studies of privacy concerns and trust in the e-commerce literature, perceived risk was found to negatively influence people's willingness to provide personal information to transact online (Malhotra et al. 2004; Van Slyke, Shim, Johnson & Jiang 2006). Therefore, based on the above studies and literature review, the following hypothesis is used to test the proposed model:

H2: Users with higher levels of privacy concerns have a lower level of trust in SNS.

Similar studies conducted by Malhotra et al (2004) and Liu et al (2005) about trust in online transactions (e-commerce) concluded that trust was found to positively influence the user's intention to use e-commerce. Hence, based on the above studies and literature review, the following hypothesis was used to test the proposed model between trust and willingness to share digital identities.

H3: Users with higher levels of trust will be more willing to share digital identities on SNS.

As discussed previously, the TPB contends that behavioural intentions are antecedents to the specific behaviours of an individual. More specifically, an individual's attitudes and perceptions will influence that individual's actions when he or she believes that certain behaviour will be linked to a specific outcome. Further, subjective norms and social pressures about whether or not to engage in a particular behaviour influences behavioural intentions, as determined by an individual's positive or negative evaluation of it (Liu et al. 2005). Based on the same logic, a user's perception of and attitudes about privacy should influence his or her attitudes toward their willingness to share information; and, in turn, shape his or her behavioural intentions about their participation in a SNS. Hence, based on the above studies and literature review, the following hypothesis is used to test the proposed model between privacy concerns and willingness to share digital identities.

H4: Users with higher levels of privacy concerns will be less willing to share digital identities.

3.5 Conclusion

This chapter reviewed and discussed several traditional theories used in information systems from the last two decades. As the project is related to human behaviour with technology, this study adopts and uses the Theory of Planned Behaviour (TPB), which is derived from the Theory of Reasoned Action (TRA) developed by Ajzen in 1991. Building on the literature review as presented in the previous chapter, a research model was developed. This research model can contribute to a more comprehensive understanding of the relationship between concerns about trust and

privacy as they relate to a user's willingness to share digital identities and SNS experiences. Together, it has the potential to offer a richer explanation of the impact of this variable on sharing information on SNS.

The author further identified and reviewed the independent and dependent variables in the model and used relevant theories to derive the variables and explain their hypothesised relationships with the dependent variables. The next chapter describes the methodology; and operationalises the constructs in order to test the hypotheses as depicted in the model.

Chapter IV: Research Design and Methodology

4.1 Introduction

There are different types of research such as exploratory, descriptive, analytical, predictive, quantitative, qualitative, deductive, inductive, applied and basic research (Collis & Hussey 2009). The main unifying theme that unites all types of research is the need for researchers to focus their efforts on answering two major significant questions (Kripanont 2007).

These questions are, firstly, what methodologies and methods will be used in the research? Secondly, how do they justify this choice and use of these methodologies and methods? Justification of the researcher's choices and use of particular methodology is something that underpins assumptions about reality that they bring to their work (Crotty 1998).

The research methodology and methods for this study were chosen in order to successfully achieve the essential research objectives. The justification of choices and uses will be presented in this chapter, as detailed in the explanation of the chosen research methodology and design of this study. The study materials contained in this chapter re-state the research objective, and then specify the research design, survey population, sampling procedures, instrumentation, data collection and data analysis. This study is guided by the following question: To what extent do privacy concerns and trust influence users' willingness to share their digital identities on social networking sites? Within this chapter the development of the relevant instrument for addressing the fundamental research question posed by this thesis (in this case by means of a survey) is discussed.

4.2 Objective

The broad objective of this study is to show the relationship between privacy concerns, levels of trust of SNS users and their willingness to share their identities with the other SNS users. To reach the goal in a meaningful way, the author has set the research questions as follows:

    i. Does prior experience of SNS have a positive impact on the users' willingness to share aspects of their digital identities?

    ii. To what extent does the users' concern about privacy impact upon their level of trust that in turn guides their willingness to share digital identities on SNS?

    iii. To what extent does trust influence users' decisions to share digital identities on SNS?

    iv. To what extent do privacy concerns influence users to share their digital identities on SNS?

4.3 Research Design

The development and refinement of a research design involves a series of rational choices. The research design is the process aimed at designing the research study in such a way that the essential data can be gathered and analysed to arrive at a solution (Sekaran 2003).

This study uses an explanatory design so that the findings of this research are based upon quantitative study (Creswell, Hanson, Clark & Morales 2007). Bryman and Bell (2007) demonstrate—as depicted in Figure 4.1—the ideal path to follow when organising research by a quantitative method. However, they also clearly state that this work process is an ideal way that is rarely followed in any research in practical

terms. Literally, the actual process followed in the research may include going backwards and forwards between these steps (Bryman et al. 2007; Liong & Mejstad 2010). Instead, they argue that the illustration should serve as a presentation of the most important steps to incorporate when performing quantitative research.
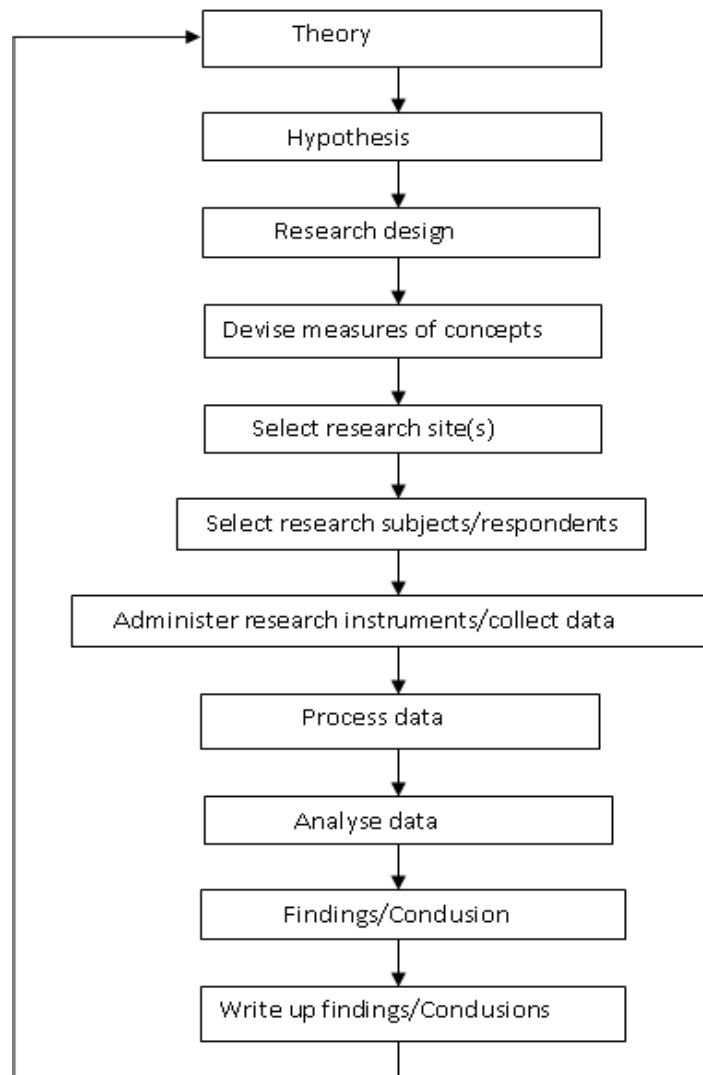
Figure 4.1 The process of quantitative research

(Source :Bryman and Bell (2007))

For this study, the work process flow has not followed the ideal path outlined. Instead, this study does go back and forth between the different steps on its progress towards completion. In doing this, this researcher makes sure that all the steps have in fact been followed, and this process model thus helped the researcher to ensure

that all the components were included and connected to each other, and the modifications subsequently made to the research design are shown below in Figure 4.2.

Figure 4.2 The flow chart of research design

(Source: The Author)

4.4 Research Philosophy and Paradigm

An appropriate research paradigm is an essential concept for any research study. Therefore, a research paradigm can be viewed as a world-view for understanding the

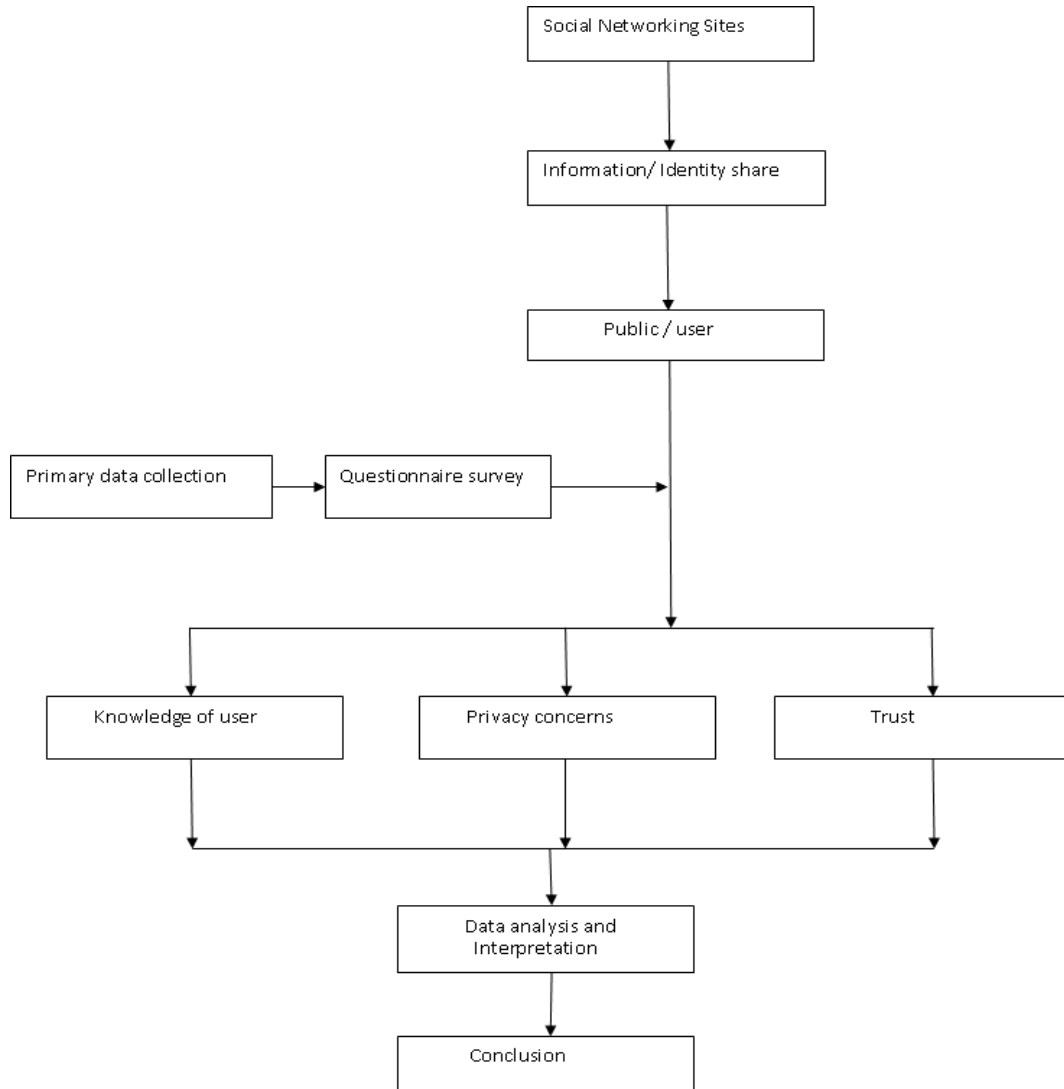complexities of the real world, or assumptions relating to a world which is shared by a society of researchers exploring that world. The research used as the guiding paradigm was positivist, in which measurement and quantification were emphasised in the pursuit of objective knowledge (Seale 1999). This is a scientific approach in which the researcher works logically, and in which the data collection and data analysis aspects of the research are seen as highly important (Creswell & Clark 2007). For the purposes of this research, online community success was a value judgment made by an individual. This perspective is consistent with Wenger's (2005) view that although social networking sites may be designed for communities, individual members were the ones who ultimately experienced the technology as they engaged with the communities. It also resonates with Seddon's (1997) observation that different people using the same system may draw very different conclusions about the success of the system.

By using quantitative research methods, this study was able to perform statistical testing, thereby allowing for higher levels of generalisability than what would be possible using qualitative research methods (Seale 1999). However, this study agrees with criticism of the positivist paradigm, most notably stemming from researchers with a post-positivist perspective (Fischer 1998). According to this criticism, the positivist paradigm is described by post-positivists as naïve, as there is no one absolute truth that can be unravelled by relying on positivist research methods. According to Fischer (1998), rather, reality is constructed and is dependent on the perspective of the individual. But even if this criticism is pertinent, especially to researchers within the social science area, this research argues that choice of paradigm and research method for this study has been done in line with post-

positivist research's emphasis on multiple methods of inquiry (Fischer 1998).

4.5 Research Approach

The specific approach of this study was to build upon previous research regarding privacy concerns and trust related to SNS. Moreover, from its literature review and theoretical background, this research was carried out with an approach that was deductive in overall terms (Bryman et al. 2007). According to Bryman and Bell (2007) the deductive approach is one in which hypotheses are commonly stated, based on previous findings and then tested using statistical methods. The study's conclusions are then based on the rejection or non-rejection of the stated hypotheses. However, Bryman and Bell (2007) note that a significant portion of quantitative research does not include a statement of hypotheses in the first place; that it is a feature most pervasive in experimental studies. This research was carried out in accordance with research processes based on the concepts of the hypothetico-deductive method (Sekaran 2003).

The following are the steps that were conducted throughout this study project:

1) Observation (which was conducted, but it was not used as methodology).

2) The use of a semi-online survey to collect data to ascertain what is happening and why, the collected data will be useful for study; and the questionnaire can be amended if necessary.

3) A broader survey of the literature was conducted so that the researcher might anticipate a myriad of scenarios that may arise during the study, and determine how to overcome each situation. This information gives additional insights into

the various possibilities that might eventuate, and helps confirm that these variables were good predictors for privacy concerns for users and the effect of trust upon user s' willingness to share their digital identities.

4) Theory formulation is a step in developing a theory incorporating all the relevant factors contributing to usage behaviour and behavioural intention of academics to use the Internet and SNS. It was an attempt to integrate all the information in a logical manner, involved a collection of theories and models from the literature to help conceptualise and test the reasons for the problems. In other words, it explained the research questions and hypotheses, and helped in the identification and labelling of variables (Hussey & Hussey 1997).

5) Hypothesising

This step was used to generate various hypotheses that would be tested to examine whether the theory formulated was valid or invalid.

6) Data collection

A questionnaire was developed, based on the previous literature and research; to determine use, privacy concerns and trust as factors that might influence SNS users' willingness to share their digital identity. This was then used as a survey tool to collect data.

7) Data analysis

The data that was collected through the online survey questionnaire was analysed to see what factors influenced users to share digital identities on SNS. Other information about the user, such as demographic data and their interest in and knowledge of social networking sites, can be obtained at this stage.

8) Deduction

This is the process of concluding the results by interpreting the meaning of the

results of data analysis.

4.6 Questionnaire Design

The online survey used in this study was created by the researcher using 'Qualtrics' and was physically located on secure servers of the Qualtrics company. Qualtrics was used to collect and store the data for analysis. The application was configured to support anonymous participation, thereby assuring anonymity, confidentiality and privacy throughout the study, and making it impossible for the researcher to make links between survey responses and specific responders. The online form of the survey also allowed the participants to complete the survey at any time and in a location convenient to them. In addition, the survey was configured so that participants could exit and start the survey at any time and return at a later time/date to recommence the survey.

The overall design of this research questionnaire was highly inspired by Dinev and Hurt (2006), Malhotra, Kim and Agarwal (2004), McKnight et al. (2003), Lo and Riemenschneider (2010) and Fogel and Nehmad's (2009) design. Similarly, in order for this research to also answer its own research questions, the questionnaire had to be divided into several parts. The first part revolved around demographic information and general knowledge of social networking sites. The second part concerned the general attitude of respondents towards privacy concerns. The third part related to the trust expressed by respondents about social networking sites; and the fourth and final part concerned the user's willingness to share digital identities on SNS.

According to Sekaran (2003), in order to minimise bias in the results of the research,

researchers need to concentrate mainly on three areas when designing a questionnaire:

i)   The wording of the questions;

ii)   Planning how the variables will be categorised, scaled and coded after receipt of the responses, and

iii)   The general layout content of the questionnaire design.

Overall, table 4.1 presents the questions asked in this research questionnaire and the scientific background pertaining to them. As such, it was up to the personal judgment of the researcher to construct relevant measurements, however, the item used to measure the research model (items used in the questionnaire) was developed from the items already used by Dinev and Hurt (2006), Malhotra, Kim and Agarwal (2004), McKnight et al. (2003), Lo and Riemenschneider (2010) and Fogel and Nehmad (2009). In addition, the scientific background mentioned in the table refers to researchers who have used similar questions to assess attitudes within the realm of SNS experiences, privacy concerns, trust and willingness to share digital identities on SNS.

The design process for the questionnaire for this project took almost 3 months (May 2011 to July 2011) prior to the pilot online survey being undertaken. This was because the researcher was aware that in designing the questionnaire it was important to proceed with caution, keeping in mind the rationale for why the research was being done (Veal 2005). Thus, the researcher acknowledged that the aim in designing the questionnaire was to achieve the research objectives (see Chapter I), with consideration for meeting the basic criteria of relevance and accuracy (Zikmund,

Griffin, Babin & Carr 2009).

The questions were structured and separated into five sections (see Table 4.1 and Appendix D). Some sections such as privacy concerns, trust and willingness to share digital identity used a 7-point Likert scale because this method it is extremely popular for measuring attitudes, and is relatively simple to administer. With the Likert scale, respondents indicate their attitudes by checking how strongly they agree or disagree with carefully constructed statements that range from very positive to very negative toward the attitudinal object. In this study, seven alternative measurement scales were used which were adopted from previous well-known studies such as Dinev and Hurt (2006), Malhotra, Kim and Agarwal (2004), McKnight et al. (2003), Lo and Riemenschneider (2010) and Fogel and Nehmad (2009). This scale ranges from strongly disagree = 1, disagree = 2, somewhat disagree = 3, neither agree nor disagree = 4, somewhat agree = 5, agree = 6, and strongly agree = 7. A brief summary of the use of scales and measurements follows.

Section A focused on general knowledge, experience and use of the SNS as it related to the demographic data of the users. This section contained 16 questions, and of the 16, five questions were open-ended and the rest of the questions were closed. It comprised six questions that are established as ordinal scales, such as 'How many friends do you have in your Social Network accounts on average?' and ten questions with nominal scales. The design of this section was based on previous studies.

Section B was an important section focused on respondents' privacy concerns about using SNS. It was established as a 7-point Likert scale. It comprised five items based

on the previous study such as 'I am concerned that the information I submit on the Internet could be misused', (see Table 4.1 for full details).

Section C was also an important section used for establishing the trust concerns of user. It was established as a 7-point Likert scale. Measurements were developed from previous studies by McKnight et al. (2002), Dinev and Hart (2006), Malhotra, Kim and Agarwal (2004) and including statements such as, 'SNS would tell the truth and fulfil its promises related to the personal information provided by me'.

Section D focused on investigating the SNS user's intention to willingly share digital identity information. This was established as a 7-point Likert scale.

Table 4-1 Questionnaire items and variable coding

Question/Statement	Scientific Background	Variable Abbreviation
Demographic		
In what age range are you?	Author develop	
What is your occupation?	Author develop	
What is your gender?	Fogel and Nehmad (2009); Hoy and Milne (2010); Manago, et al. (2008); Lewis, et al., (2008)	
What is your marital status?	Author develop	
What is your highest education level?	Author develop	
Why do you use Social Networking?	Author develop	
I am using Social Networking Site	Fogel and Nehmad (2009); Dwyer, et al., (2007)	
I know Social Networking Site from	Author develop	
How many Social Networking accounts you have?	Fogel and Nehmad (2009); Tufekci (2008)	
How many friends do you have in your Social Network accounts in average	Fogel and Nehmad (2009); Lewis, et al., (2008); Ellison et al., (2007)	
Has the usage of social networking made a positive impact in your social life?	Author develop	
What is your country of origin? Please specify	Author develop	
SNS Experience and Knowledge		
I am using Internet since	Fogel and Nehmad (2009)	SNS1
I am using Social Networking Site since	Fogel and Nehmad (2009)	SNS2
Did you read the Terms of use/ Privacy policy while creating the Social Networking Site account?	Author develop	SNS3
Did you modify privacy settings from default settings after creating the account?	Gross and Acquisti (2005);	SNS4
Privacy Concerns		
I am concerned that the information I submit onto social networking sites could be misused.	Dinev and Hart (2006), Malhotra, Kim and Agarwal (2004)	PC1

Question/Statement	Scientific Background	Variable Abbreviation
I am concerned that a person can find private information about me on the Internet.	Dinev and Hart (2006), Malhotra, Kim and Agarwal (2004)	PC2
I am concerned about submitting information on the Internet because of what others might do with it.	Dinev and Hart (2006), Malhotra, Kim and Agarwal (2004)	PC3
I am concerned about submitting information on the Internet because it could be used in a way I did not foresee	Dinev and Hart (2006), Malhotra, Kim and Agarwal (2004)	PC4
I am concerned that online companies are collecting too much personal information about me	Dinev and Hart (2006), Malhotra, Kim and Agarwal (2004)	PC5
Trust		
I believe that SNS would act in my best interest when dealing with my personal information.	McKnight et al. (2002), Dinev and Hart (2006), Malhotra, Kim and Agarwal (2004	T1
SNS is interested in protecting my personal information according to the preferences I specify.	McKnight et al. (2002), Dinev and Hart (2006), Malhotra, Kim and Agarwal (2004	T2
SNS would tell the truth and fulfill its promises related to the personal information provided by me.	McKnight et al. (2002), Dinev and Hart (2006), Malhotra, Kim and Agarwal (2004	T3
SNS is sincere and genuine in managing my personal information.	McKnight et al. (2002), Dinev and Hart (2006), Malhotra, Kim and Agarwal (2004	T4
SNS handles personal information submitted by users in a competent fashion.	McKnight et al. (2002), Dinev and Hart (2006), Malhotra, Kim and Agarwal (2004	T5
SNS performs its role of managing my personal information according to my privacy settings very well.	McKnight et al. (2002), Dinev and Hart (2006), Malhotra, Kim and Agarwal (2004	T6
I believe that if I allowed my SNS friends to view my personal information, they would act in my best interest when dealing with this information.	McKnight et al. (2002), Bhattacherjee, A. (2002), Dinev and Hart (2006)	T7
My SNS friends would not use my personal information opportunistically.	McKnight et al. (2002), Bhattacherjee, A. (2002), Dinev and Hart (2006)	T8
I would characterize my SNS friends as honest in handling my personal information.	McKnight et al. (2002), Bhattacherjee, A. (2002), Dinev and Hart (2006)	T9
My SNS friends are sincere and genuine in dealing with my personal information.	McKnight et al. (2002), Bhattacherjee, A. (2002), Dinev and Hart (2006)	T10
My SNS friends have the skills and expertise to handle my personal information carefully.	McKnight et al. (2002), Bhattacherjee, A. (2002), Dinev and Hart (2006)	T11
Willingness to share digital identities		
I am willing to share my real name.	Fogel and Nehmad (2009); Gross and Acquisti (2005); Christofides, et al., (2009); Lo and Riemenschneider (2010)	DI1
I am willing to share my real date of birth.	Fogel and Nehmad (2009); Gross and Acquisti (2005); Christofides, et al., (2009); Lo and Riemenschneider (2010)	DI2
I am willing to share my real hometown address.	Fogel and Nehmad (2009); Gross and Acquisti (2005); Christofides, et al., (2009); Lo and Riemenschneider (2010	DI3
I am willing to share my real email address.	Fogel and Nehmad (2009); Gross and Acquisti (2005); Christofides, et al., (2009); Lo and Riemenschneider (2010)	DI4
I am willing to share my real home phone number.	Fogel and Nehmad (2009); Gross and Acquisti (2005); Christofides, et al., (2009); Lo and Riemenschneider (2010)	DI5
I am willing to share my real mobile phone number.	Fogel and Nehmad (2009); Gross and Acquisti (2005); Christofides, et al., (2009); Lo and Riemenschneider (2010)	DI6
I am willing to share my real photograph.	Fogel and Nehmad (2009); Gross and Acquisti (2005); Christofides, et al., (2009); Lo and Riemenschneider (2010)	DI7
I am willing to share the name of my real high school(s), I have attended.	Fogel and Nehmad (2009); Gross and Acquisti (2005); Christofides, et al.,	DI8

Question/Statement	Scientific Background	Variable Abbreviation
	(2009); Lo and Riemenschneider (2010)	
I am willing to share the name of my real college(s) attended.	Fogel and Nehmad (2009); Gross and Acquisti (2005); Christofides, et al., (2009); Lo and Riemenschneider (2010)	DI9
I am willing to share my real name of employer.	Fogel and Nehmad (2009); Gross and Acquisti (2005); Christofides, et al., (2009); Lo and Riemenschneider (2010)	DI10
I am willing to share my real interests.	Fogel and Nehmad (2009); Gross and Acquisti (2005); Christofides, et al., (2009); Lo and Riemenschneider (2010)	DI11
I am willing to share my real personality	Fogel and Nehmad (2009); Gross and Acquisti (2005); Christofides, et al., (2009); Lo and Riemenschneider (2010)	DI12
I am willing to share my real gender	Fogel and Nehmad (2009); Gross and Acquisti (2005); Christofides, et al., (2009); Lo and Riemenschneider (2010)	DI13

4.7 Data Collection and Sample Size

In order to examine SNS users' privacy concerns and trust and behaviour, and willingness to share their digital identity in SNS, the population of this research (i.e. the entire group of people that the researchers' desires to examine) (Sekaran 2003) are all SNS users. Consequently, if this study were to use a probabilistic sampling method, it would require the construction of a selection procedure in which all SNS users would have the same likelihood of being selected to participate in this study (Anderson, Sweeney, Williams, Freeman & Shoesmith 2010). Regardless of how the probabilistic sampling method would be performed in practice (simple, stratified or cluster), this requirement was simply not be possible to fulfil due to the limited time available for this Masters level study.

To collect data, an online survey link was posted on different SNS forums, and requests were made for users to participate in the survey. This study was careful in choosing a Facebook forum where the visitors would, to a significant extent, include persons displaying the same diversity in attitudes as the general public. The sample population of this study is taken from Facebook users where, according to Facebook (2011), they have more than 500 million users; however, for this study purpose data is collected from Facebook Forum users where the number of registered users is

approximately 17,000 and a list of the users is publicly available in the forum and the total number of participants in the online survey were 155 users. Facebook Forum is a community forum where users are able to share, discuss and comment on anything related to Facebook and other SNS, such as a new SNS feature, its advantages and disadvantages, an application, games, new privacy settings, scams, photos, videos, events, and numerous other general topics where users can request help. There are also forum contests, general chat areas and an interactive Chatbox, where online members gather to chat together in real-time (Forum 2011). Facebook Forum was selected for this study because it is a subset of Facebook and it will improve the credibility of the results because participation includes users from different backgrounds including application developers, professionals, students and social workers, who represent much broad population of SNS users.

As this research collected data on the number of people who have visited the questionnaire, as well as the number of people who have completed it, an assessment can be made regarding this type of non-response error. It was found that 191 people visited the survey and out of those 191 only 161 people attempted the survey. Of these 161 participants only 155 completed the entire questionnaire, which corresponds to a mean survey completion rate of approximately 96.27%. This value is reflective of good questionnaire design.

Another data collection method that could have been used is posting links to questionnaires in different SNS forums. Even if that had increased the sample size, the detrimental effects on the generalisability of these research findings would have been too significant. Overall, this study argues that the data collection method

actually employed by the researcher ensured that the researcher received a sample that was more diverse than what would be the case using any other available methods.

4.8 Ethical Considerations

In any research study, ethical clearance is important, and is mandatory if the research involves humans. This study directly involved people through the process of the online survey instrument. Therefore, procedures were followed to gain ethical clearance from the USQ Ethics Committee. At the same time, participants in the online survey were clearly notified about their voluntary participation, the confidentiality of the data and the participants' identities. Furthermore, participants in this research were informed about their right to privacy and their option of discontinuing their participation in the study at any time. In this research, an informed consent was implied to the participations. Anonymity of the respondents was guaranteed: there was no entry in the questionnaire to identify a specific respondent, so it is impossible for the researcher to identify any individual response. Furthermore, all the data gathered in this study were kept secure and confidential, according to USQ regulations.

Data and information gathered in this study were stored in digital format on a secure USQ server. It was also clear to the participants that under no circumstances would the identity of any individual or group of individuals be released in any publications that may eventuate from this study.

4.9 Data Analysis

This section presents an analysis of the data that was collected from the online surveys. Non-parametric techniques are ideal for use when the collected data are measured on nominal and ordinal scales. They are also useful when the samples are relatively small and when data do not meet stringent assumptions of the parametric techniques (Pallant 2011). With this in mind, Statistical Package (SPSS 19.0) was used to analyse the data. Following the analysis of demographic data, Exploratory Factor Analysis was then conducted to check if the proposed factor structures were indeed consistent with the actual data. The various loadings are shown in a number of tables in Chapter 5. Next, Confirmatory Factor Analysis (CFA) was conducted to check the reliability and validity of the measurement model. This measurement model was estimated using AMOS 19.0. A correlation study investigated the relationship between independent and dependent variables using a Structural Equation Modelling (SEM), a casual modelling statistical tool.

4.9.1 Descriptive Statistics Analysis

The purpose of conducting descriptive statistical analysis is to illustrate the characteristics of the constructs associated with frequencies, the mean values, and standard deviation of each variable. Descriptive statistics is also designed to provide information about the distribution of the variables (Cooper & Schindler 2003).

4.9.2 Reliability

Testing the veracity of the data is done through testing the reliability and validity of the measures. According to Veal (2005), reliability is the extent to which research

findings would be the same if the research were to be repeated at a later date, or with a different sample of subjects. In other words, the reliability of a measure indicates the extent to which the measure is without bias (error free) and, hence, offers consistent measurement across time and across the various items in the instrument. It helps to assess the goodness of measure, and indicates accuracy in measurement (Sekaran 2003).

The most common and popular way to check reliability is by using Cronbach's alpha (Cronbach 1951; Peter 1979; Sekaran 2003) or the mean inter-item correlation between the items (Pallant 2011). This is a test of the consistency of respondents' answers to all the items in a measure. To the degree that items are independent measures of the same concept, they will be correlated with one another (Sekaran 2003). The Cronbach's Alpha for each construct was calculated to check the reliability of the scales. The calculation also provided a baseline for the analysis of internal consistencies. The Cronbach's Alpha for each construct is displayed in Table 4.2. All constructs were found to have a Cronbach's Alpha higher than 0.6. According to Sekaran (2003), reliabilities less than 0.6 are considered to be poor; those in the 0.7 range are acceptable; and those over 0.8 good. The closer the reliability coefficient gets to 1.0, the better. In other words, the generally agreed upon lower limit for Cronbach's alpha is 0.70, but this may decrease to 0.60 in exploratory research (Robinson, Shaverm & Wrightsman 1991). The results suggest that the items consistently measured the constructs and were suitable inclusions in the final scales (Nunnally 1994). Moreover, the items and measurement are adopted from the previous studies so that they are reliable for this study.

4.9.3 Validity

Validity is defined as the extent to which the data collected truly reflects the phenomenon being studied. Usually, business research faces difficulties about validity, specifically in the measurement of attitudes and behaviour since there are always doubts about the true meanings of responses made in surveys, interviews, and self-reporting of behavior (Malhotra 2008; Veal 2005).

Sekaran (2003) suggests several types of validity tests for testing the integrity of measures including content validity, criterion-related validity, and construct validity.

4.11.3.2 Construct Validity

The construct validity that was used in this research testified as to how well the results obtained from the use of the measure fit the theories around which the test was designed. In other words, construct validity testified that the instrument did tap the concept as theorised. Construct validity can be established through (1) correlation analysis (convergent and discriminant validity), (2) factor analysis, and (3) the multi-trait, multi-method method matrix of correlations. Others suggest the three most widely-accepted forms of validity are convergent, discriminant, and nomological validity (Biesanz & West 2004; Campbell & Fiske 1959).

Convergent validity is synonymous with criterion validity (Zikmund et al. 2009) and with correlation analysis, and is one way of establishing construct validity for this research. It indicates that items that are indicators of a specific construct should converge or share a high proportion of variance in common (Hair Jr et al. 2006). In other words, it assesses the degree to which two measures of the same concept are

correlated, with high correlation indicating that the scale is measuring its intended concept. Thus, reliability is also an indicator of convergent validity (Hair Jr et al. 2006).

According to rules of thumb, it has been suggested that item-to-total correlations exceed 0.50 and the inter-item correlations exceed 0.30 (Robinson et al. 1991). Cohen (1988) suggests correlation (r) = 0.10 to 0.29 (small correlation: both positive and negative correlation), r = 0.30 to 0.49 (medium correlation), and r = 0.50 to 1.00 (large correlation). As results of the inter-item correlation values of the indicators in each construct being in both medium and high levels (higher than 0.30, and most of them higher than 0.50) (except some inter-items correlation values in usage behaviour), and the item-total correlation values were also in higher levels (higher than 0.50) (except some item-total correlation values in usage behaviour), these indicated the convergent validity of the instrument.

Because of the reliability of results with high coefficient alpha, and the correlation values of the questionnaire and the results of the convergent validity of this pilot study, a minor change was made to the wording of the questionnaire after the pilot study. The instrument was developed and designed based upon the theoretical literature survey and adopted from previous studies. Thus, the measures of the instrument provided adequate coverage of the concepts; and the instrument has clear and understandable questions. Consequently, the instrument was reliable, valid when considering content validity, construct validity and theoretical validity; and was ready to be used in the main survey.

4.9.4 Factor Analysis

Factor analysis is used to explore the underlying pattern or relationship for a large number of variables and to determine whether the information can be condensed or summarised in a smaller set of factors or components (Hair Jr et al. 2006). Construct validity will be examined via Confirmatory Factor Analysis (CFA). CFA is to be used when the research knows about the number of the factors, as well as which variables load on the specific factors (Hair Jr et al. 2006; Liao, Chen & Yen 2007).

4.9.5 Structural Equation Modelling (SEM)

The main objective of this SEM analysis was to generate a model that best described the effect of privacy concerns and trust as they impacted upon the willingness of users to share information on SNS. In order to achieve this main research objective, Structural Equation Modeling was considered to be suitable. The generated model is expected to be a model that is both substantively meaningful and statistically well-fitting (Joreskog & Sorbom 1996).

Structural Equation Modeling (SEM) is a multivariate technique combining aspects of multiple regression (examining dependence relationships) and factor analysis (representing unmeasured concepts-factors with multiple variables) to estimate a series of interrelated dependence relationships simultaneously (Hair Jr et al. 2006; Schumacker & Lomax 2004). SEM also integrates other techniques such as recursive path analysis, non-recursive econometric modeling, ANOVA, analysis of covariance, principal component analysis and classical test theory (Holmes-Smith 2000). In addition, SEM is also known as path analysis with latent variables and is now a regularly-used method for representing dependency (arguably 'causal') relations in

multivariate data in behavioural and social sciences (Kripanont 2007; McDonald & Ho 2002).

A structural equation model or path model depicts the structural relationships among constructs (Sharma 1995). In other words, it is a model of relationships among variables (Hayduk 1987), and is a statistical methodology that takes a confirmatory (i.e. hypothesis-testing) approach to the analysis of a structural theory relating to some phenomenon with two important aspects: (1) the causal processes under study are represented by a series of structural equations, and (2) these structural relations can be modeled pictorially to enable a clearer conceptualisation of the theory under study (Byrne 2001). When compared to other multivariate techniques, it has four significant benefits over those techniques (Byrne 2001):

> 1) SEM takes a confirmatory approach rather than an exploratory approach to the data analysis, although SEM can also address the latter approach. SEM lends itself well to the analysis of data for the purposes of inferential statistics. On the other hand, most other multivariate techniques are essentially descriptive by nature (e.g. exploratory factor analysis) so that hypothesis testing is possible, but is rather difficult to do.
>
> 2) SEM can provide explicit estimates of error variance parameters, but traditional multivariate techniques are not capable of either assessing or correcting for measurement error.
>
> 3) Data analysis using SEM procedures can incorporate both unobserved (i.e. latent) and observed variables, but the former data analysis methods are based on observed measurements only.

4) SEM methodology has many important features including modeling multivariate relations for estimating point and/or interval indirect effects, although there are no widely and easily applied alternative methods for these kinds of features.

In particular, SPSS version 19.0 was used to input and conduct preliminary analyses of data (see Chapter 5) together with an SEM software package called AMOS version 19.0. This was used to test the model fit. Structural Equation modeling techniques demonstrate and test the theory of representation with a model that shows how measured variables combine together to represent construct validity (Hair Jr et al. 2006). Furthermore, Confirmatory Factor Analysis (CFA) enables the researcher to illustrate how well the measured variables are represented in the constructs, and it also shows how the results are combined with construct validity tests in order to maintain a good understanding of quality of the measurement according to Hair Jr et al (2006).

4.10 Conclusion

This chapter outlined the methodology used for the research design and data collection within this study. It described and justified how the data was prepared for analysis and was then analysed within each hypothesis. The author described the process of ensuring validity and reliability in order to come up with the final instrument. Wherever possible, existing measures that were proven to be reliable and valid were adapted from prior studies. However, rather than setting out to validate the measures that have already been validated many times in various IT adoption and online electronic business studies, the purpose of this study has been to develop or modify a new set of measures in the SNS context, provided there is support from the

existing literature. As mentioned in the data analysis strategy above, Chapter Five will discuss the data analysis procedure using SPSS 19.0 and AMOS 19.0 and present the results.

Chapter V: Results and Analysis

5.1 Introduction

This chapter contains the empirical results of this study and divides the data analysis measurements into the following steps. The first step is the descriptive analysis to describe the respondents' characteristics, and the last part contains the statistical data analysis using SPSS, followed by a presentation of the results. The results of the SEM analysis are presented to test the interrelationships among SNS users' experiences on how they are influenced by knowledge, privacy concerns and trust and how it affects their willingness to share digital identities.

To investigate, the following objective of this study was established to determine the relationship among the construct and shows effect on willingness to share digital identities in SNS:

> To what extent do privacy concerns and trust influence user willingness to
> share digital identities on social networking sites?

5.2 Data Quality and Characteristics of Respondents

Data quality and its suitability for analysis were ensured through careful inspection and review of the data. The attributes of respondents consisted of six major variables including gender, marital status, age, education, occupation, number of friends on SNS, the number of SNS accounts; and the results of these questions and answers will be discussed in detail with reference to each variable in the below Figure. The automatic survey system showed that 196 respondents started filling in the questionnaire, however, only 155 were completed sufficiently to allow for adequate

future research.

This research follows Hair Jr et al's (2006) approach to missing data patterns and, according to their guidelines, adherence to statistical assumptions, identification of outliers and a review of skewness and kurtosis were inspected. The data was carefully reviewed and tested, and the results showed that the data was suitable for further analysis. Two types of missing data patterns were examined: missing data for each case and missing data for each variable. While several missing data of both types were found, the examination revealed that missing data was not a problem.

Among the 155 respondents 54.2% were male, and from this it seems that almost equal numbers of users of each gender user were accessing the SNS, as shown in Table 5-1. This was a surprising result, because most of the online groups to which the researcher promoted the survey had female moderators. The majority of the respondents were aged between 18–30 years. A graphical representation of the age distribution of the respondents is shown in Figure 5.1. A total of 81.95% of participants were between the ages of 18 and 40, while 16% were more than 40 years of age. However 1.29% of users did not disclose their age.
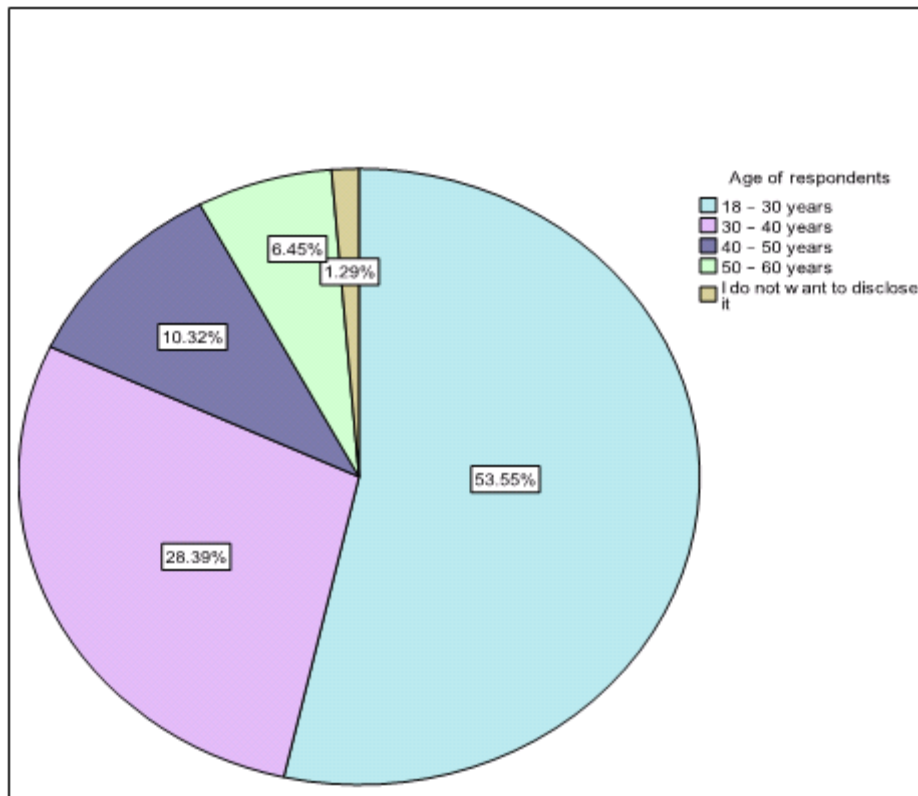
Figure 5.1 Respondent age groups percentiles

The length of time that participants had been using the Internet is shown in Figure 5.2. More than 36% of the participants had more than 5 years of Internet experience (n=155). Only 1.6% of respondents had used the Internet for two years or for less than two years. This result shows that the number of Internet users is increasing year by year.
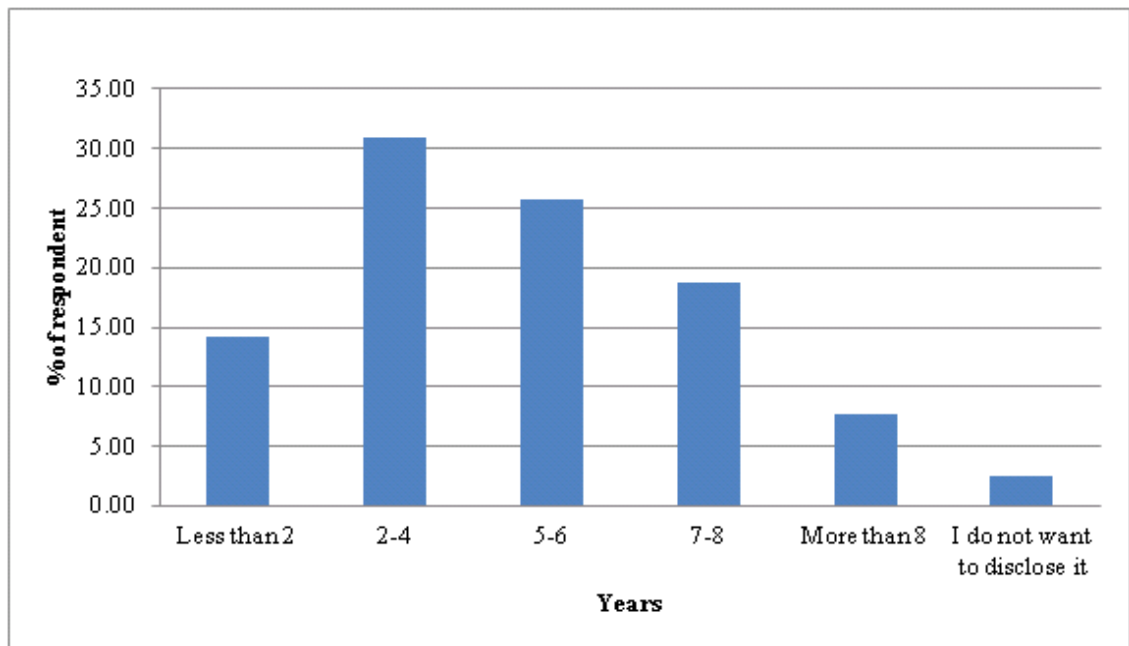
Figure 5.2 Use of Internet

Figure 5.3 describes how long the participants had been using SNS. Altogether, more than 30% of the respondents had been members of and using SNS for the last 2 to 4 years. More than 25% had been members for the last 5 to 6 years. More than 7% of respondents had used SNS for more than 8 years. However less than 3% of users did not want to disclose how long they had been using SNS.
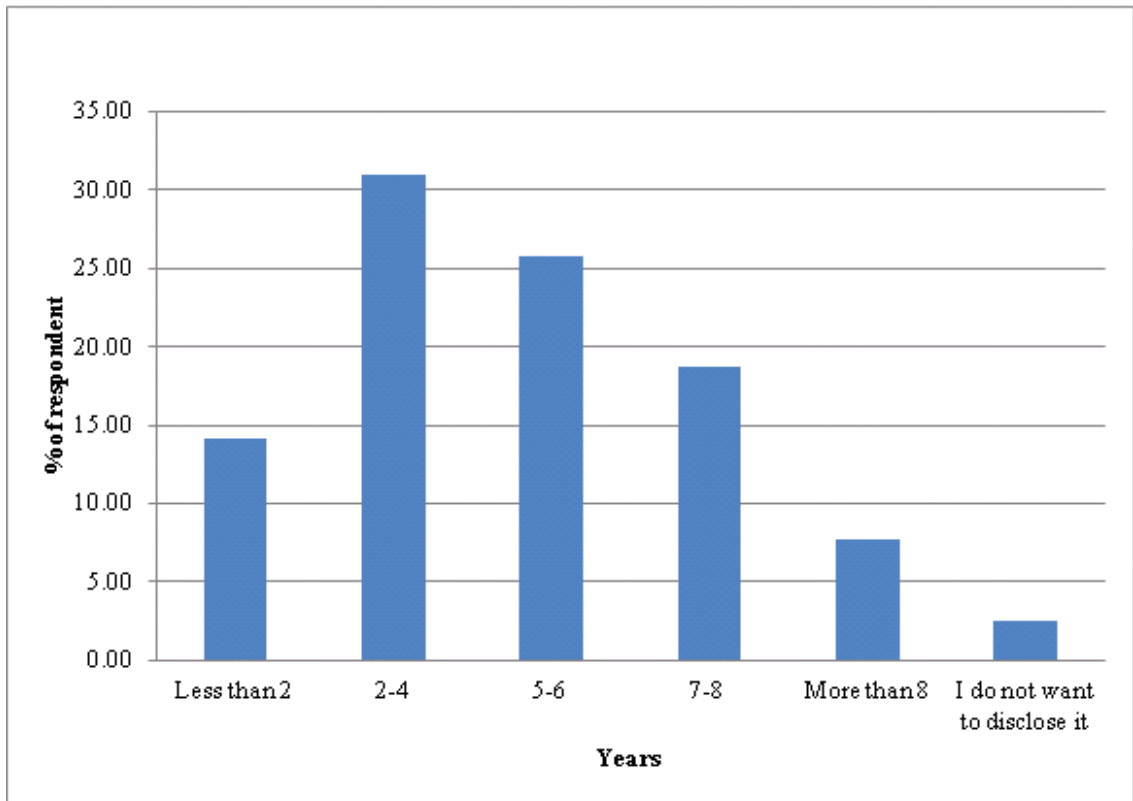
Figure 5. 3 Use of social networking sites

All of the participants belonged to at least one SNS. The number of SNS accounts opened by respondents at the time of their participation in the survey is graphically displayed in Figure 5.4. More than 31% of respondents had two different SNS accounts. More than 29% of respondents have one SNS account and less than 12% of respondents have more than four SNS accounts. A few respondents did not want to disclose how many SNS accounts they had registered.
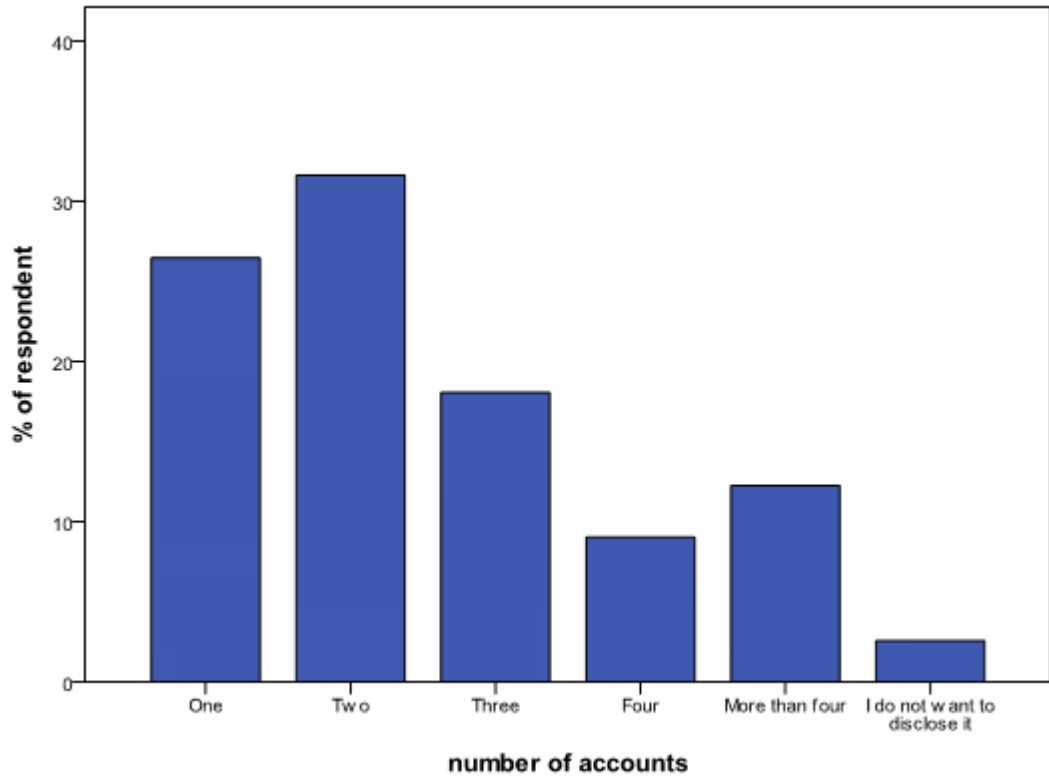
Figure 5.4 Current number of accounts on different SNS

The graphical representation in Figure 5.5 shows how often users logged into their SNS accounts. While 46.5% of respondents said they had visited the site several times a day, 23.2% visited only once per day. A total of 15.5% of respondents did not visit the site each day, but they did visit the site within a week, while a further 3.2% of users logged onto the SNS once a month. Fewer than 2% of respondents did not want to disclose how often they visited SNS.
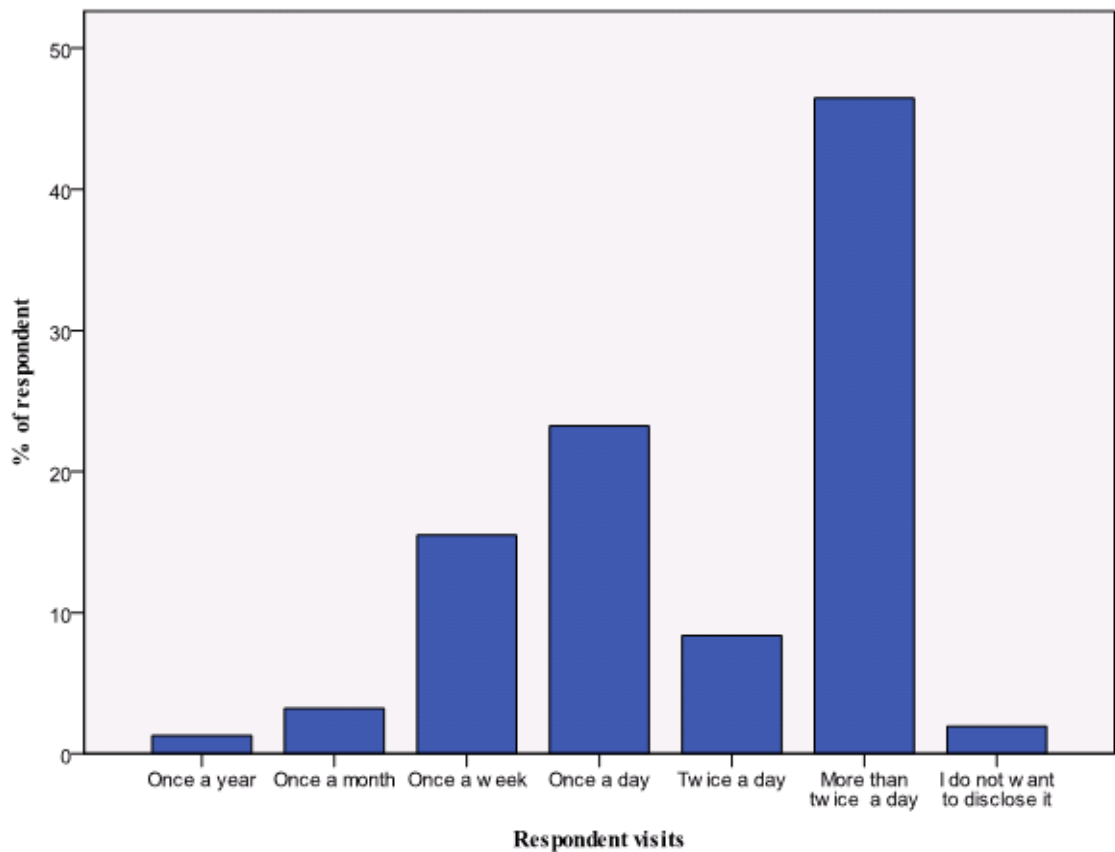
Figure 5.5 Number of visits to social networking sites

SNS are growing exponentially, and the majority of respondents became aware of SNS through friends, news and media. Most of the respondents (61.9%) responded that they became aware about the SNS for first time from their friends, as shown in Figure 5.6. Due to the frequent use of Internet, 39% of participants gained awareness of SNS through their use of the Internet and 9.7% of users came to know about SNS through news and the media. However, less than 1% of users did not want to disclose how they came to know about SNS.
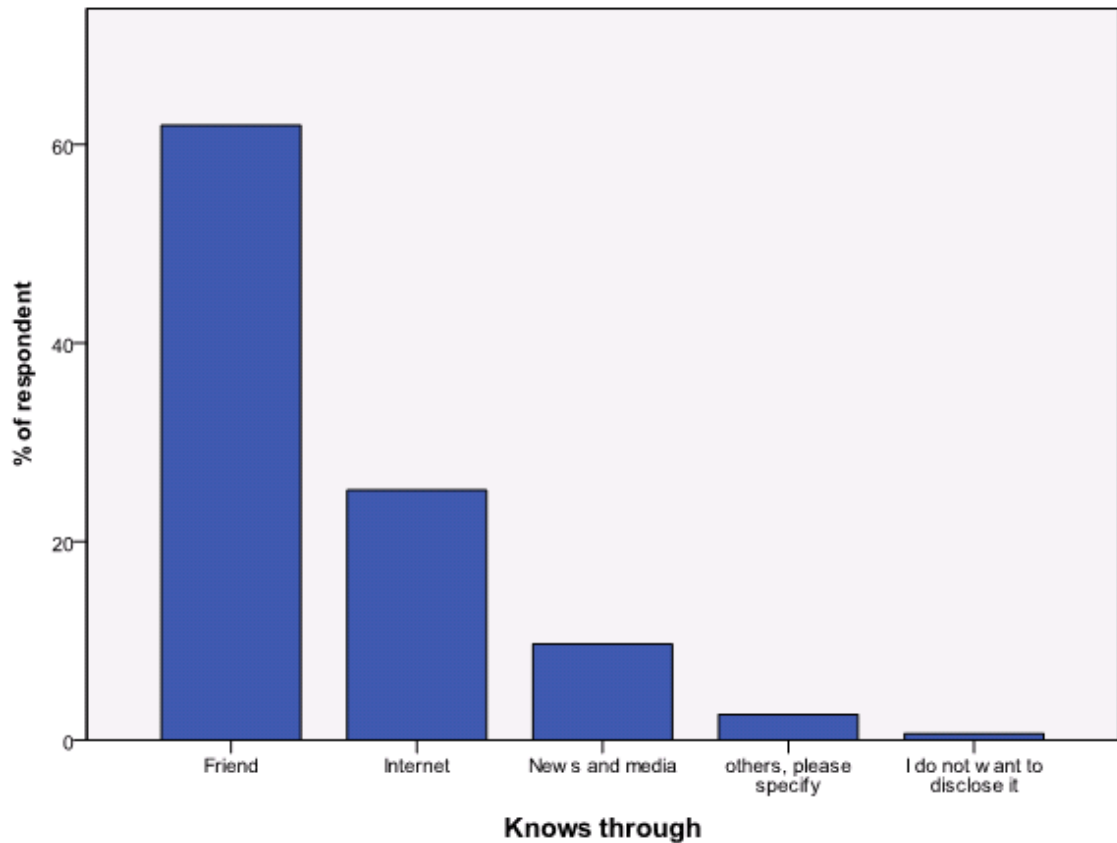
Figure 5.6 Source of original knowledge about SNS

Graphical representation in Figure 5.7 shows that each of the respondents had a number of friends in their network; 27.1% of participants had more than 150 friends in their network in their SNS account; and 23.9% of respondents reported more than 200 friends listed in their SNS account. Of the respondents, 16 % reported they had more than 100 friends listed; 12.9% of users reported that they had less than 100 friend connections; and 9% of users had more than 300 friends listed in their SNS accounts. Less than 2% of all respondents did not want to disclose how many friends they have in their SNS account.
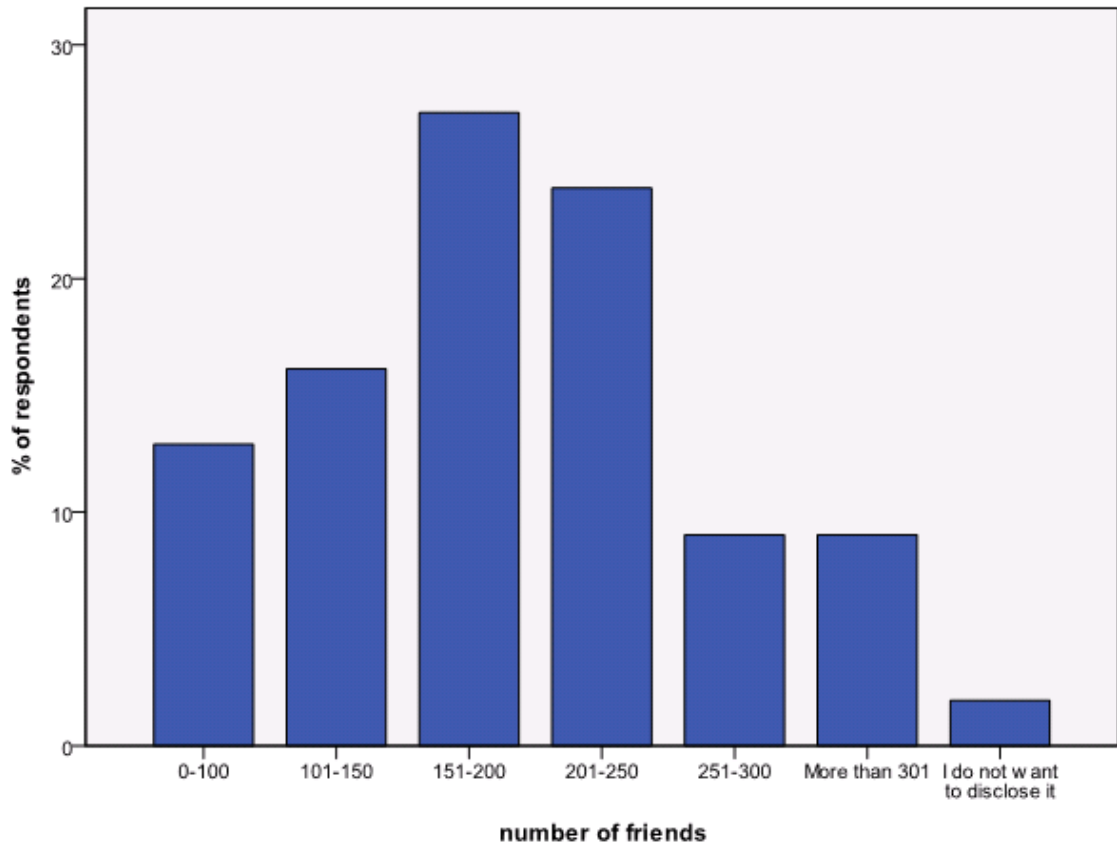
Figure 5.7 Average numbers of friends in each social networking account

Users cited different reasons for visiting SNS, as displayed in Figure 5.8. Most of the respondents (56.1%) used SNS to keep in touch with friends and family; followed by 21.9% of participants who were looking for new friends on SNS. More than 11.6% of respondents used SNS for the purposes of professional or work related tasks. More than 10% of participants used SNS for professional reasons, to socialise or to access the latest news.
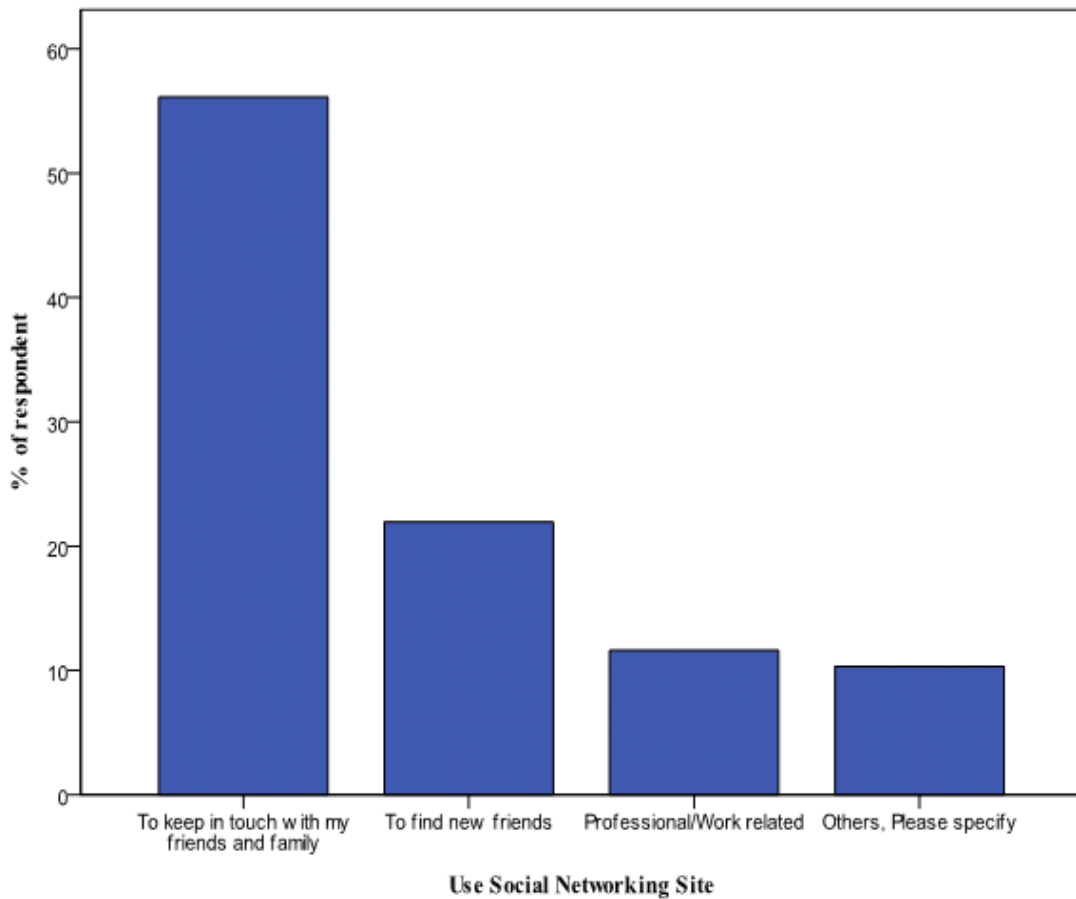
Figure 5.8 Purpose for visiting social networking sites

Figure 5.9 displays graphically the varying levels of education of the questionnaire respondents. From the results, it is clear that 7.7% of respondents had completed a Doctoral degree, 31% reported they had completed a Master's degree; 30.3% had completed a Bachelor's degree; more than 25% reported they had completed a Diploma; and less than 6% reported their highest level of education as the completion of high school.
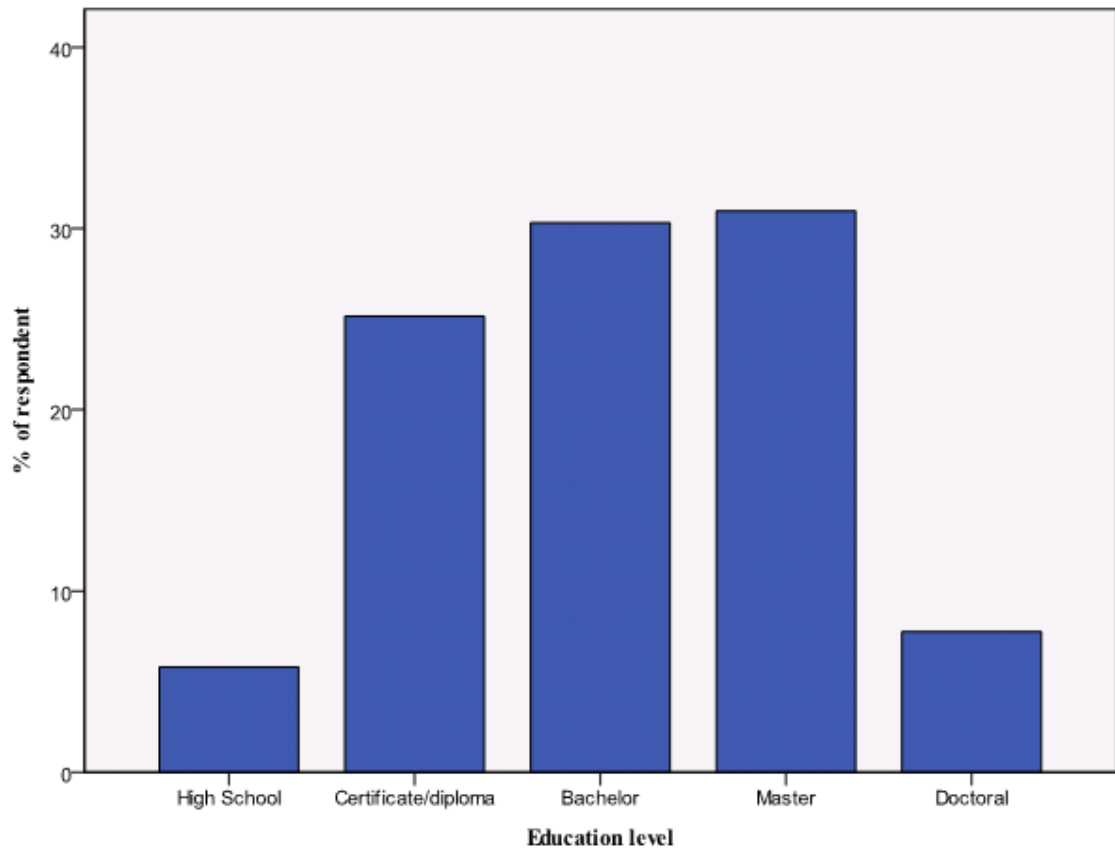
Figure 5.9 Education status of respondents

Other attributes of the respondents that were analysed included their gender, marital status and occupation, as shown in Table 5-1. Of the 155 respondents, 56.1% were married; 40% of participants were single; and 1.9% of participants mentioned that they had a partner or were engaged to be married. However, 1.9% of users did not want to disclose their marital status. The results also analysed the different occupations of the respondents, and the findings were that the majority of participants were students (47.7%), followed by professionals 24.5%, while 12.9% of respondents were from an academic background.

Table 5-1 Characteristics of the respondents

Personal Information	Frequency	Percentage
Gender		
Male	84	54.2%
Female	71	45.8%
Marital status		
Single	62	40%
Married	87	56.1%
Others	3	1.9%
Do not want to disclose	3	1.9%
Occupation		
Student	74	47.7%
Academic	20	12.9%
Manufacturing/construction	1	0.6%
Profession	38	24.5%
Business	6	3.9%
Self-employed	5	3.2%
Retiree	2	1.3%
Others	6	3.9%
Do not want to disclose	3	1.9%

5.3 Confirmatory Factor Analysis (CFA)

The confirmatory factor analysis (CFA) was adapted to verify the adequacy of the item to factor associations and the number of dimensions underlying the construct (Thompson & Daniel 1996). CFA is a way of testing how well measured variables represent a smaller number of constructs (Thompson 2004). One of the biggest advantages of CFA is its ability to assess the construct's validity (Hair Jr et al. 2006).

Validity is defined as the extent to which the research was accurate.

The constructs of SNS experience, privacy concerns, trust and willingness to share digital identities were adopted from previous studies as stated factors; and to further validate the constructs, confirmatory factor analysis was used within structural equation modelling. Confirmatory factor analysis in structural equation modelling gives a more accurate depiction of the relationship between the dimensions since measurement error is taken into consideration (Hair Jr, Anderson, Tatham & Black 1998). The validity and reliability of this research was found to be significant, as shown in Table 5-2. However, this may not be true if the construct and paths are put together in an overall SEM framework. Therefore, a more rigorous method of statistical analysis is used to show the interactions between dependent and independent variables.

Construct validity is made up of three important components, namely, factor loadings, variance extracted, and construct reliability. The standardised loading estimates should be 0.5 or higher and, ideally, 0.7 or higher. With CFA, the average percentage of variance extracted (VE) among a set of construct items can be calculated simply using standardised loadings that are squared before summing them and dividing by the total number of items (N). The measurement of Construct Reliability (CR) is quite similar to the VE where CR is computed from the squared sum of factor loadings and a sum of the error variance for each construct; whereas error variance is calculated by taking one minus factor loading square: the mathematical calculation is shown below (Hair Jr et al. 2006, p. 612).

$$VE = \frac{\sum_{i=1}^{n} \lambda_i^2}{N}$$

Error Variance = 1- λ^2

$$CR = \frac{\left(\Sigma_{i=1}^{n} \lambda_i\right)^2}{\left(\Sigma_{i=1}^{n} \lambda_i\right)^2 + \left(\Sigma_{i=1}^{n} \delta_i\right)}$$

Where λ_i is standardised loadings obtained from each latent construct, N is number of item and δ_i is the measurement of error for each indicator. The measurement error is 1.0 minus the reliability of the indicator, which is the square of the indicator's standardised loading (Hair Jr et al. 2006).

This is in accordance with a suggestion by Hair Jr et al (2006) that the criteria of construct validity are as follows:

i) Standardised loading estimates ≥ 0.5

ii) Variance extracted (VE) ≥ 0.5

iii) Construct reliability (CR) ≥ 0.7

On the other hand, to access overall reliability the Cronbach's alpha coefficient for each dimension and construct was calculated as shown Chapter IV Table 5-2. An alpha score that is greater than 0.70 was considered to be acceptable (Nunnally 1994; Sekaran 2003). The alpha value for each item for this model ranged from 0.816 to 0.906, and all scales had construct reliabilities above 0.7, therefore, data collection for each construct are reliable and have validity for further analysis.

Table 5-2 Reliability statistics

Construct	Cronbach's Alpha	Cronbach's Alpha Based on Standardised Items	Number of Items
SNS Experience	.753	.757	4
Privacy Concerns	.816	.817	5
Trust	.881	.882	11
Willingness to share digital identity	.906	.911	13

Details of the measurement for each construct item are separately tested by the CR, VE and alpha value in order to check the reliability and validity of data (see Appendix E). Item values of less than 0.7 are considered as unreliable for study so these items are deleted and the items with higher than 0.7 (listed in Table 5-3) are considered for further data analysis.

The results of CFA for all variables are shown in Table 5-2. Construct *privacy* has one factor with five items (PC1, PC2, PC3, PC4, PC5) with factor loadings of .61, .67, .77, .75 and .63 respectively as shown in Figure 5-10. CR for privacy is greater than 0.7 so values are adequate for this study.

The construct *trust* has also one factor with 11 items (T1 to T11) where most of the items have a factor loading of more than 0.7, although some items had a factor loading of less than 0.5 and these items have been deleted and left for future research. VE and CR for the *trust* construct were higher than 0.5 and 0.7 respectively.

The construct 'willingness to share digital identities' has one factor that consists of thirteen items (DI1 to DI13) for which the factor loading is shown in Table 5-2. VE and CR for this factor are higher than 0.5 and 0.7 respectively.

The construct 'SNS experience' consists of one factor with four items (SK1 to SK4) with factor loadings .76, .71, .66, .70 respectively. CR is greater than 0.7. Details of the statistical table SPSS output are attached in Appendix E.

Table 5-3 Convergent validity of the model variables

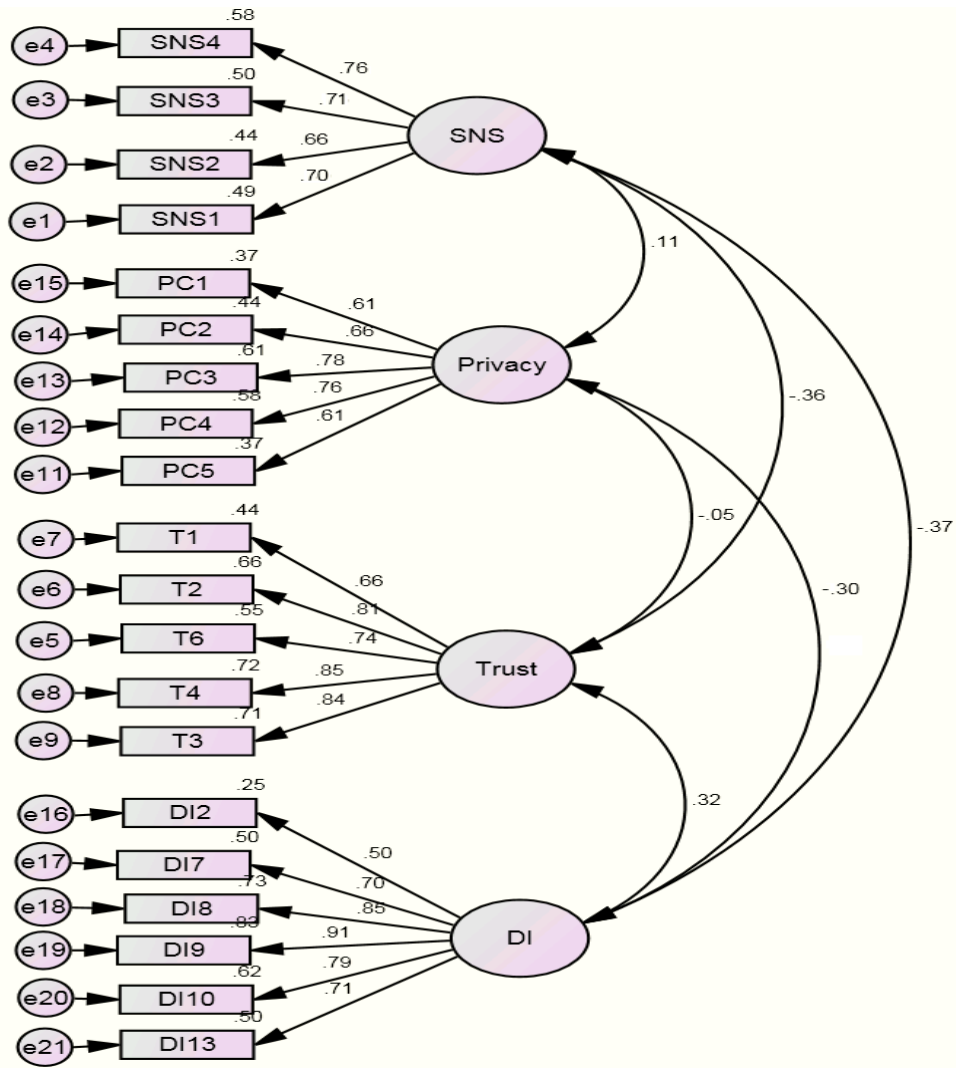| Factor	Items	Standardised Factor Loadings	Corrected Item Total Correlation	VE	Cronbach's Alpha If Item Deleted	CR
	PC1	0.61	0.564		0.793	
	PC2	0.66	0.612		0.779	
Privacy concerns	PC3	0.78	0.652	0.480	0.767	0.816
	PC4	0.76	0.636		0.771	
	PC5	0.61	0.573		0.791	
	T1	0.66	0.620		0.884	
	T2	0.81	0.769		0.846	
Trust	T3	0.84	0.762	0.614	0.848	0.886
	T4	0.85	0.789		0.843	
	T6	0.74	0.678		0.868	
	SNS1	0.76	0.732		0.710	
SNS experience	SNS2	0.71	0.690	0.510	0.705	0.707
	SNS3	0.66	0.648		0.701	
	SNS4	0.70	0.685		0.707	
	DI2	0.50	0.468		0.892	
	DI7	0.70	0.633		0.852	
Willingness to share digital identity	DI8	0.85	0.777	0.567	0.827	.869
	DI9	0.91	0.823		0.821	
	DI10	0.79	0.737		0.833	
	DI13	0.71	0.663		0.850	

Figure 5.10 Measurement fit model (Source: The Author)

5.4 Dimensional Level Analysis – The Measurement Model

To further validate the constructs, confirmatory factor analysis was used within structural equation modelling. Confirmatory factor analysis in structural equation modelling gives a more true relationship of the dimensions since the measurement error is taken into consideration (Hair Jr et al. 2006).

According to Anderson and Gerbing (1988), the measurement model specifies how the latent variables or hypothetical constructs are measured in terms of the observed

variables, taking into account specification error. Before starting on testing the proposed measurement models for each construct, various fit indices need to discussed. Although there are number of fit indices, Maruyama (1998) argued that there is no single test that best describes the fit of a model. He categorises fit measurement as corresponding with three types: absolute, relative and adjusted indexes.

Absolute Fit indexes provide information about how closely the model fits compared to perfect fit (Maruyama 1998). This can be measured mainly by χ^2 (chi-square) test. A low χ^2 value, which would have a p-value greater than 0.05, indicates that the actual and predicted values are not significantly different. Another index, relative fit index, also known as Comparative Fit Index (CFI), is a measure of how the model compares with other possible models with the same data (Maruyama 1998). CFI provides an estimate of the model's relative misfit to a baseline model. Higher numbers indicate a lower misfit. Normed Fit Index (NFI) also compares the theoretical model to a baseline model. A recommended value of fit for both NFI and CFI is 0.90 and a model will be marginally fit at greater than 0.8 (Hair Jr et al. 2006).

Another index is Goodness of Fit Index (GFI) that tells that proportion of the variance in the sample variance-covariance matrix is accounted for by the model. This should exceed 0.9 for a good model and 0.8 for marginal fit. For the full model, a perfect 1 would be recommended. AGFI (Adjusted GFI) is an alternate GFI index in which the value of the index is adjusted for the number of parameters in the model. According to Etezadi-Amoli and Farhoomad (1996) for a good model AGFI should be greater than 0.8 and near to GFI.

Another fit statistic is the Root Mean Square Error of Approximation (RMSEA), as a measure of fit. Joreskog and Sorborn (1996) suggests that a value of the RSMEA of about 0.06 or less would indicate a close fit of the model in relation to the degrees of freedom although this figure is based on subjective judgement and cannot be regarded as infallible (Arbuckle 2006, p. 496; Shin 2010a).

The following Table 5-4 shows the details of the Confirmatory Factor Analysis in the structural equation model. To determine the best-fitting model, this study used the chi-square difference tests as well as the Comparative Fit Index. Bagozzi and Edwards (1998) have made the suggestion that the CFI was particularly useful for a small sample size because it, unlike the chi-square statics, operates independently of sample size. Table 5-4 represents the result of Goodness of Fit Indexes of the Measurement Model. The Model Fit Index values prove the model is fit where the chi-square/d.f (χ^2/df) is less than 5, GFI and CFI have met the acceptance criteria.

Table 5-4 Goodness of Fit Indexes of the Measurement Model

Fit Indexes	Criteria	Indicators	Acceptability
Chi-Square (χ^2)	>0.05	238.378(.000)	Acceptable
Chi-Square/d.f (χ^2/df)	<5.00	1.454	Acceptable
Goodness of Fit Index (GFI)	>0.90	.867	Marginal
Adjusted GFI	>0.80	.829	Acceptable
Comparative Fit Index (CFI)	>0.90	.939	Acceptable
Normed Fit Index (NFI)	>0.90	.831	Marginal

Fit Indexes	Criteria	Indicators	Acceptability
Incremental Fit Index (IFI)	>0.90	.941	Acceptable
Tucker-Lewis coefficient (TLI)	>0.90	.930	Acceptable
Root Mean Square Error of Approximation (RMSEA)	<0.06	.054	Acceptable

5.5 Descriptive Statistics and Correlation for All Variables

Table 5-5 shows the means, standard deviations and correlation matrix for all variables of the research models that contain privacy concerns, trust, SNS experience and willingness to share digital identities.

Based on the data shown in Table 5-5, it is suggested that for the construct of privacy concerns, respondents tend to perceive a relatively higher degree of agreement where the mean value for privacy concerns is 5.16 in a 7-point Likert scale. These results indicate that the respondents have high levels of privacy concerns. In addition, for the construct of trust in SNS, respondents have neutral level of agreement on the measurement factors with a mean score 4.52. This indicates that users have relatively high levels trust of with SNS and with its users. The results of SNS experience scored over 3, which indicates that respondents were using SNS for over 5 years and using SNS at least once a day. The construct of willingness to share digital identity had a mean score of 4.88 which indicates that in 7 point scale, the respondents had a low level of intention to share all aspects of their digital identities in SNS.

Table 5-5 Descriptive Analysis and Correlation

	Mean	Std Dev	Correlation			
			Privacy	Trust	Identity	SNS Experience
Privacy	5.16	1.083	1			
Trust	4.52	.955	-.035	1		
Identity	4.88	1.136	-.336[**]	.360[**]	1	
SNS Experience	3.82	.893	-.038	-.089	-.033	1

** Correlation is significant at the 0.05 level (2-tailed).

5.6 Structure Equation Modelling (SEM)

The major purpose of using SEM is to test and estimate the relationships between research constructs and to provide estimates of the strength of all hypothesised relationships between variables in the theoretical model (Anderson et al. 1988). A Structural Equation Model (SEM) can provide information about hypothesised impact, both directly from one variable to another, and also indirectly through other variables (Maruyama 1998). Additionally, Baumgartner and Homburg (1996, p. 141) argued that using structural equation models can be specified to investigate measurement issues to examine structural relationships among sets of variables or to accomplish both purposes simultaneously. The use of SEM for this research is to confirm the hypothesised paths and overall fit of the theoretical model.

There are two distinct parts of SEM: measurement model and structural model (Maruyama 1998). The structural model defines relationships between the unobserved variables. The constructs or unobserved variables for this study have been statistically validated through measurement model as shown in previous section (Fig 5-10), and as such the model that will be used in this section is the structural model. To analyse this SEM, we used SPSS AMOS 19 software for data analysis purpose and details of the output of AMOS is shown in Appendix - E.

Importantly there are several Goodness of Fit measures that can be used to assess the outcome of SEM analysis, they include the Root Mean Square Error of Approximation (RMSEA) which is based on chi-square values and measure the discrepancy between observed and predicted values per degree of freedom (a good model has an RMSEA value of less than 0.06) (Joreskog et al. 1996; Shin 2010a); the Comparative Fit Index (CFI), which compares proposed model with baseline model with no restrictions (a good model should exhibit a value greater than 0.90) and Goodness of Fit measures, which compare the sample and model implied variance covariance matrices such as the standardised root mean square residual (SRMR) and a value less than 0.08 (Bentler 1990; Shin 2010a) is considered as a good fit. The adjusted goodness of fit index (AGFI) considered the greater the value better. Moreover, the main criteria for SEM are the following:

Chi-square value should be higher than 0.05

Chi-square/ degree of freedom should be smaller than 2

Goodness of Fit Index should be higher than 0.80

Root Mean Square of Standardised Residual should be smaller than 0.060

Furthermore, based on the standardised structure equation model (Figure 5.11) overall Goodness of Fit Indices and path coefficient are shown in Table 5-6 and Table 5-7 respectively.
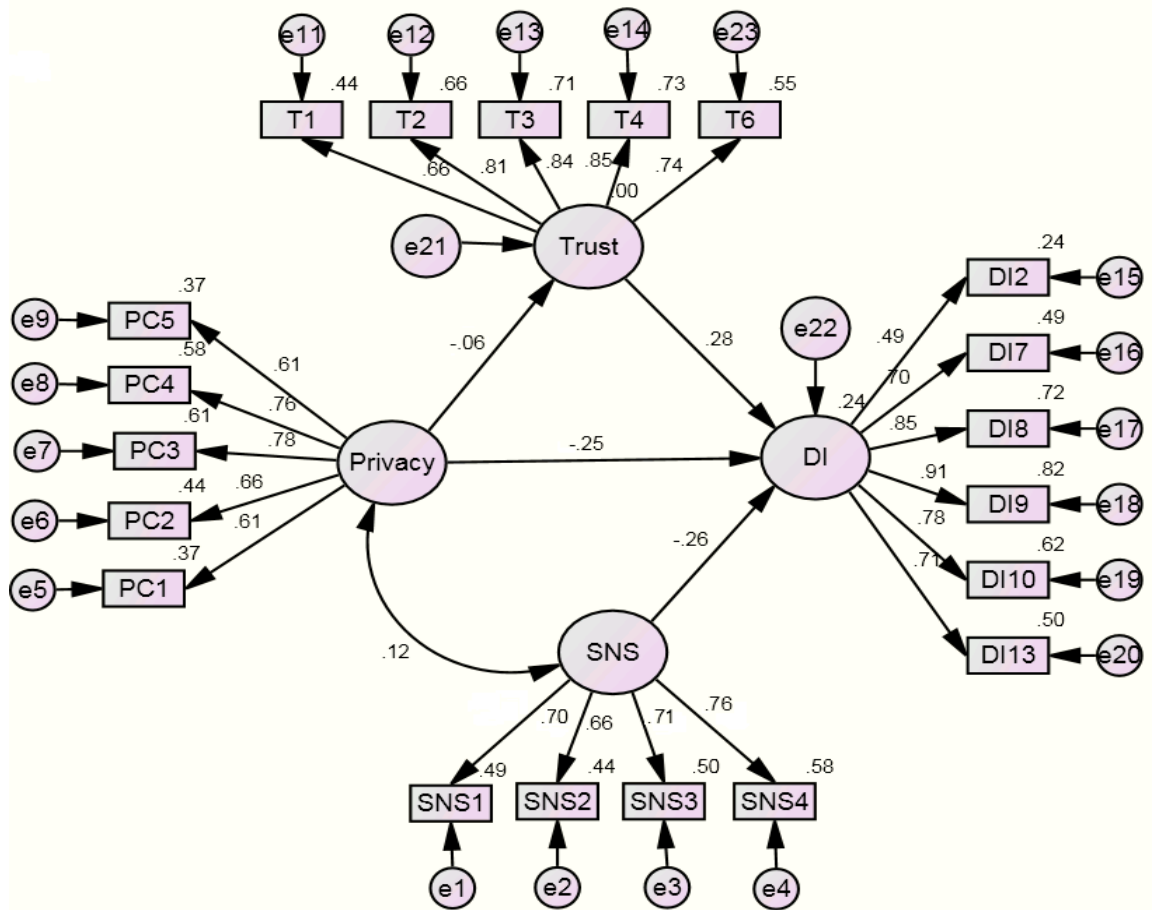
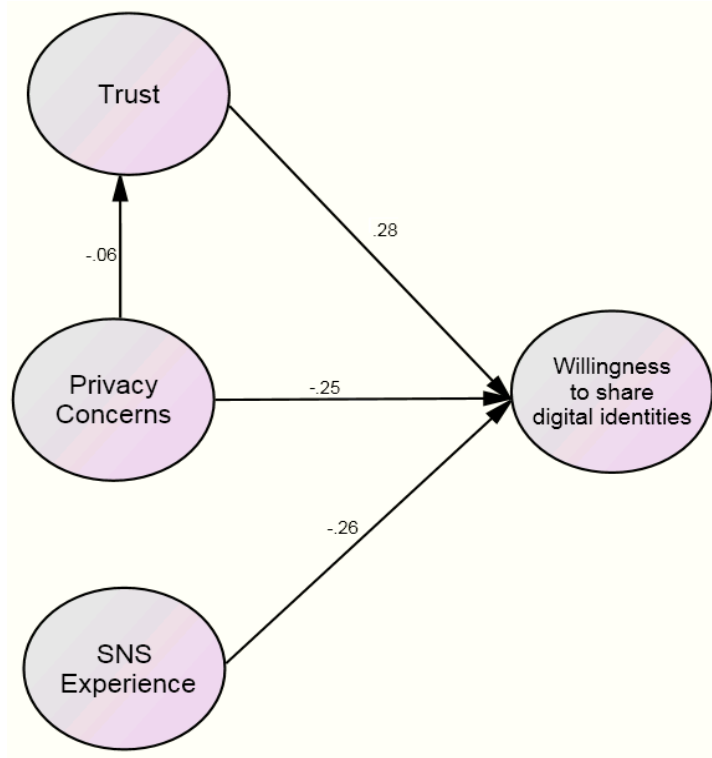**Figure 5.11 Standardised Structure equation model path diagram (Source: The Author)**

Figure 5.12 Final Structural equation model of impact of privacy concerns and trust in SNS for willingness to share digital identities (Source: The Author)

Table 5-6 Goodness-of-Fit indices of structural model

Fit Indexes	Criteria	Indicators	Acceptability
Chi-Square (χ^2)	>0.05	243.770(.000)	Acceptable
Chi-Square/d.f (χ^2/df)	<5.00	1.477	Acceptable
Goodness of Fit Index (GFI)	>0.90	.865	Marginal
Adjusted GFI	>0.80	.828	Acceptable
Comparative Fit Index (CFI)	>0.90	.936	Acceptable
Normed Fit Index (NFI)	>0.90	.828	Marginal
Incremental Fit Index (IFI)	>0.9	.937	Acceptable
Tucker-Lewis coefficient (TLI)	>0.9	.926	Acceptable
Root Mean Square Error of Approximation (RMSEA)	<0.06	.056	Acceptable

5.6.1 Overall Model Fit

According to Bentler (1990; 2007, p. 827) and Jorsekog and Sorbom (1996) GFI, AGFI, RMSEA, IFI and TLI are useful for describing the best fit model. The result represented in Table 5-6 shows that the Chi-square value of this research model is 243.770 with degree of freedom 165 significant at <0.001. Table 5-6 shows the details of goodness of fit indices for structural model where Chi-square/ d.f is 1.477 that is less than 5. GFI value is .865, according to Hair Jr et al (2006) greater than 0.8 is marginal acceptance, to become best fit GFI should be >0.90 and AGFI >0.80 (Etezadi-Amoli et al. 1996; Shin 2010a). The model also supports the CFI is 0.936 and NFI is 0.828 which must be greater than 0.9 for a best fit and greater than 0.8 for

marginal acceptance according to Hair Jr et al (2006). The model has also get a better RMSEA value as shown in Table 5-6 which is 0.053 and value of RMSEA should be less than 0.06 according to Joreskog & Sorborn (1996); and Bentler (1990) respectively. The incremental fit index (IFI) and Tucker-Lewis index (TLI) has values greater than 0.9, which indicates higher levels of Goodness of Fit. Overall the results of Goodness of Fit indicate that the model was a good fit.

5.6.2 Path Results

Table 5-7 Path Coefficients for structural model

	Estimate	S.E	Critical Ratio	p
SNS experience → Willingness to share digital identities	-0.257	1.101	-1.021	.307
Privacy concerns → Willingness to share digital identities	-0.255*	.109	-2.474	.013
Trust → Willingness to share digital identities	0.282**	.089	2.962	.003
Privacy concerns → Trust	-0.058	.166	-2.108	.536

Note: * p< 0.05, **p<0.003

To test the research hypothesis, path analysis is performed using AMOS 19 software tools and based on the SEM of this study there are four paths and the details of the path analysis and strength of the relationship between constructs are shown in Table 5-7 and based on this results, the summary of testing of the hypothesis is shown in Table 5-8. This study has established four hypotheses: dependent relationships were established between the constructs of privacy concerns, trust, SNS experience and willingness to share digital identities and out of the four, two hypotheses were found to be supported.

According to Hair Jr et al (2006), to support the hypothesis each path should be significant at level of 0.005 and its C.R. must be greater than 1.96. No significant relationship was found between SNS experience and willingness to share digital identities, so there is a weak relationship and, therefore, hypothesis (H1) was not supported for this study—which would suggest that the SNS experience does not influence people's willingness to share digital identities on SNS. Also, there is no significant difference between privacy concerns and trust; moreover, there is very low standardised estimated path coefficient for the relationship between privacy and trust. So, this finding strongly rejects the hypothesised relationship between privacy concerns and trust. However, some previous studies have shown that there must be a relationship between them in order for them to share information. This will be discussed in detail in the next chapter. All of the paths between other variables have shown that they are strongly significant and C.R. are higher than 1.96 which means that all the hypotheses implemented under this path are supported by this study.

Table 5-8 Results of hypotheses testing

	Hypothesis	Results of study
H1	Users with high levels of SNS Experience will be more willing to share digital identities	Not supported
H2	Users with higher level of privacy concern has lower level of trust in SNS.	Not Supported
H3	Users with higher level of trust will be more willing to share digital identities in SNS.	Supported
H4	Users with higher levels of privacy concerns will be less willing to share digital identities.	Supported

5.7 Conclusion

A great deal of analysis has been undertaken in this chapter of the responses to the questionnaire questions. These results have been verified and tested, and then presented in this chapter. The analysis has focused on reliability analysis, factor

analysis and structural equation model of this study. To test reliability, the Cronbach's alpha test was run for which the results need to be greater than 0.7 and the findings show that most of the items are reliable for this study. The researcher also calculated variance, for which the data extracted must be greater than 0.5 and these findings were significant for this study. Confirmatory Factor Analysis for each variable with a loading factor greater than 0.50 were used for the analysis, and those with a result below 0.50 loading factor were deleted. The different types of Goodness of Fit indices were conducted to measure the fitness of model such as GFI, AGFI, CFI, NFI, IFI, TLI and RMSEA.

The value of AGFI, CFI, IFI, TLI and RMSEA are respectively .828, .936, .937, .926 and .056, which indicates that the model is a better fit. The GFI and NFI has a value .865 and .828 respectively, which are at the marginal acceptance level.

The outcome of measurement model is acceptable and the main purpose of SEM was the testing of the proposed hypothesis stated in Chapter III, and hypotheses were tested using path analysis. Estimation values show that the extent of SNS experience has a negative impact upon users' willingness to share digital identities. Similarly, privacy concerns have negative effects on trust and willingness to share digital identities. However, trust is shown to have a positive effect on willingness to share digital identities. The results show that two hypotheses are fully supported, while two hypotheses could not be supported.

All of the analysis was aimed at understanding the impact of privacy and trust on users of SNS in sharing digital identities. The following chapter provides a

discussion of the implications of accepting and rejecting hypotheses in terms of the findings of the path analysis, as well as an examination of the limitations of the study and suggestions for areas of further research.

Chapter VI: Conclusion

6.1 Introduction

This chapter will discuss the findings associated with the statistical analysis of the hypothesised relationships of the research model for this study. Each of the hypotheses developed in Chapter III will be reviewed, followed by a subsequent discussion of the findings. It should be noted that the Kline (2010) method has been used to discuss the impact of privacy concerns and trust on using SNS. That is, if the absolute value of the standardised path coefficient in an structural equation model is less than .10, this will indicate a 'small' impact, while a coefficient of around .30 will indicate a 'medium' impact, and a coefficient greater than .50 will indicate a 'large' impact.

This study shows that there is an impact of privacy concerns, trust and SNS experience upon the willingness of SNS users to share information. However, there is a positive and negative effect between different variables.

This study carried out analyses of four different types of relationships, namely, privacy concerns, trust, SNS experience and willingness to share digital identities in SNS. The literature confirms that users with high levels of Internet experience have more confidence, and are willing to share more information; and for those with low levels of experience, the opposite was found to be true. The following sections discuss these findings in more detail, including the possible limitations of the study and suggestions for future research.

6.2 Summary of the study

This section provides a summary of the research problem and general research question investigated in this study, the research hypotheses which were tested, and the research method used in this study. The key findings of descriptive demographic data analyses and hypotheses testing are then summarized.

6.2.1 Research problem

Dwyer, Hiltz and Passerini (2007) found that privacy concerns and trust were major issues for users of SNS. As the world has become more digitised, protection of the privacy of the user has become more complicated. Nysveen and Pedersen (2004) found that privacy concerns in SNS were similar to those found for users of electronic commerce in terms of concerns by users about providing personal information. Pavlou and Fygenson (2006) established that customers who were using SNS and online business transactions were worried about their personal data regarding its security and privacy, however, their research suggests that customers conducting online business transaction are more concerned about their privacy in this domain than in sharing the same personal information on SNS. Furthermore, they suggest that despite their concerns about security, users remained willing to share their personal information within SNS. However, these researchers were unable to justify the reasons why users were more willing to share their personal information within SNS.

Previous studies conducted by Lo (2010) on privacy concerns in SNS suggest that knowledge and experience may affect the perception of users about privacy issues as they relate to the sharing of personal information. However, his study did not justify

whether users' SNS knowledge and experience play critical role to influence users' privacy concerns and trust to share personal information in SNS.

Moreover, very few previous studies have investigated privacy concerns and trust in e-commerce (e.g. Lio 2005)—which is almost a similar concept to SNS—or on how the users' privacy concerns and trust impact on sharing users' identities on SNS. Based on the research problem the main research question of this study is:

To what extent do privacy concerns and trust influence users' willingness to share information about their digital identity within Social Networking Sites?

Therefore, the main research objectives that underpin the general research question of this study are:

❖ To examine the impact of users' experience with SNS upon their willingness to share their digital identities.

❖ To examine the influences of privacy concerns as they relate to the trust needed for users to share their digital identities within SNS.

❖ To examine the influence of trust about SNS upon users' willingness to share their digital identities.

❖ To examine the impact of privacy concerns upon the willingness of users of SNS to share their digital identities.

6.2.2 Research hypotheses

The four hypotheses were formulated from the four research questions above after being justified and grounded in the existing relevant literature on SNS experiences

and knowledge, privacy concerns, trust and willingness to share digital identities. The four hypotheses are as follows:

H1: Users with high levels of SNS experience will be more willing to share digital identities.

H2: Users with higher levels of privacy concern have lower levels of trust in SNS.

H3: Users with higher levels of trust will be more willing to share digital identities on SNS.

H4: Users with higher levels of privacy concerns will be less willing to share digital identities.

These four hypotheses test how the users' SNS experience and knowledge, privacy concerns and trust will impact on sharing the users' digital identities in SNS.

6.2.3 Research Methodology

This is explanatory research using a quantitative approach to test the research model which examines the relationship between the independent variables such as SNS experiences and knowledge, privacy concerns and trust; and the dependent variable willingness to share digital identities. For the purpose of this study, data is collected from Facebook Forum users where the numbers of registered users are publicly available in the forum and the total numbers of participants in the online survey were 169 users. Facebook Forum is a community forum where users are able to share, discuss and comment on anything related to Facebook or other SNS such as a new SNS feature, its advantages and disadvantages, an application, games, new privacy settings, scams, photos, videos, events, and numerous other general topics where users can request help. There are also forum contests, general chat areas and an

interactive Chatbox, where online members gather to chat together in real-time (Forum 2011). Facebook Forum was selected for this study because it is a subset of Facebook and it will improve the credibility of the results because participation includes users from different backgrounds including application developers, professionals, students and social workers, which can represent a much broader population of SNS users.

6.2.4 Conclusions about descriptive demographic data

Of the 155 respondents to the survey, 54.2% were male and 45.8% were female. A total of 81.95% of participants were aged between 18-40, while 16% were more than 40 years of age. From this background of age, it can be seen that most of the participants were young; and 47.4% participants were students—with the remainder involved in various professions or other categories (see Table 5-1). A total of 96% of participants were concerned about their privacy with 76.1% of participants modifying their privacy settings; however, only 35.5% had read about privacy policies or terms and conditions of social networking sites.

6.2.5 Conclusions about SEM model fit

The different types of Goodness of Fit indices were conducted to measure the fitness of model such as GFI, AGFI, CFI, NFI, IFI, TLI and RMSEA. The value of AGFI, CFI, IFI, TLI and RMSEA are respectively .828, .936, .937, .926 and .056, which indicates that the model is a better fit. The GFI and NFI has a value .865 and .828 respectively, which are at the marginal acceptance level. The outcome of measurement model is fit and the main purpose of SEM was the testing of the proposed hypothesis stated above, and hypotheses were tested using path analysis.

6.2.6 Conclusions concerning Results of Research Hypotheses Tests

H1: Users with high levels of SNS experience will be more willing to share digital identities.

The validity and reliability of four dimensions of the construct SNS experience were found to be significant, as shown in Chapter V. However, this did not prove to be true when the construct and paths were put together in an overall comprehensive framework as shown in Figure 5-11 (Chapter V). The 'p' value between SNS experience and willingness to share digital identities was not found to be significant. As such, the structural equation model did not support this hypothesis. However, the results of path estimations show that there is negative relationship between individual users' SNS experiences and the sharing of their digital identities.

A plausible explanation for this result could be found when it is considered that the majority of SNS users were university students and were aged under 30 years (54%)—which shows that this is the age at which users were influenced by friends (more than 60%) and were susceptible to peer pressure.

The rejection of this hypothesis is, however, consistent with the problems inherent in the successful measurement of SNS experiences, which has not kept pace with theoretical developments. Novaka, Hoffman and Yung (2000) argued that Internet experiences were usually defined as general experience with Web sites and not as experiences with one particular Web site. Prior experience has been found to be an important determinant of behaviour. Long term experience effects and changes the behaviour of the user according to Ajen and Fishbein (1980). The statistical analysis of the study shows that the majority of respondents had just started using SNS during

the last four years, which indicated that respondents had less SNS experience. Moreover, the negative value of estimated path coefficient shows that the SNS experience has a negative effect on willingness to share digital identities.

H2: User with higher level of privacy concern has lower level of trust in SNS.

The validity and reliability dimensions of the construct were found to be significant. The path analysis result shows that there is no significant (p <0.005) effect between privacy concerns and trust, but the C.R. is greater than 1.96, which shows the hypothesis is partially supported by the study results. However, there is no significant result found between privacy concerns and trust; and, additionally, there is very low standardised estimated path coefficient for the relationship between privacy and trust. Thus, this finding strongly rejects the hypothesised relationship between privacy concerns and trust. The negative value estimations on path analysis show that if the user has high privacy concerns, then they have low trust and vice-versa, which is a logical outcome. Protections of privacy, as well as the mechanism to protect trust, are critical to designers and developers of SNS systems, according to Joinson, Reips, Buchanan and Schofield (2010). According to Grewal, Munger, Iyer and Levy (2003), privacy policy statements appear to be most beneficial to the web developer who is seeking to increases users' trust (Meinert, Peterson, Criswell & Crossland 2006b). However, this study's findings are inconsistent with previous findings by Liu et al (2004) which found that privacy concerns had positive impacts on trust in electronic commerce.

H3: Users with higher levels of trust will be more willing to share digital identities on SNS.

There is a strong significant relationship between trust and willingness to share digital identities on SNS. As a result, the reliability and validity dimensions of the construct were found to be significant, and also the path estimations between two constructs were found to be significant at p < 0.003 and C.R. is greater than 1.96. As such, the structural equation model strongly supports this hypothesis.

This statistical result suggests that high levels of trust in SNS by users had the effect of heightening the probability that users would be willing to share digital identities on SNS. The business market research conducted by Grayson and Ambler (1999) found that trust has a central role in building long–term relationships with their clients. Also, some of the findings regarding trust and identity sharing in this study are consistent with prior findings. For example, studies by Lo et al (2010), Dwyer at al (2007) and Fogel and Nehmad (2009) found that trust has a positive impact on users. Thus, this finding suggests that users will share more information on SNS if they have a high level of trust in SNS.

H4: Users with higher levels of privacy concerns will be less willing to share digital identities.

Concerns about privacy have a strong impact upon users' willingness to share identities, and this impact is statistically significant, as shown in Figure 5-11. The path analysis shows that there is a significant path (p<0.05) and C.R. is greater than 1.96, which indicates that the structural equation model strongly support this hypothesis for this study. Also, reliability and validity dimensions of the construct

were found to be significant, which makes the structural equation model fit for this study. Additionally, the strong negative impact of estimation path results show that high levels of privacy concerns make users less inclined to share digital identities on SNS, and low levels of privacy concerns create a high level of willingness to share digital identities on SNS. However, the findings of this study are inconsistent with a prior finding about privacy concerns by Metzger (2004), but the finding is consistent with Lo et al (2010). However, unlike Lo et al (2010), this study has found that there is a significant relationship between privacy concerns and users' willingness to share digital identities.

6.3 Contribution of Study

This research study makes several practitioner contributions, especially for the literature, SNS developers and users. The researcher summarises the contributions and implications to practitioners as follows:

6.3.1 Contributions to the Literature

This study provides at least two contributions to the literature. Firstly, it provides a better understanding and new insights into privacy concerns and trust, and their effect on users' willingness to share their digital identities on SNS. Secondly, this study will enrich existing literature regarding user experiences and knowledge of the Internet, especially in relation to SNS's effect on users' willingness to share identity information. In addition, this study also shows the relationship between trust and privacy.

Furthermore, from the analysis of results, it can be seen that the extent of users' SNS experience and knowledge has a negative effect upon their willingness to share digital identities. Similarly, users with higher levels of privacy concerns were less willing to share digital identities. Finally, users with higher levels of trust had a more positive disposition towards their willingness to share digital identities.

6.3.2 Contributions for SNS Users

This study contributes practical knowledge for social networking site users and developers. SNS users have different approaches to sharing identity information, with the results of this study demonstrating that users with high levels of privacy concerns were less willing to share digital identities and vice-versa. Similarly, trust is another important factor that impacts upon their likelihood of sharing information. This study shows that users with high levels of trust were always willing to share digital identities without concerns. At the same time, users' SNS experience and knowledge were important factors in determining their willingness to share information on SNS. This study suggests that SNS users' identities need to be safeguarded in order to maintain their own privacy, and users need to choose carefully the identities they want to share. It is recommended that users should read the privacy policies and term and conditions of SNS before they join and share their private information.

6.3.3 Contribution to SNS Developers

From the literature of this study it can be seen that millions of people are using SNS daily—and for varying purposes. Different people have different experiences and knowledge, which can be deciding factors that govern their willingness to share identities on SNS. It can also be seen that higher privacy concerns of users have

negative effects upon their willingness to disclose personal information, however, trust has a positive effect upon their willingness to share digital identities on SNS. This statement suggests that SNS developers need to develop easy-to-understand privacy policies and control settings for general users that increase the level of trust that users feel about their participation in SNS.

6.4 Limitations of the Study and Future Research Opportunities

As in all research there are several limitations of this dissertation. The findings are limited by certain choices and by the inevitable constraints imposed on the researcher by circumstances during the time that this project was being conducted. Nevertheless, some of the limitations discussed in this section have led the researcher to perceive further opportunities for study in this area. A number of the limitations of this study, as discussed in the sections below, point to research opportunities and guidelines for future research.

First, there were limitations on data collection techniques used, sampling issues and the time taken for data collection. Despite efforts to collect the data from different sources, data could only be collected from one SNS, namely Facebook. The consequences for this research of this outcome were that it limited the researcher's ability to compare the experience of the respondents' use of Facebook with users of other SNS. As such, an opportunity exists for further research to take the results of this study and cross-compare them with results harvested from responses of users of other SNS.

Second, there were concerns about the time taken for data collection. Because of

various constraints and the need to contact different owners and administrators of different forums, it took two months to collect the data. The collection of the data was dependent on the permission provided by the forum users and, because of the voluntary nature of the survey, a great number of users ignored the links. This limitation might be overcome if the survey was conducted by a different organisation, such as a college or university. This could present a research opportunity in the future to collect data because, from the research conducted for this study, it became obvious that most of the SNS users were students, so there is an opportunity for a more comprehensive data capture that might be organised under the auspices of a university, college or similar institution.

This study conducted a survey with a mass population, and the sample used did not include individuals in equal proportions based on demographical characteristics of choice. This distribution may well increase the chance of bias in data collection and, therefore, another recommendation for a further area of research might be the distribution of a similar survey to a generalised population in a specific area for data collection—which may yield different results. This may well provide a good opportunity for further studies at a higher level.

Moreover, further research could focus on different aspects of trust that impact upon SNS users' willingness to share their digital identities, for example, useful further exploration could be made of the degree of sharing of information that takes place between friends, as compared with the level of sharing between users whose only connection to each other is via SNS.

Additionally, in general terms it is always mentioned that knowledge and experience

have an effect upon any decisions, whereas in this study it is shown that SNS experience does not really impact on users' willingness for sharing digital identities. In this scenario it will be preferable to collect data for qualitative data analysis by conducting focus groups and expert interviews for further investigation to further explore the findings.

6.5 Summary

The goal of this study was to develop a groundwork model of privacy and trust-based users' willingness to share digital identities on SNS to explain the impact of these factors on using SNS. For this purpose, this study developed a conceptual model describing the privacy and trust based decision-making process and tested the proposed model using a structural equation modelling technique on SNS user behaviour data collected via a web survey. The result helps in understanding users' attitudes and the intentions of SNS in terms of the management of privacy concerns and trust dimension; and assists in clarifying the implications for the development of effective SNS services and application. The results of the measurement and structural model tests lend support to the purposed research model. The structural model provided a good fit to the data and most path coefficient in the model were found to be statistically significant.

The major findings of this study are that if users have a high level of trust in SNS, then they are much more willing to share digital identities on these sites. At the same time, privacy is another major factor that impacts upon trust and willingness to share digital identities. The results show that if users' privacy concerns have a negative effect towards trust, they are less willing to share digital identities. Finally, this study suggests that user privacy concerns are the major reason effecting users' willingness

to share digital identities.

This study has made a major contribution towards the literature by providing a better understanding and new insights into privacy concerns; as well as trust and its effect upon users' willingness to share their digital identities on SNS. This study also contributes to knowledge of SNS users and developers regarding privacy concerns and how this impacts upon sharing digital identities on SNS. Finally, this study experienced some limitations in terms of methodology for collecting data and sample size, where a forum was used to collect data, for which the results might vary when compared to data collected from a more generalised population sample of SNS users. There are great opportunities for further study by researchers via the collection of data using different methodologies, such as collecting data from different sources (e.g., universities, colleges and institutes). Also, there are other opportunities for further study to develop current understanding of the direct effect of user knowledge and experience upon privacy concerns and trust as it relates to users of SNS.

References

Ahn, GJ, Ko, M & Shehab, M 2008, 'Portable User-Centric Identity Management', paper presented to The IFIP TC 11 23rd International Information Security Conference, Milano, Italy, September 7-10,2008.

Ahn, Y-Y, Han, S, Kwak, H, Moon, S & Jeong, H 2007, 'Analysis of topological characteristics of huge online social networking services', paper presented to 16th international conference on World Wide Web, Banff, Alberta, Canada, May 8–12, 2007.

Ajzen, I 1991, 'The theory of planned behavior', *Organizational behavior and human decision processes*, vol. 50, no. 2, pp. 179-211.

Ajzen, I & Fishbein, M 1977, 'Attitude-behavior relations: A theoretical analysis and review of empirical research', *Psychological bulletin*, vol. 84, no. 5, pp. 888 -918.

Ajzen, I & Fishbein, M 1980, *Understanding attitudes and predicting social behavior*, illustrated edn, Prentice Hall, New York.

Albrechtslund, A 2008, 'Online social networking as participatory surveillance', *First Monday*, vol. 13, no. 3, p. 3.

Altheide, DL 2000, 'Identity and the definition of the situation in a mass-mediated context', *Symbolic Interaction*, vol. 23, no. 1, pp. 1-27.

Anderson, DR, Sweeney, DJ, Williams, TA, Freeman, J & Shoesmith, E 2010, *Statistics for business and economics*, 2nd edn, Cengage Learning, Hampshire, United Kingdom.

Anderson, JC & Gerbing, DW 1988, 'Structural equation modeling in practice: A review and recommended two-step approach', *Psychological bulletin*, vol. 103, no. 3, pp. 411-23.

Andrews, D, Preece, J & Turoff, M 2001, 'A conceptual framework for demographic groups resistant to online community interaction', paper presented to 34th Annual Hawaii International Conference on System Sciences, MD, USA January 3-6, 2001.

Andrews, DC 2002, 'Audience-specific online community design', *Communications of the ACM*, vol. 45, no. 4, April, 2002, pp. 64-8.

Arbuckle, JL 2006, *Amos 7.0 user's guide*, 1ST edn, SPSS Chicago, IL.

Bagozzi, RP & Edwards, JR 1998, 'A general approach for representing constructs in organizational research', *Organizational Research Methods*, vol. 1, no. 1, pp. 45-87.

Barber, BM & Odean, T 2001, 'The internet and the investor', *The Journal of*

Economic Perspectives, vol. 15, no. 1, pp. 41-54.

Barnes, SB 2006, 'A privacy paradox: Social networking in the United States', *First Monday*, vol. 11, no. 9, pp. 11-5.

Bateman, PJ, Pike, JC & Butler, BS 2011, 'To disclose or not: publicness in social networking sites', *Information Technology & People*, vol. 24, no. 1, pp. 78-100.

Baumgartner, H & Homburg, C 1996, 'Applications of structural equation modeling in marketing and consumer research: a review', *International Journal of Research in Marketing*, vol. 13, no. 2, pp. 139-61.

Bentler, PM 1990, 'Comparative fit indexes in structural models', *Psychological bulletin*, vol. 107, no. 2, pp. 238-46.

Bentler, PM 2007, 'On tests and indices for evaluating structural models', *Personality and Individual Differences*, vol. 42, no. 5, pp. 825-9.

Bhattacherjee, A & Sanford, C 2006, 'Influence processes for information technology acceptance: An elaboration likelihood model', *MIS quarterly*, vol. 30, no. 4, pp. 805-25.

Biesanz, JC & West, SG 2004, 'Towards Understanding Assessments of the Big Five: Multitrait-Multimethod Analyses of Convergent and Discriminant Validity Across Measurement Occasion and Type of Observer', *Journal of Personality*, vol. 72, no. 4, pp. 845-76.

Binder, J, Howes, A & Sutcliffe, A 2009, 'The problem of conflicting social spheres: effects of network structure on experienced tension in social network sites', paper presented to 27th international conference on Human factors in computing systems, Boston, MA, USA, April 4-9, 2009.

Bonhard, P & Sasse, M 2006, ''Knowing me, knowing you'—Using profiles and social networking to improve recommender systems', *BT Technology Journal*, vol. 24, no. 3, pp. 84-98.

Boyd, AW 2011, 'A Longitudinal Study of Social Media Privacy Behavior', PhD thesis, Pace University,New York.

Boyd, DM & Ellison, NB 2008, 'Social network sites: Definition, history, and scholarship', *Journal of Computer Mediated Communication*, vol. 13, no. 1, pp. 210-30.

Brass, DJ, Butterfield, KD & Skaggs, BC 1998, 'Relationships and unethical behavior: A social network perspective', *Academy of management review*, vol. 23, no. 1, pp. 14-31.

Bryman, A & Bell, E 2007, *Business research methods*, 2nd edn, Oxford University Press, New York.

Buote, VM, Wood, E & Pratt, M 2009, 'Exploring similarities and differences between online and offline friendships: The role of attachment style', *Computers in Human Behavior*, vol. 25, no. 2, pp. 560-7.

Byrne, BM 2001, 'Structural equation modeling with AMOS, EQS, and LISREL: Comparative approaches to testing for the factorial validity of a measuring instrument', *International Journal of Testing*, vol. 1, no. 1, pp. 55-86.

Campbell, DT & Fiske, DW 1959, 'Convergent and discriminant validation by the multitrait-multimethod matrix', *Psychological bulletin*, vol. 56, no. 2, pp. 81-105.

Chang, HH & Chen, SW 2008, 'The impact of customer interface quality, satisfaction and switching costs on e-loyalty: Internet experience as a moderator', *Computers in Human Behavior*, vol. 24, no. 6, pp. 2927-44.

Chiu, PY, Cheung, CMK & Lee, MKO 2008, 'Online social networks: Why do "we" use Facebook?', in JMC Miltiadis D. Lytras, Ernesto Damiani, Robert D. Tennyson, David Avison, Gottfried Vossen, Patricia Ordonez De Pablos (ed.), *The Open Knowlege Society. A Computer Science and Information Systems Manifesto*, illustrated edn, Springer, Athens, Greece, vol. 19, pp. 67-74.

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*, vol. 12, no. 3, pp. 341-5.

Collis, J & Hussey, R 2009, *Business Research-a Practical Guide for Undergraduate and Postgraduate Students*, 3rd edn, Palgrave MacMillan Limited, London.

Constant, D, Sproull, L & Kiesler, S 1996, 'The kindness of strangers: The usefulness of electronic weak ties for technical advice', *Organization science*, vol. 7, no. 2, pp. 119-35.

Cooper, DR & Schindler, PS 2003, *Business research methods*, 7th edn, McGraw Hill Internationa, New York.

Corritore, CL, Kracher, B & Wiedenbeck, S 2003, 'On-line trust: concepts, evolving themes, a model', *International Journal of Human-Computer Studies*, vol. 58, no. 6, pp. 737-58.

Crespo Herrero, A & Bosque, I 2008, 'The effect of innovativeness on the adoption of B2C e-commerce: A model based on the Theory of Planned Behaviour', *Computers in Human Behavior*, vol. 24, no. 6, pp. 2830-47.

Creswell, JW & Clark, VLP 2007, *Designing and conducting mixed methods research*, 2nd edn, Sage Publications, California, USA.

Creswell, JW, Hanson, WE, Clark, VLP & Morales, A 2007, 'Qualitative research designs: Selection and implementation', *Counseling Psychologist*, vol. 35, no. 2, p. 236.

Cronbach, LJ 1951, 'Coefficient alpha and the internal structure of tests', *Psychometrika*, vol. 16, no. 3, pp. 297-334.

Crotty, M 1998, *The foundations of social research: Meaning and perspective in the research process*, 1st edn, Sage Publications Ltd, California, USA.

Culnan, MJ & Bies, RJ 2003, 'Consumer privacy: Balancing economic and justice considerations', *Journal of Social Issues*, vol. 59, no. 2, pp. 323-42.

Dahlen, M 2002, 'Learning the web: internet user experience and response to web marketing in Sweden', *Journal of Interactive Advertising*, vol. 3, no. 1, pp. 25-33.

Davis, FD 1989, 'Perceived usefulness, perceived ease of use, and user acceptance of information technology', *MIS quarterly*, vol. 13, no. 3, pp. 319-40.

Davis, FD 1993, 'User acceptance of information technology: system characteristics, user perceptions and behavioral impacts', *International Journal of Man Machine Studes*, vol. 38, no. 3, pp. 475-87.

Davison, RM, Clarke, R, Jeff, H, Langford, D & Kuo, B 2003, 'Information privacy in a globally networked society: implications for IS research', *Communications of the Association for Information Systems*, vol. 12, no. 1, pp. 341 - 65.

Debatin, B, Lovejoy, JP, Horn, AK & Hughes, BN 2009, 'Facebook and online privacy: Attitudes, behaviors, and unintended consequences', *Journal of Computer Mediated Communication*, vol. 15, no. 1, pp. 83-108.

DiMicco, J, Millen, DR, Geyer, W, Dugan, C, Brownholtz, B & Muller, M 2008, 'Motivations for social networking at work', paper presented to 2008 ACM conference on Computer supported cooperative work, San Diego, CA, USA, November 8–12, 2008.

Dinev, T & Hart, P 2006, 'An extended privacy calculus model for e-commerce transactions', *Information Systems Research*, vol. 17, no. 1, p. 61.

Dwyer, C, Hiltz, SR & Passerini, K 2007, 'Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace', paper presented to 13th Americas Conference on Information Systems, Keystone, Colorado, August 9-12 2007.

Dwyer, C, Hiltz, SR & Widmeyer, G 2008, 'Understanding development and usage of social networking sites: The social software performance model', paper presented to 41st Annual Hawaii International Conference on System Sciences, Waikoloa, HI, January 7 -01- 2008.

Eagly, AH & Chaiken, S 1993, *The psychology of attitudes*, illustrated edn, Harcourt Brace Jovanovich College Publishers, New York, USA.

Ellison, NB & Boyd, D 2007a, 'Social network sites: Definition, history, and scholarship', *Journal of Computer-Mediated Communication*, vol. 13, no. 1,

pp. 210-30.

Ellison, NB, Steinfield, C & Lampe, C 2007b, 'The benefits of Facebook "friends:" Social capital and college students' use of online social network sites', *Journal of Computer Mediated Communication*, vol. 12, no. 4, pp. 1143-68.

Eriksen, A 2008, *Glitch opens Bebo users' private details to others*, The New Zealand Herald, viewed 1st August 2011, <http://www.nzherald.co.nz/nz/news /article.cfm?c_id=1&objectid=10511780>.

Etezadi-Amoli, J & Farhoomand, AF 1996, 'A structural model of end user computing satisfaction and user performance', *Information & Management*, vol. 30, no. 2, pp. 65-73.

Facebook 2011, *Press room, statistics.*, Palo Alto, CA, viewed March 23, 2011, <http://www.facebook.com/press/info.php?statistics>.

Fischer, F 1998, 'Beyond empiricism: policy inquiry in post positivist perspective', *Policy Studies Journal*, vol. 26, no. 1, pp. 129-46.

Fishbein, M & Ajzen, I 1975, *Belief, attitude, intention and behavior -An Introduction to Theory and Research*, illustrated edn, Addison-Wesley series in social psychology, Addison-Wesley, MA,USA.

Flicker, MH 2004, 'Securities trading on the Internet', in H Bidgoli (ed.), *The Internet Encyclopedia*, 3rd edn, Wiley Online Library, New Jersey, USA, vol. 3, p. 284.

Fogel, J & Nehmad, E 2009, 'Internet social network communities: Risk taking, trust, and privacy concerns', *Computers in Human Behavior*, vol. 25, no. 1, pp. 153-60.

Forum, F 2011, *What is Facebook Forum?*, Palo Alto, CA, viewed 01 July 2011, <http://www.thefacebookforum.net/>.

Fox, S & Purcell, K 2010, *Chronic Disease and the Internet*, Pew Research Center, viewed 30th November 2011, <http://pewinternet.org/Reports/2010/Chronic-Disease.aspx>.

Fuchs, C 2010, 'studiVZ: social networking in the surveillance society', *Ethics and Information Technology*, vol. 12, no. 2, pp. 171-85.

Fukuyama, F 1996, 'Trust Still Counts in a Virtual World', *FORBES*, vol. 158, December 2, 1996, pp. 33-5.

Gangadharbatla, H 2010, '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*, vol. 8, no. 2, pp. 5-15.

Ganley, D & Lampe, C 2009, 'The ties that bind: Social network principles in online communities', *Decision Support Systems*, vol. 47, no. 3, pp. 266-74.

Gecas, V 1986, 'The motivational significance of self-concept for socialization theory', in EJ Lawer (ed.), *In Advances in group processes*, JAI, Greenwich, vol. 3, pp. 131-56.

Gefen, D & Straub, DW 2000, 'The relative importance of perceived ease of use in IS adoption: A study of e-commerce adoption', *Journal of the Association for Information Systems*, vol. 1, no. 1, pp. 1-30.

Gefen, D, Karahanna, E & Straub, DW 2003, 'Inexperience and experience with online stores: The importance of TAM and trust', *IEEE Transactions on Engineering Management*, vol. 50, no. 3, pp. 307-21.

George, JF 2002, 'Influences on the intent to make Internet purchases', *Internet Research*, vol. 12, no. 2, pp. 165-80.

Gerbing, DW & Anderson, JC 1988, 'An updated paradigm for scale development incorporating hnidimensionality and its assessment', *Journal of Marketing Research*, vol. 25, no. 2, pp. 186-92.

Granovetter, M 1973, 'The strength of weak ties', *American journal of Sociology*, vol. 78, no. 6, pp. 1360-80.

Granovetter, M 1983, 'The strength of weak ties: A network theory revisited', *Sociological theory*, vol. 1, no. 1, pp. 201-33.

Grayson, K & Ambler, T 1999, 'The dark side of long-term relationships in marketing services', *Journal of Marketing Research*, vol. 36, no. 1, pp. 132-41.

Grewal, D, Munger, JL, Iyer, GR & Levy, M 2003, 'The influence of internet-retailing factors on price expectations', *Psychology and Marketing*, vol. 20, no. 6, pp. 477-93.

Gross, R & Acquisti, A 2005, 'Information revelation and privacy in online social networks', paper presented to 2005 ACM workshop on Privacy in the electronic society, Alexandria, VA, USA, November 7, 2005.

Hair Jr, JF, Anderson, R, Tatham, R & Black, WC 1998, *Multivariate Data Analysis*, 5 th edn, Prentice Hall, NJ.

Hair Jr, JF, Black, W, Babin, B, Anderson, R & Tatham, R 2006, *Multivariate Data Analysis*, 6th edn, Prentice Hall, NJ.

Hargittai, E 2008, 'Whose Space? Differences Among Users and Non Users of Social Network Sites', *Journal of Computer Mediated Communication*, vol. 13, no. 1, pp. 276-97.

Harrison, R & Thomas, M 2009, 'Identity in online communities: Social networking sites and language learning', *International Journal of Emerging Technologies & Society*, vol. 7, no. 2, pp. 109-24.

Hayduk, LA 1987, *Structural equation modeling with LISREL: Essentials and advances*, 1st edn, The Johns Hopkins University Press, Baltimore, Maryland.

Hodge, MJ 2006, 'Fourth Amendment and Privacy Issues on the New Internet: Facebook. com and Myspace. com, The', *Southern Illinois University Law School Journal*, vol. 31, no. 3, pp. 95-122.

Hoffman, DL, Novak, TP & Peralta, M 1999, 'Building consumer trust online', *Communications of the ACM*, vol. 42, no. 4, pp. 80-5.

Hoy, MG & Milne, G 2010, 'Gender Differences in Privacy-Related Measures for Young Adult Facebook Users', *Journal of Interactive Advertising*, vol. 10, no. 2, pp. 28-45.

Hu, Q & Ma, S 2010, 'Does Privacy Still Matter in the Era of Web 2.0? A Qualitative Study of User Behavior towards Online Social Networking Activities', paper presented to 14th Pacific Asia Conference on Information Systems, Taipei, Taiwan, July 9-12, 2010.

Joinson, AN, Reips, UD, Buchanan, T & Schofield, CBP 2010, 'Privacy, trust, and self-disclosure online', *Human–Computer Interaction*, vol. 25, no. 1, pp. 1-24.

Joreskog, KG & Sorbom, D 1996, *LISREL 8 user's reference guide*, 2nd edn, Scientific Software International, Inc, Lincolnwood.

Kamel Boulos, MN & Wheeler, S 2007, 'The emerging Web 2.0 social software: an enabling suite of sociable technologies in health and health care education1', *Health Information & Libraries Journal*, vol. 24, no. 1, pp. 2-23.

Khosrow-Pour, M 2007, *Web Technologies for Commerce and Services Online*, illustrated edn, IGI Publishing, Hershey, PA.

Kim, DJ, Steinfield, C & Lai, YJ 2008, 'Revisiting the role of web assurance seals in business-to-consumer electronic commerce', *Decision Support Systems*, vol. 44, no. 4, pp. 1000-15.

Kline, RB 2010, *Principles and practice of structural equation modeling*, 3rd edn, The Guilford Press, NY.

Kripanont, N 2007, 'Examining a technology acceptance model of internet usage by academics within Thai business schools', PhD thesis, Victoria University.

Lach, J 1999, 'The new gatekeepers', *American Demographics*, vol. 21, no. 6, pp. 41-2.

Lai, LSL & Turban, E 2008, 'Groups formation and operations in the Web 2.0 environment and social networks', *Group Decision and Negotiation*, vol. 17, no. 5, pp. 387-402.

Leedy, PD & Ormrod, JE 2009, *Practical research: Planning and design*, 9th

edn, NJ.

Lenhart, A 2009, *Adults and social network websites*, Pew Internet and American Life Project, viewed 29th November 2011, <http://www.pewinternet.org/Reports /2009/Adults-and-Social-Network-Websites.aspx>.

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*, vol. 14, no. 1, pp. 79-100.

Liao, C, Chen, JL & Yen, DC 2007, 'Theory of planning behavior (TPB) and customer satisfaction in the continued use of e-service: An integrated model', *Computers in Human Behavior*, vol. 23, no. 6, pp. 2804-22.

Lin, HF 2006, 'Understanding behavioral intention to participate in virtual communities', *CyberPsychology & Behavior*, vol. 9, no. 5, pp. 540-7.

LinkedIn 2011, *About us*, LinkedIn, viewed 28th September 2011, <http://press.linkedin.com/about>.

Liong, EL & Mejstad, T 2010, 'Privacy and Information Sharing on Social Networking Sites', Master thesis, Lund University.

Liu, C, Marchewka, JT, Lu, J & Yu, CS 2005, 'Beyond concern--a privacy-trust-behavioral intention model of electronic commerce', *Information & Management*, vol. 42, no. 2, pp. 289-304.

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*, vol. 10, no. 3, pp. 393-411.

Lo, J 2010, 'Privacy Concern, Locus of Control, and Salience in a Trust-Risk Model of Information Disclosure on Social Networking Sites', paper presented to Americas Conference on Information Systems, Lima, Peru, August 12-15, 2010.

Lo, J & Riemenschneider, C 2010, 'An Examination of Privacy Concerns and Trust Entities in Determining Willingness to Disclose Personal Information on a Social Networking Site', paper presented to Americas Conference on Information Systems, Lima, Peru, August 12-15, 2010.

Luan, WS, Fung, NS, Nawawi, M & Hong, TS 2005, 'Experienced and inexperienced Internet users among pre-service teachers: Their use and attitudes toward the Internet', *Educational Technology & Society*, vol. 8, no. 1, pp. 90-103.

Luo, X 2002, 'Trust production and privacy concerns on the Internet: A framework based on relationship marketing and social exchange theory', *Industrial Marketing Management*, vol. 31, no. 2, pp. 111-8.

Madden, M & Fox, S 2006, *Riding the waves of "Web 2.0."*, Pew Internet & American Life Project, viewed 10th November 2011,

<http://www.pewinternet.com/~/media/Files/Reports/2006/PIP_Web_2.0.pdf.>.

Malhotra, NK 2008, *Marketing Research: An Applied Orientation*, 5th edn, Pearson Education, India.

Malhotra, NK, Kim, SS & Agarwal, J 2004, 'Internet Users' Information Privacy Concerns(IUIPC): The Construct, the Scale, and a Causal Model', *Information Systems Research*, vol. 15, no. 4, pp. 336-55.

Manago, AM, Graham, MB, Greenfield, PM & Salimkhan, G 2008, 'Self-presentation and gender on MySpace', *Journal of Applied Developmental Psychology*, vol. 29, no. 6, pp. 446-58.

Mansfield-Devine, S 2008, 'Anti-social networking: exploiting the trusting environment of Web 2.0', *Network Security*, vol. 2008, no. 11, pp. 4-7.

Maruyama, G 1998, *Basics of structural equation modeling*, 1st edn, Sage Publications, Inc, Thousand Oaks, California

Mayer, RC, Davis, JH & Schoorman, FD 1995, 'An integrative model of organizational trust', *The Academy of Management Review*, vol. 20, no. 3, pp. 709-34.

Mayer, RC, Schoorman, FD & Davis, JH 2007, 'An integrative model of organizational trust: Past, present, and future', *The Academy of Management Review*, vol. 32, no. 2, pp. 344-54.

mc² 2011, *my connected community*, viewed 5th November 2011, <http://mc2.vicnet.net.au/>.

McDonald, RP & Ho, MHR 2002, 'Principles and practice in reporting structural equation analyses', *Psychological Methods*, vol. 7, no. 1, p. 64.

McKnight, DH, Cummings, LL & Chervany, NL 1998, 'Initial trust formation in new organizational relationships', *The Academy of Management Review*, vol. 23, no. 3, pp. 473-90.

McKnight, DH, Choudhury, V & Kacmar, C 2003, 'Developing and validating trust measures for e-commerce: An integrative typology', *Information Systems Research*, vol. 13, no. 3, pp. 334-59.

Meinert, DB, Peterson, DK, Criswell, JR & Crossland, MD 2006a, 'Privacy policy statements and consumer willingness to provide personal information', *Journal of Electronic Commerce in Organizations*, vol. 4, no. 1, pp. 1-17.

Meinert, DB, Peterson, DK, Criswell, JR & Crossland, MD 2006b, 'Would Regulation of Web Site Privacy Policy Statements Increase Consumer Trust?', *Informing Science Journal*, vol. 9, no. 4, pp. 123-41.

Meredith, P 2006, *Facebook and the Politics of Privacy*, Mother Jones, viewed 5th

November 2011, <http://motherjones.com/politics/2006/09/facebook-and-politics-privacy>.

Metzger, MJ 2004, 'Privacy, trust, and disclosure: Exploring barriers to electronic commerce', *Journal of Computer Mediated Communication*, vol. 9, no. 4, pp. 00-.

Metzger, MJ & Docter, S 2003, 'Public opinion and policy initiatives for online privacy protection', *Journal of Broadcasting & Electronic Media*, vol. 47, no. 3, pp. 350-74.

Milne, GR & Culnan, MJ 2004, 'Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices', *Journal of Interactive Marketing*, vol. 18, no. 3, pp. 15-29.

Mislove, A, Marcon, M, Gummadi, KP, Druschel, P & Bhattacharjee, B 2007, 'Measurement and analysis of online social networks', paper presented to 7th ACM SIGCOMM conference on Internet measurement, San Diego, California, USA, October 24-26, 2007.

Molok, NNA, Chang, S & Ahmad, A 2010, 'Information Leakage through Online Social Networking: Opening the Doorway for Advanced Persistence Threats', paper presented to 8th Australian Information Security Management, Perth, Australia, 30th November-2nd December, 2010.

Mori, J, Sugiyama, T & Matsuo, Y 2005, 'Real-world oriented information sharing using social networks', paper presented to GROUP 05 international ACM SIGGROUP conference on Supporting group work, Sanibel Island, Florida, USA, November 6-9, 2005.

MySpace 2011, *Pressroom, fact sheet*, Los Angeles, CA, viewed 23 March 2011, <http://www.myspace.com/pressroom/2011/03/>.

Nahapiet, J & Ghoshal, S 1998, 'Social capital, intellectual capital, and the organizational advantage', *Academy of management review*, vol. 23, no. 2, pp. 242-66.

Nooteboom, B 2007, 'Social capital, institutions and trust', *Review of Social Economy*, vol. 65, no. 1, pp. 29-53.

Novak, TP, Hoffman, DL & Yung, YF 2000, 'Measuring the customer experience in online environments: A structural modeling approach', *Marketing Science*, vol. 19, no. 1, pp. 22-42.

Nunnally, J 1994, *Psychometric theory*, 3rd edn, Social Psychology, McGraw-Hill, New York.

Nysveen, H & Pedersen, PE 2004, 'An exploratory study of customers' perception of company web sites offering various interactive applications: moderating effects of customers' internet experience', *Decision Support Systems*, vol. 37, no. 1, pp. 137-50.

Paine, C, Reips, UD, Stieger, S, Joinson, A & Buchanan, T 2007, 'Internet users' perceptions of privacy concerns' and privacy actions", *International Journal of Human-Computer Studies*, vol. 65, no. 6, pp. 526-36.

Pallant, J 2011, *SPSS Survival Manual*, 4th edn, Allen & Unwin, Crows Nest, NSW.

Park, JH, Konana, P, Gu, B & Man Leung, AC 2010, 'An investigation of information sharing and seeking behaviors in virtual communities', paper presented to International Conference on Information Systems, St. Louis, 8-01-2010.

Park, N, Kee, KF & Valenzuela, S 2009, 'Being immersed in social networking environment: Facebook groups, uses and gratifications, and social outcomes', *CyberPsychology & Behavior*, vol. 12, no. 6, pp. 729-33.

Paul, A, Hepworth, M, Kelly, B & Metcalfe, R 2007, 'What is Web 2. 0? Ideas, technologies and implications for education ', *Technology and Standards Watch*, vol. 60, no. 1, pp. 2-64.

Pavlou, PA 2003, 'Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model', *International Journal of Electronic Commerce*, vol. 7, no. 3, pp. 101-34.

Pavlou, PA & Fygenson, M 2006, 'Understanding and predicting electronic commerce adoption: An extension of the theory of planned behavior', *Management Information Systems Quarterly*, vol. 30, no. 1, pp. 115-43.

Peluchette, J & Karl, K 2008, 'Social networking profiles: An examination of student attitudes regarding use and appropriateness of content', *CyberPsychology & Behavior*, vol. 11, no. 1, pp. 95-7.

Peter, JP 1979, 'Reliability: A review of psychometric basics and recent marketing practices', *Journal of Marketing Research*, vol. 16, no. 1, pp. 6-17.

Peter, JP 2001, 'Construct validity: a review of basic issues and marketing practices', *Journal of Marketing Research*, vol. 18, no. 2, pp. 133-45.

Plant, R 2004, 'Online communities', *Technology in Society*, vol. 26, no. 1, pp. 51-65.

Ramgovind, S, Eloff, M & Smith, E 2010, 'The management of security in cloud computing', paper presented to Information Security for South Africa (ISSA), Sandton, Johannesburg August 2-4, 2010

Richards, DV 2006, 'Posting Personal Information on the Internet: A Case for Changing the Legal Regime Created by Sec. 230 of the Communications Decency Act', *Texas Law Review*, vol. 85, no. 5, pp. 1321-58.

Robards, B 2010, 'Randoms in my bedroom: Negotiating privacy and unsolicited contact on social network sites', *PRism*, vol. 7, no. 3, p. 00.

Robinson, J, Shaverm, P & Wrightsman, L 1991, 'Criteria for scale selection and

evaluation ', in JP Robinson, PR Shaver & LS Wrightsman (eds), *Measures of personality and social psychological attitudes*, Gulf Professional Publishing, San Diego, CA, vol. 1, pp. 1-16.

Rosenblum, D 2007, 'What anyone can know: The privacy risks of social networking sites', *IEEE Security & Privacy*, vol. 5, no. 3, pp. 40-9.

Rowe, M 2010, 'The credibility of digital identity information on the social web: a user study', paper presented to WICOW'10, Raleigh, North Carolina, USA, April 27, 2010.

Schumacker, RE & Lomax, RG 2004, *A beginner's guide to structural equation modeling*, 2nd edn, vol. 1, Lawrence Erlbaum, Mahwah, New Jersey.

Seale, C 1999, *Quality in qualitative research*, 1st edn, vol. 5, Qualitative inquiry, SAGE publications, London.

Seddon, PB 1997, 'A respecification and extension of the DeLone and McLean model of IS success', *Information Systems Research*, vol. 8, no. 3, pp. 240-53.

Sekaran, U 2003, *Research methods for business: A skill building approach*, 4th edn, CourseSmart, John Wiley and Sons, India.

Shafie, LA, Mansor, M, Osman, N, Nayan, S & Maesin, A 2011, 'Privacy, Trust and Social Network Sites of University Students in Malaysia', *Research Journal of International Studies*, no. 20, pp. 154 -62.

Sharma, S 1995, *Applied multivariate techniques*, 1st edn, John Wiley & Sons, New York.

Shin, D-H 2010a, 'The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption', *Interacting with Computers*, vol. 22, no. 5, pp. 428-38.

Shin, DH 2010b, 'Effect of Trust and Privacy Concerns on Social Networking: A Trust-Based Acceptance Model for Social Networking Systems', paper presented to International Communication Association, Suntec Singapore International Convention & Exhibition Centre, Suntec City, Singapore, Jun 22, 2010

Son, JY & Kim, SS 2008, 'Internet users' information privacy-protective responses: A taxonomy and a nomological model', *Management Information Systems Quarterly*, vol. 32, no. 3, pp. 503-29.

Staksrud, E & Lobe, B 2010, *Evaluation of the implementation of the safer social networking principles for the EU*, Europe's Information Society viewed 30th August 2011,
<http://ec.europa.eu/information_society/activities/social_networking/eu_action/implementation_princip/index_en.htm>.

Stone, GP 2005, 'Appearance and the self: A slightly revised version', in CE Dennis

Brissett (ed.), *Life as theater: a dramaturgical sourcebook*, 2nd edn, Transaction Publishers, New Jersey, vol. 2, pp. 141–62.

Sussman, SW & Siegal, WS 2003, 'Informational influence in organizations: An integrated approach to knowledge adoption', *Information Systems Research*, vol. 14, no. 1, pp. 47-65.

Taylor, S & Todd, P 1995a, 'Assessing IT usage: The role of prior experience', *MIS quarterly*, vol. 19, no. 4, pp. 561-70.

Taylor, S & Todd, PA 1995b, 'Understanding information technology usage: A test of competing models', *Information Systems Research*, vol. 6, no. 2, pp. 144-76.

Thelwall, M 2009, 'Social Network Sites:: Users and Uses', in M Zelkowitz (ed.), *Advances in computers*, 1st edn, Academic Press, Massachusetts, vol. 76, pp. 19-73.

Thompson, B 2004, *Exploratory and confirmatory factor analysis: Understanding concepts and applications*, 1^{at} edn, American Psychological Association, Washington, D.C

Thompson, B & Daniel, LG 1996, 'Factor analytic evidence for the construct validity of score: a historical overview and some guidelines', *Educational and Psychological Measurement*, vol. 56, no. 2, pp. 197-208.

Timm, DM & Duven, CJ 2008, 'Privacy and social networking sites', *New Directions for Student Services*, vol. 2008, no. 124, pp. 89-101.

Trembath, L 2011, 'Determinants of success for online communities: An emprical study', Doctor of Business Adminstration thesis, Swinburne University of Technology, Melbourne.

Tufekci, Z 2008, 'Can you see me now? Audience and disclosure regulation in online social network sites', *Bulletin of Science, Technology & Society*, vol. 28, no. 1, pp. 20-36.

Tull, DS & Hawkins, DI 1990, *Marketing research: measurement and method: a text with cases*, 5th edn, Macmillan, New York.

USC 2011, *Digital Future Report*, USC Annenberg School for Communication & Journalism, viewed 15th August 2011, <http://www.digitalcenter.org/pdf/2011_digital_future_final_release.pdf>.

Valenzuela, S, Park, N & Kee, KF 2009, 'Is There Social Capital in a Social Network Site?: Facebook Use and College Students' Life Satisfaction, Trust, and Participation1', *Journal of Computer Mediated Communication*, vol. 14, no. 4, pp. 875-901.

Van Slyke, C, Shim, J, Johnson, R & Jiang, JJ 2006, 'Concern for information privacy and online consumer purchasing', *Journal of the Association for Information Systems*, vol. 7, no. 6, pp. 415-44.

Veal, AJ 2005, *Business research methods: A managerial approach*, 2nd edn, Pearson Education, NSW.

Warren, SD & Brandeis, LD 1890, 'The right to privacy', *Harvard law review*, vol. 4, no. 5, pp. 193-220.

Warshaw, PR & Davis, FD 1985, 'The accuracy of behavioral intention versus behavioral expectation for predicting behavioral goals', *The Journal of psychology*, vol. 119, no. 6, pp. 599-602.

Wasko, MML & Faraj, S 2005, 'Why should I share? Examining social capital and knowledge contribution in electronic networks of practice', *MIS quarterly*, vol. 29, no. 1, pp. 35-57.

Weik, P & Wahle, S 2010, 'Towards a Generic Identity Enabler for Telco Networks', paper presented to 12th International Conference on Intelligence in Service Delivery Networks (ICIN), Bordeaux, France, October 20-23 2008.

Wellman, B 1997, 'An electronic group is virtually a social network', in S Kiesler (ed.), *Culture of the Internet*, 4th edn, Routledge, New Jersey, pp. 179-205.

Wenger, E 2005, *Communities of practice: Learning, meaning, and identity*, 13th edn, Cambridge University Press, New York.

Williams, S, Fleming, S, Lundqvist, K & Parslow, P 2010, 'Understanding your digital identity', *Learning Exchange*, vol. 1, no. 1, pp. 1-5.

Windley, P 2005, *Digital identity*, 1st edn, O'Reilly Media, Inc., California.

Wixom, BH & Watson, HJ 2001, 'An empirical investigation of the factors affecting data warehousing success', *MIS quarterly*, vol. 25, no. 1, pp. 17-41.

Wu, A, DiMicco, JM & Millen, DR 2010, 'Detecting professional versus personal closeness using an enterprise social network site', paper presented to 28th international conference on Human factors in computing systems, Atlanta, Georgia, USA, April 10-15, 2010.

Xu, H 2009, 'consumer responses to the Introduction of Privacy Protection Measures', *International Journal of E-Business Research*, vol. 5, no. 2, pp. 21-47.

Yahoo 2011, *Connect with a world of people who share your passions*, viewed 10th November 2011, <http://au.groups.yahoo.com/>.

Ybarra, ML & Mitchell, KJ 2008, 'How risky are social networking sites? A comparison of places online where youth sexual solicitation and harassment occurs', *American Academy of Pediatrics*, vol. 121, no. 2, pp. 350-7.

Yu, T & Wu, G 2007, 'Determinants of Internet Shopping Behavior: An Application of Reasoned Behaviour Theory', *International Journal of Management*, vol. 24, no.

4, p. 744.

Zarsky, TZ 2004, 'Desperately seeking solutions: Using implementation-based solutions for the troubles of information privacy in the age of data mining and the internet society', *Maine Law Review*, vol. 56, no. 1, pp. 13-59.

Zhang, Y & Tatipamula, M 2011, 'The freshman handbook: a hint for the server placement of social networks', paper presented to 20th international conference companion on World wide web, Hyderabad, India, March 28–April 1, 2011.

Zhao, S 2005, 'The digital self: Through the looking glass of telecopresent others', *Symbolic Interaction*, vol. 28, no. 3, pp. 387-405.

Zhao, S, Grasmuck, S & Martin, J 2008, 'Identity construction on Facebook: Digital empowerment in anchored relationships', *Computers in Human Behavior*, vol. 24, no. 5, pp. 1816-36.

Zikmund, WG, Griffin, M, Babin, BJ & Carr, JC 2009, *Business research methods*, 8th edn, Cengage Learning, Mason, Ohio, USA.

Appendix A

Participant Information sheet

U n i v e r s i t y   o f   S o u t h e r n   Q u e e n s l a n d

The University of Southern Queensland

Participant Information Sheet

TO: Participants

TITLE OF PROJECT: Understanding impact of privacy concerns and trust in social networking sites: Analysing user intentions towards willingness to share digital identities

RESEARCH TEAM: Sanjib Tiwari, MBSR Student, Faculty of Business and Law, University of Southern Queensland, Phone: +62 7 46875775, email: Sanjib.Tiwari@usq.edu.au

Description

The purpose of this project is to address how user' privacy concerns and trust influence their intentions towards willingness to share information in social networking sites.

The research team request your assistance because you are social networking sites user which eligible as a participant of this project.

This project is being undertaken as part of a MBSR project for Sanjib Tiwari.

Participation

Your participation in this project is voluntary and non- participation will not affect you in any way. You can withdraw from the project at any stage without comment or penalty. Your decision to participate or not, or to withdraw from the project will not affect your current or future relationship with the University of Southern Queensland.

This project involves the submission of anonymous (non-identifiable) material. Please note: it will not be possible to withdraw your data once submitted.

It is expected your participation will take approximately 15 minutes of your time.

Please note: the data obtained from this project may be used at a later time for any research purpose.

Risks

There are no risks beyond day-to-day living associated with your participation in this project. This survey is not expected to cause any discomfort or stress. If it does, you may discontinue taking the survey. There is no compensation provided for taking this survey.

Confidentiality

Any information obtained in connection with this project and that can identify you will remain confidential. It will only be disclosed with your permission, subject to legal requirements. If you give us your permission by signing the Consent Form, we plan to publish the results with my supervisor to the Academic Journal**.**

In any publication, information will be provided in such a way that you cannot be identified.

All data received for this project will remain stored for a minimum of 5 years in secure facilities.

Consent to Participate

Please read this information sheet carefully so that you understand what the project involves. If you do not understand any part of the project or require further information please contact the research teams members named above. Please find the ethical acceptance letter from USQ ethics officer for the above mention project.

The return of the completed anonymous survey is accepted as an indication of your consent to participant in this project

Questions/further information about the project

You are encouraged to print this consent form and keep safe place you could contact the research teams members named above if you have any questions or if you require further information about the project. Now if you want to participate in this survey please click the below link or copy paste the link in web browser:

http://usqbusiness.us.qualtrics.com/SE/?SID=SV_5vWRCqaLfUMG6Ve

Concerns/complaints regarding the conduct of the project

If you have any concerns or complaints about the ethical conduct of the project you may contact the USQ Ethics Officer on +61 7 4631 2690 or email ethics@usq.edu.au. The Ethics Officer is not connected with the project and can facilitate a resolution in an impartial manner.

Where the research may cause distress, independent 24 hour counselling services are available through Lifeline on 13 11 14 from anywhere in Australia.

Appendix B

Ethics Approval

25 July 2011

Sanjib Tiwari
Faculty of Business
USQ Toowoomba Campus 4350

Dear Sanjib

The Chair of the USQ Fast Track Human Research Ethics Committee (FTHREC) recently reviewed your responses to the FTHREC's conditions placed upon the ethical approval for the below project. Your proposal now meets the requirements of the *National Statement on Ethical Conduct in Human Research (2007)* and full ethics approval has been granted.

Project Title	Understanding impact of privacy concerns and trust in social networking sites: Analysing user intentions towards willingness to share digital identities.
Approval no.	H11REA123
Start Date	21/07/2011
Expiry date	31/10/2011
FTHREC Decision	**Approved**

The standard conditions of this approval are:

    (a) conduct the project strictly in accordance with the proposal submitted and granted ethics approval, including any amendments made to the proposal required by the HREC
    (b) advise (email: ethics@usq.edu.au) immediately of any complaints or other issues in relation to the project which may warrant review of the ethical approval of the project
    (c) make submission for approval of amendments to the approved project before implementing such changes
    (d) provide a 'progress report' for every year of approval
    (e) provide a 'final report' when the project is complete
    (f) advise in writing if the project has been discontinued.

For (c) to (e) forms are available on the USQ ethics website: http://www.usq.edu.au/research/ethicsbio/human

Please note that failure to comply with the conditions of approval and the *National Statement (2007)* may result in withdrawal of approval for the project.

You may now commence your project. I wish you all the best for the conduct of the project.

Helen Phillips
Ethics Officer
Office of Research and Higher Degrees

Appendix C

Information and informed consent statement (online version)

Understanding the Social networking sites:

You are invited to participate in a research project that looks at" Understanding impact of privacy concerns and trust in social networking sites: Analysing user intentions towards willingness to share digital identities"

You can participate in this project by completing the online questionnaire about the social networking sites and by participating in this research you might find that you will learn something about impact of privacy concerns and trust in SNS. It is expected that up to 200 members of a variety of social networking sites will volunteer to participate in the study.

This questionnaire should take approximately 7 minutes to complete.

You will not be asked for any personal information that could identify you. This ensures your anonymity, confidentially and privacy. To participate in this study you are required to be 18 years of age, or older and be a member of at least one social networking sites.

Findings from the study, using aggregated data, will be reported in my thesis and possibly some co-authored academic publications. The thesis will be submitted as partial fulfilment of a MBSR at University of Southern Queensland.

Agreeing to complete this questionnaire is taken as your Informed Consent. Informed Consent means you agree that your participation is voluntary and you understand that you are free to stop answering the questions at any time. Only answers from completed questionnaires will be used in this study.

If you have any questions regarding this project please contact:
Sanjib Tiwari
MBSR Candidate
Sanjib.Tiwari@usq.edu.au

Dr. Jianming Yong
Principal Supervisor
Jianming.Yong@usq.edu.au,

Dr. Michael Lane
Associate Supervisor
Michael.Lane@usq.edu.au

This project has been approved by or on behalf of USQ Fast Track Human Research Ethics Committee (FTHREC) in line with the *National Statement on Ethical Conduct in Research Involving Humans*.
If you have any concerns or complaints about the ethical conduct of the project you may contact the USQ Ethics Officer on +61 7 4631 2690 or email ethics@usq.edu.au. The Ethics Officer is not connected with the project and can facilitate a resolution in an impartial manner.

Where the research may cause distress, independent 24 hour counselling services are available through Lifeline on 13 11 14 from anywhere in Australia.

If you would like to assist us by completing the survey, please click on the start Link below:
http://usqbusiness.us.qualtrics.com/SE/?SID=SV_5vWRCqaLfUMG6Ve

Appendix D

Online Survey

A few glimpse of the online survey:

http://usqbusiness.us.qualtrics.com/SE/?SID=SV_5vWRCqaLfUMG6Ve

Apple   Yahoo!   Google Maps   YouTube   Wikipedia   News (115) ▼   Popular ▼

USQ   UNIVERSITY OF SOUTHERN QUEENSLAND   **Faculty of Business and Law**

Q17. Privacy Concerns

	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
I am concerned that the information I submit onto social networking sites could be misused.	○	○	○	○	○	○	○
I am concerned that a person can find private information on the social networking sites.	○	○	○	○	○	○	○
I am concerned about submitting information onto social networking sites because of others might do with it.	○	○	○	○	○	○	○
I am concerned about submitting information onto social networking sites because it could be used in a way I did not foresee	○	○	○	○	○	○	○
I am concerned that online companies are collecting too much personal information	○	○	○	○	○	○	○

Survey Completion
0%   100%

PREVIOUS   NEXT

Survey Powered By Qualtrics

start   Qualtri...   7C83B...   H:\Dis...   C:\Do...   EndNo...   flood p...   Docum...   appen...   iPads_...   letter ...   Under...   12:04 AM

USQ UNIVERSITY OF SOUTHERN QUEENSLAND   **Faculty of Business and Law**

Q18. Trust in Social networking site

	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
I believe that Social Networking Site would act in my best interest when dealing with my personal information.	○	○	○	○	○	○	○
Social Networking Site is interested in protecting my personal information according to the preferences I specify.	○	○	○	○	○	○	○
Social Networking Site would tell the truth and fulfill its promises related to the personal information provided by me.	○	○	○	○	○	○	○
Social Networking Site is sincere and genuine in managing my personal information.	○	○	○	○	○	○	○
Social Networking Site handles personal information submitted by users in a competent fashion.	○	○	○	○	○	○	○
Social Networking Site performs its role of managing my personal information according to my privacy settings very well.	○	○	○	○	○	○	○

Survey Completion

0%   100%

PREVIOUS   NEXT

Survey Powered By Qualtrics

USQ UNIVERSITY OF SOUTHERN QUEENSLAND **Faculty of Business and Law**

Q20. Willingness to share digital identities

	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
I am willing to share my real name.	○	○	○	○	○	○	○
I am willing to share my real hometown address.	○	○	○	○	○	○	○
I am willing to share my real date of birth.	○	○	○	○	○	○	○
I am willing to share my real email address.	○	○	○	○	○	○	○
I am willing to share my real home phone number.	○	○	○	○	○	○	○
I am willing to share my real mobile phone number.	○	○	○	○	○	○	○
I am willing to share my real photograph.	○	○	○	○	○	○	○
I am willing to share the names of my real high school(s), I have attended.	○	○	○	○	○	○	○
I am willing to share the names of my real college(s) attended.	○	○	○	○	○	○	○
I am willing to share my real name of employer.	○	○	○	○	○	○	○
I am willing to share my real interests.	○	○	○	○	○	○	○
I am willing to share my real personality	○	○	○	○	○	○	○
I am willing to share my real gender	○	○	○	○	○	○	○

Survey Completion
0%   100%

PREVIOUS   NEXT

Survey Powered By Qualtrics
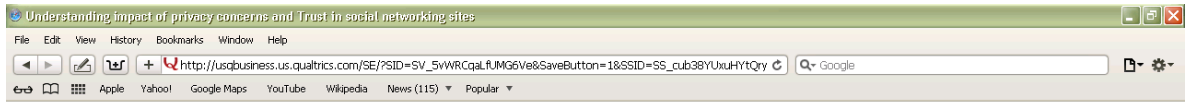
USQ UNIVERSITY OF SOUTHERN QUEENSLAND **Faculty of Business and Law**

We thank you for your time spent taking this survey.
Your response has been recorded.

Survey Completion

0%   100%

Survey Powered By Qualtrics

Appendix E

Statistical data analysis details

Reliability and Factor loading Statistics test using SPSS for Privacy Concerns

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardised Items	N of Items
.816	.817	5

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
PC1	20.85	20.114	.564	.332	.793
PC2	20.54	20.237	.612	.387	.779
PC3	20.77	19.426	.652	.486	.767
PC4	20.71	18.961	.636	.464	.771
PC5	20.38	19.445	.573	.331	.791

Factor Matrix[a]

	Factor
	1
PC1	.611
PC2	.673
PC3	.770
PC4	.749
PC5	.626

Extraction Method: Maximum Likelihood.

a. 1 factors extracted. 3 iterations required.

Reliability and Factor loading Statistics test using SPSS for Trust

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardised Items	N of Items
.883	.886	5

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
T1	18.25	23.086	.620	.406	.884
T2	18.12	22.051	.769	.603	.846
T3	18.23	22.267	.762	.627	.848
T4	18.37	22.896	.789	.652	.843
T6	17.80	24.953	.678	.505	.868

Factor Matrix[a]

	Factor
	1
T1	.660
T2	.810
T3	.840
T4	.857
T6	.736

Extraction Method: Maximum Likelihood.

a. 1 factors extracted. 4 iterations required.

Reliability and Factor loading Statistics test using SPSS for SNS Experience

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardised Items	N of Items
.707	..709	4

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
SNS1	18.77	2.413	.732	.021	.710
SNS2	19.38	1.939	..690	.017	..705
SNS3	10.52	3.108	.648	.042	..701
SNS4	17.95	3.166	.685	.048	.707

Factor Matrix[a]

	Factor
	1
SNS1	.760
SNS2	.710
SNS3	.660
SNS4	.700

Extraction Method: Maximum Likelihood.

a. 1 factors extracted. 4 iterations required.

Reliability and Factor loading Statistics test using SPSS for Digital Identity

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardised Items	N of Items
.869	.879	6

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
DI2	27.14	40.417	.468	.252	.892
DI7	26.36	41.609	.633	.472	.852
DI8	26.30	38.524	.777	.659	.827
DI9	26.27	38.498	.823	.721	.821
DI10	26.53	37.627	.737	.579	.833
DI13	25.79	43.169	.663	.477	.850

Factor Matrix[a]

	Factor
	1
DI2	.491
DI7	.701
DI8	.856
DI9	.909
DI10	.785
DI13	.711

Extraction Method: Maximum Likelihood.

a. 1 factors extracted. 4 iterations required.

Snapshot of AMOS first structural model with latent variable

The snapshot below describe that this is the model draw in AMOS 19 software tools. Where we can see there are four variables Trust, Privacy, SNS and DI with number of its latent variable
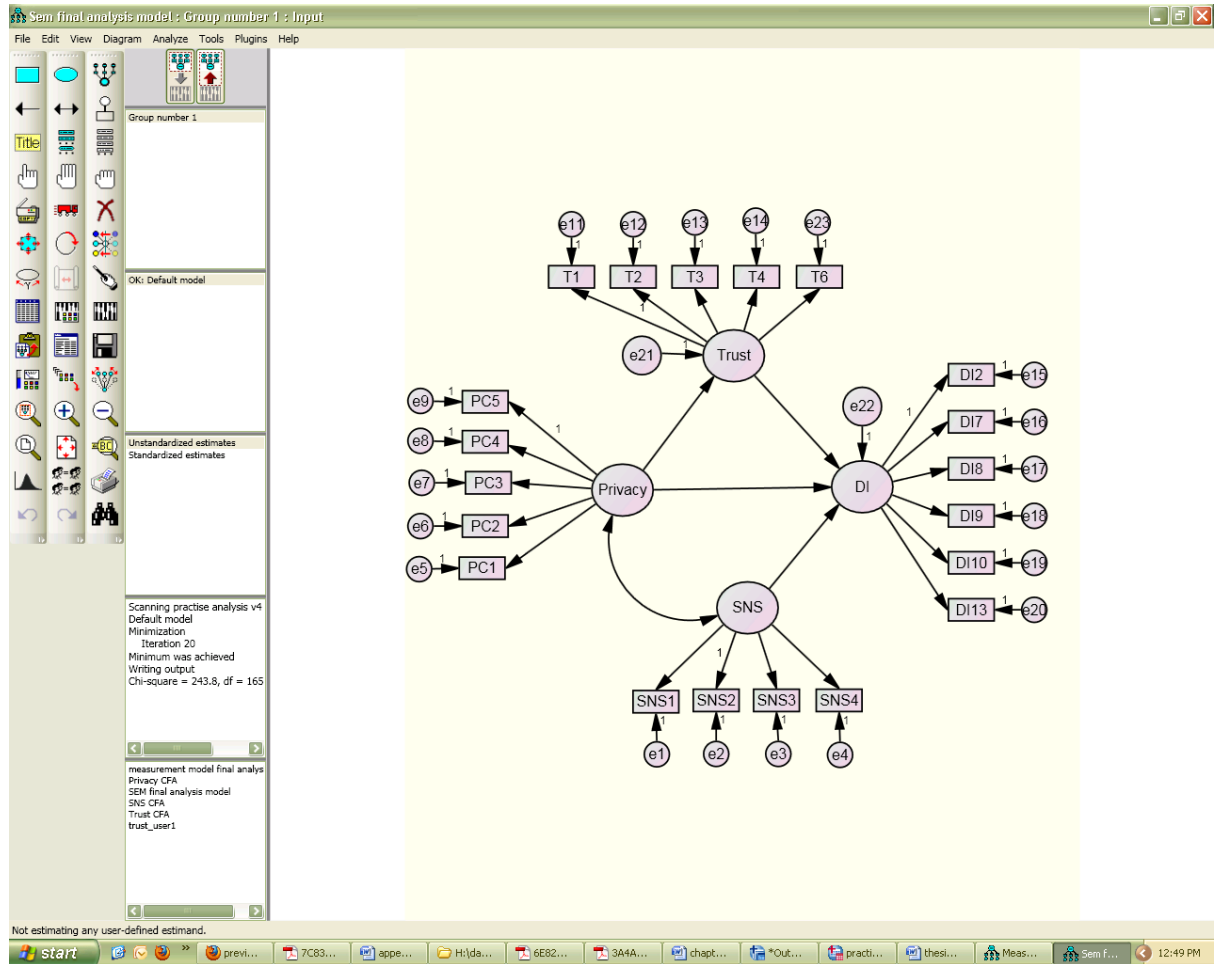
Snapshot of AMOS Unstandardised estimates structural model with latent variable and factor loading
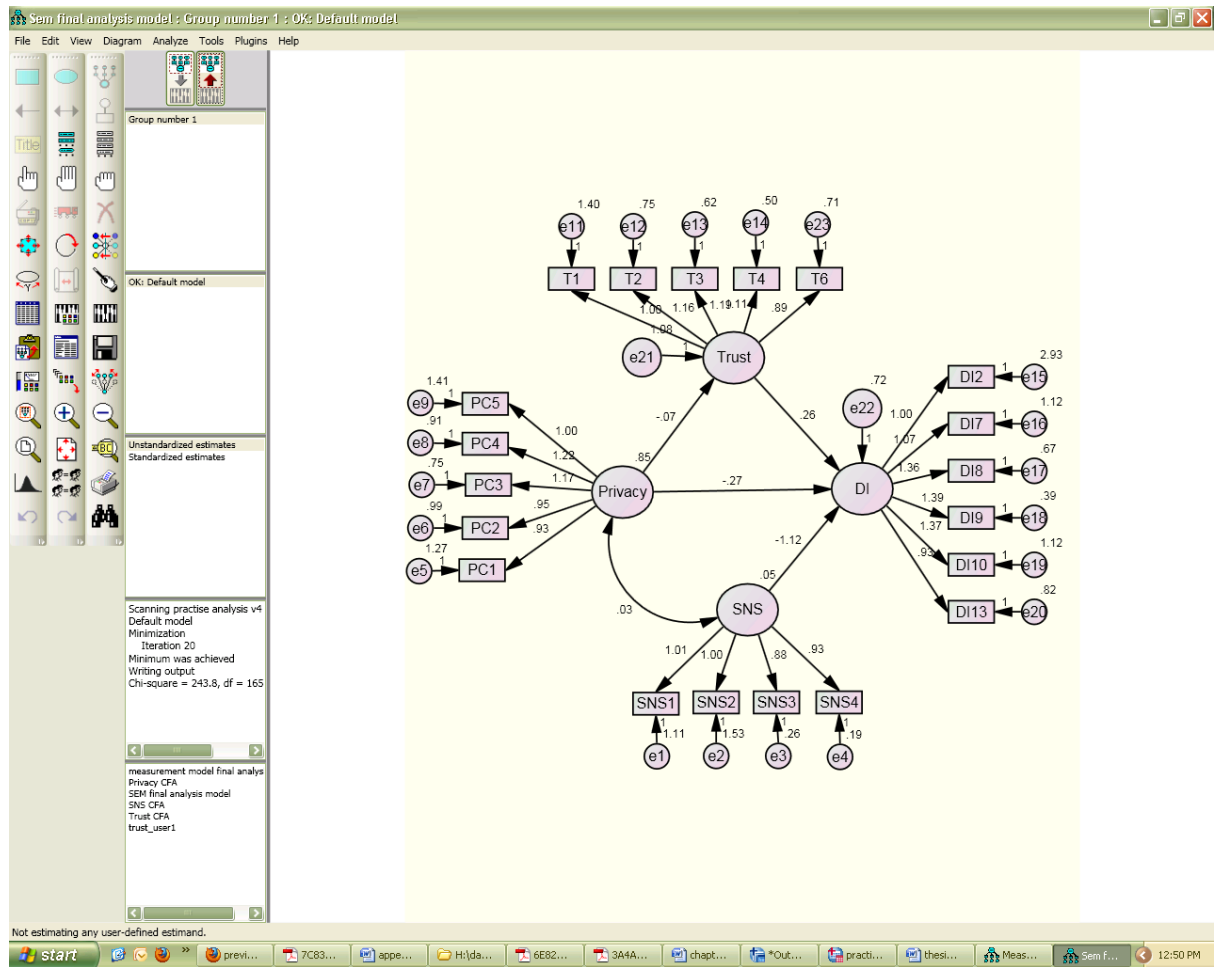
Snapshot of AMOS output of analysis summary for structural model

The snapshot below describe the analysis summary of the output of AMOS , where we can see the time and model name which is analysed.
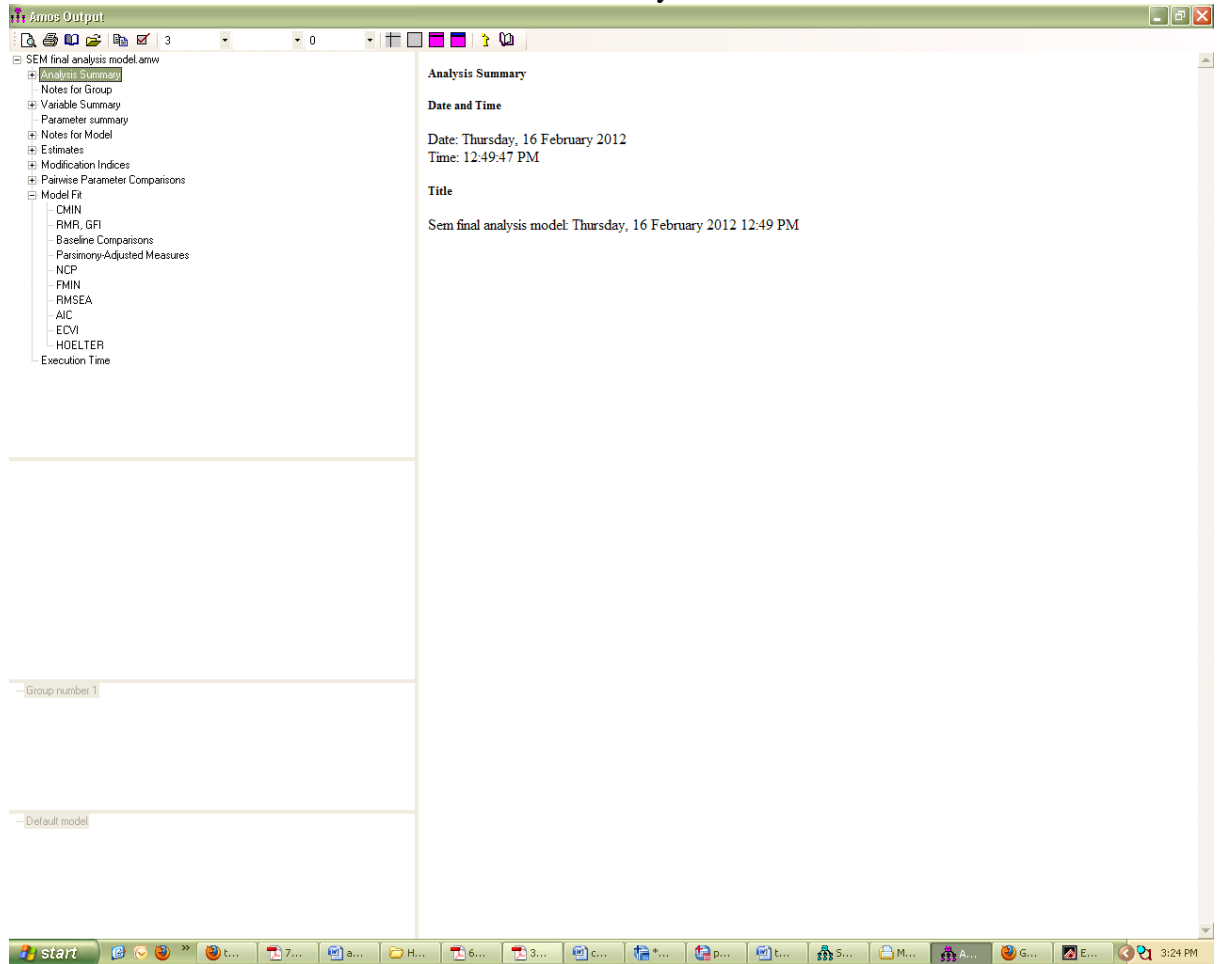
The snapshot below shows the summary of the variable used in model. The details of variable are also shown in table below:
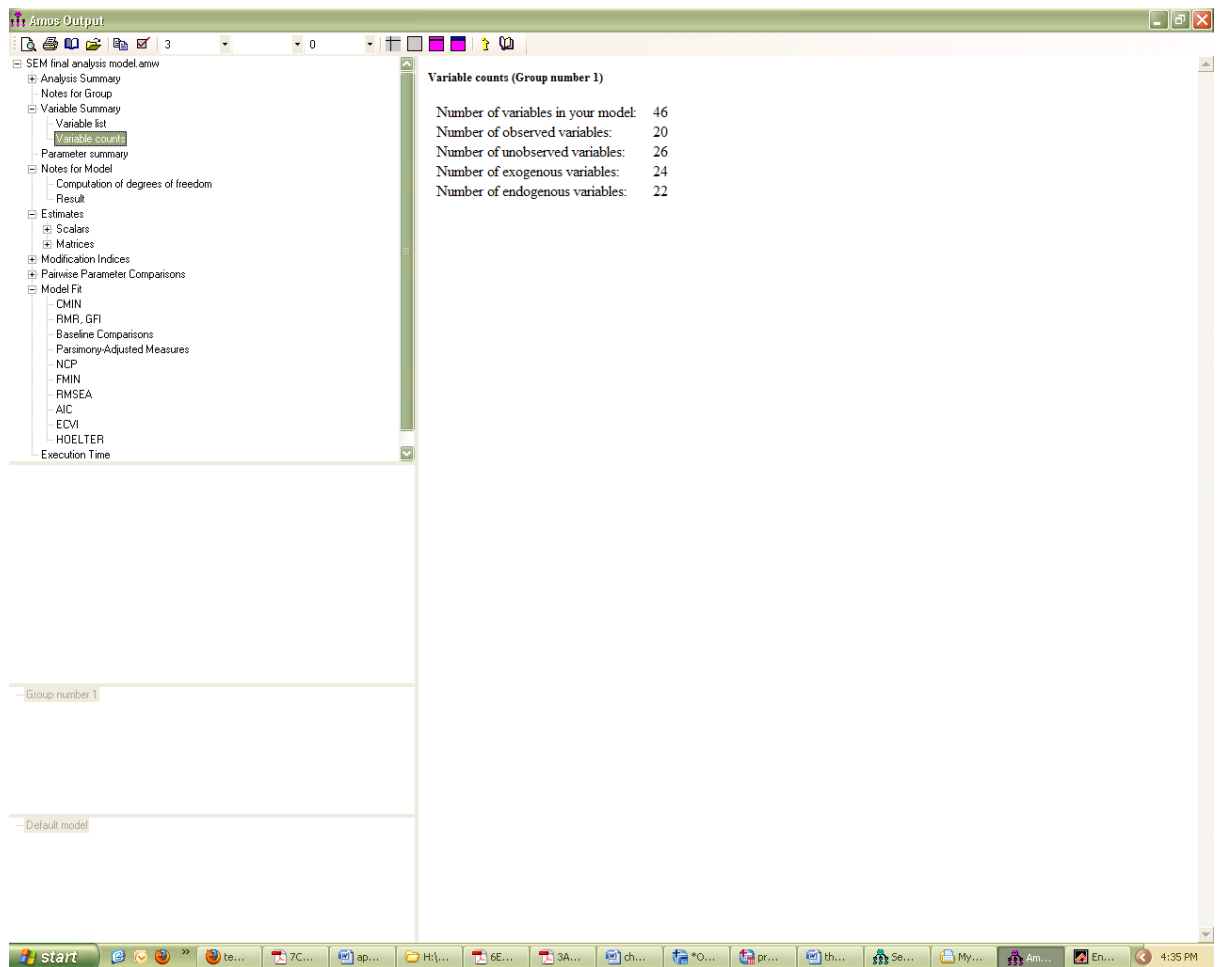
Variable counts (Group number 1)

Number of variables in your model:	46
Number of observed variables:	20
Number of unobserved variables:	26
Number of exogenous variables:	24
Number of endogenous variables:	22

Snapshot of AMOS output of structural model parameter summary

	Weights	Covariances	Variances	Means	Intercepts	Total
Fixed	26	0	0	0	0	26
Labeled	0	0	0	0	0	0
Unlabeled	20	1	24	0	0	45
Total	46	1	24	0	0	71

Snapshot of AMOS output of structural model
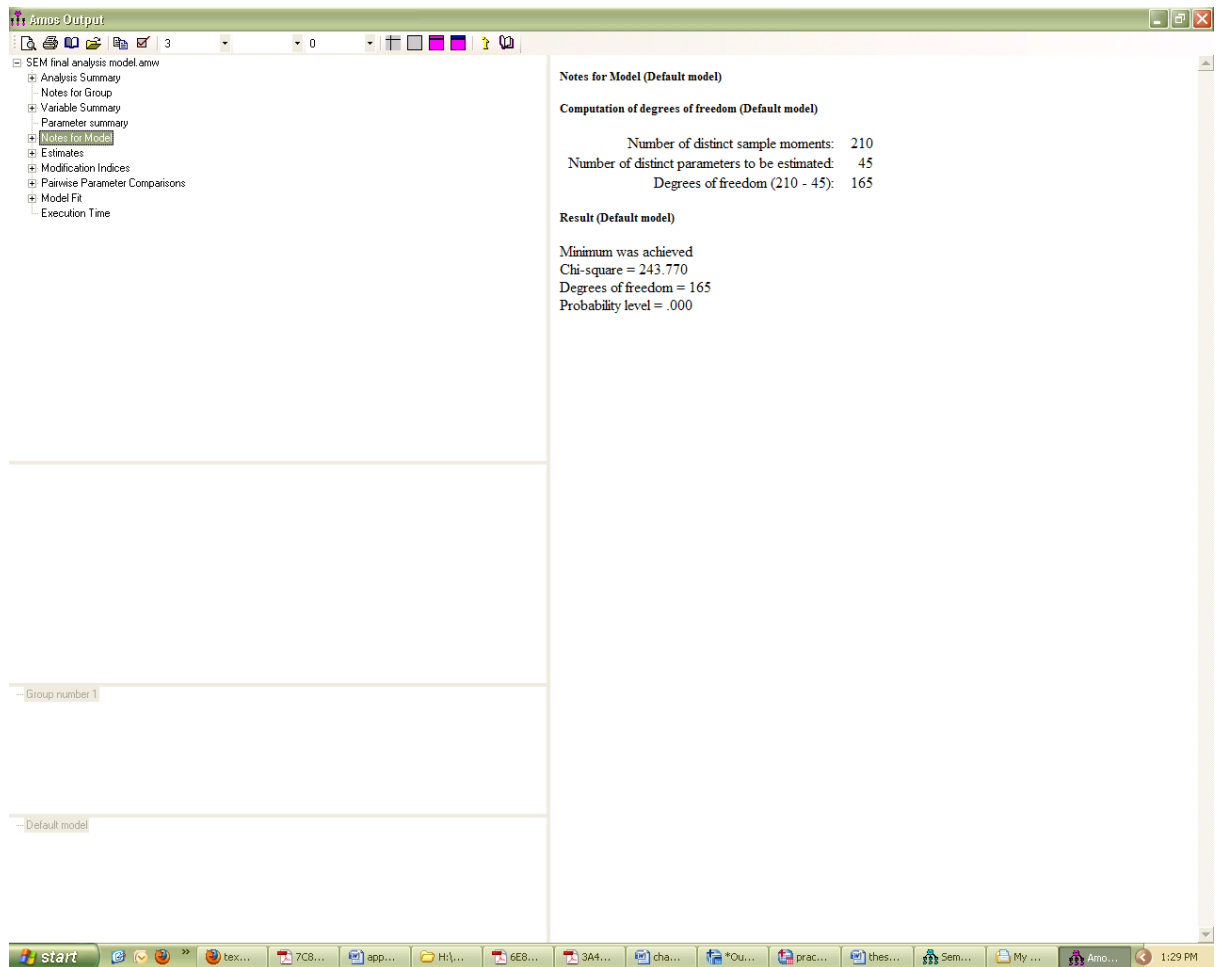
Number of distinct sample moments: 210
Number of distinct parameters to be estimated: 45
Degrees of freedom (210 - 45):   165

This Chi-square tests the null hypothesis that the over identified (reduced) model fits

the data as well as does a just-identified (full, saturated) model. In a just-identified

model there is a direct path (not through an intervening variable) from each variable

to each other variable. When we delete one or more of the paths we obtain an over

identified model. The non-significant Chi-square here indicated that the fit between

our over identified model and the data is not significantly worse than the fit between

the just-identified model and the data While one might argue that non-significance of

this Chi-square indicates that the reduced model fits the data well, even a well-fitting reduced model will be significantly different from the full model if sample size is sufficiently large.   A good fitting model is one that can reproduce the original variance-covariance matrix (or correlation matrix) from the path coefficients, in much the same way that a good factor analytic solution can reproduce the original correlation matrix with little error.
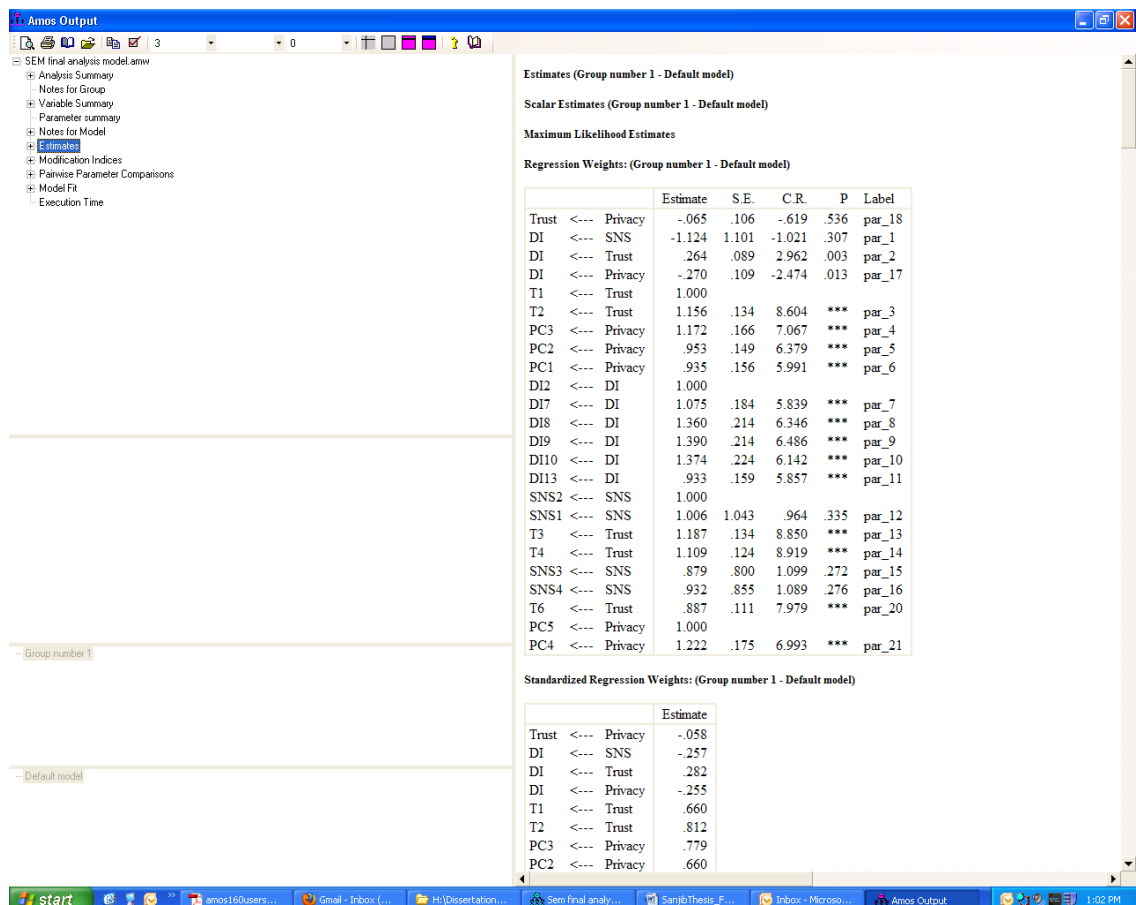
			Estimate	S.E.	C.R.	P	Label
Trust	<---	Privacy	-.065	.106	-.619	.536	par_18
DI	<---	SNS	-1.124	1.101	-1.021	.307	par_1
DI	<---	Trust	.264	.089	2.962	.003	par_2
DI	<---	Privacy	-.270	.109	-2.474	.013	par_17

	Estimate

153

	Estimate
Trust <--- Privacy	-.058
DI <--- SNS	-.257
DI <--- Trust	.282
DI <--- Privacy	-.255

	Estimate	S.E.	C.R.	P	Label
SNS <--> Privacy	.025	.038	.667	.505	par_19

Below are the simple correlations between exogenous variables.

	Estimate
SNS <--> Privacy	.124