LUND UNIVERSITY
School of Economics and Management

Privacy and Information Sharing on Social Networking Sites

Edwin Leonardi Liong and Tobias Mejstad

Master's thesis in Informatics, 15 HEC

Supervisor:
Paul Pierce

Examiners:
Agneta Olerup
Magnus Wärja

Seminar Date: June 10, 2010

Edwin.Leonardiliong@hermes.ics.lu.se
tobias.mejstad.762@student.lu.se

Title	Privacy and Information Sharing on Social Networking Sites
Authors	Edwin Leonardi Liong Tobias Mejstad
Publisher	Department of Informatics
Supervisor	Paul Pierce
Examiners	Agneta Olerup, Magnus Wärja
Presented	June, 2010
Thesis type	Master's thesis
Language	English
Keywords	social networking sites, social exchange theory, privacy, information sharing, gender, age, geographical background, quantitative

Abstract

Social networking sites are becoming more and more widely used, increasing their importance as vehicles for communication and collaboration. Due to this, a significant amount of information is shared on these sites, with considerable potential implications for the area of personal privacy. There have been reports that the users of these sites do not understand the potential harms of information-sharing. In our study, we examine individuals' perceptions of privacy as they relate to these sites as well as how these perceptions differ between genders, age groups and geographical backgrounds.

Using quantitative methods by surveying 240 individuals we find that they are, indeed, highly concerned about their privacy, both on the Internet and on SNS. Furthermore, even if they share a significant amount of information on these sites, they are both aware of and make use of the privacy settings available to them. However, we find that the terms and agreements and privacy policies pertaining to these sites are not important factors influencing the decision of whether or not to get involved in them. Our findings make us conclude that individuals are performing cost and benefit analyses related to their level of participation and information-sharing, in line with the social exchange theory.

Our study also confirms that the phenomenon of information disclosure on SNS is to some extent associated with the user's gender and age, as has been suggested in previous studies. However, we find differences concerning the specific characteristics of privacy awareness and privacy protection on SNS as compared to previous studies. Finally, we examine these areas with respect to geographical backgrounds, and discover differences not previously reported.

Table of Contents

1. Introduction

The emerging phenomenon of social networking sites (SNS[1]) has over the recent years gained widespread popularity among people of various demographic backgrounds including age, gender and nationality. With growing media coverage and polarizing public perception, SNS remains an interesting topic to discuss. The early adopters as well as the early majority have seen the benefits to participate in this social environment whereas the late majority and the laggards are not aware of the hype or, alternatively, do not yet see the point in following the trend. But even considering this success in growing participation, SNS have met with several disputes including access to the site being banned in several countries (MacDonald, 2009) and also at workplaces (Benzie, 2007). Numerous researchers, performing both qualitative and quantitative research have explored different areas of SNS such as the adoption (including influencing drivers and detractors), prevailing ideas of Web 2.0 as well as demographic and privacy related research questions. These have sometimes been cross-disciplinary studies as well as articles that have been associated with and have contributed to the medical field (Farmer, et al., 2009), cultural studies (Harrison and Thomas, 2009), education (Griffith and Liyanage, 2008) and the world of business and marketing (Clemons, et al., 2007; Harris and Rae, 2009).

According to Boyd (2006), a SNS is defined as *"a category of websites with profiles, semi-persistent public commentary on the profiles and a traversable publicly articulated social network displayed in relation to the profile"*. Some forms of SNS such as Friendster, Facebook and MySpace allow people to create an account, upload their profile and then make connections to other members of the sites traversing the network. But what are the primary reasons for being part of SNS? Motivations to participate vary from making new acquaintances with people, maintain relationships with existing friends and known coworkers, posting photos and testimonials and sharing experiences to sharing personal updates (Dwyer, et al., 2007). Also, people want to engage in identity expression and like

[1] SNS will be treated as both singular and plural throughout the entire document

to ‘see and be seen’ (Tufekci, 2008). The latter is also being supported by individuals using the SNS to find out what is going on in other people’s life.

As these SNS have become more and more sophisticated, they enable the storing of different types of information which the users are naturally tempted to provide. We find it interesting yet strange that people seem to reveal so much personal information about themselves on a public site. As a matter of fact, nobody is literally forced to join these sites and certainly not forced to reveal their personal data (Acquisti and Gross, 2006). As for the information on one’s SNS profile, it ranges from basic data and contact details to personal interests and multimedia content like pictures and videos. This means that the amount (richness) and value of the information is interesting to examine too. For example, users can attach rich media to customize their profiles as well as using less rich media, for example by simply describing their personality traits, experiences and hobbies with a snippet of text.

Developing in parallel, ever since the rise of the Internet, has been the erosion of privacy among individuals. It has shown itself as fear of information being disclosed, for example when an individual makes transactions online in communicative (social) arenas through multiple channels such as forums and chat rooms. Likewise, SNS may offer significant value to the users, but at the same also raise privacy concerns. Gross and Acquisti (2005) note that in certain situations, people are willing to reveal personal information even to individuals that they do not know at all. Also, the open nature of SNS has given opportunities for many individuals and parties to easily target the users, capitalizing on the users’ behavior on SNS related activities. For example, the organization behind the SNS may lay claim to provided information, or it may allow external search engines access to it. It has been said that information given out on the Internet is ‘there forever’, meaning that individuals would be wise to be careful regarding what information that is shared on the Internet in general and, arguably, on SNS in particular as they harbor vast amounts of personal information. However, there have been indications that individuals are not aware of the implications of sharing information online as recent examples of employees losing their jobs (Matyszczyk, 2009) and home-owners having their houses

broken into (Chetry, 2010), facilitated by information shared online have shown. Based on this worrying development, we have determined to explore the area of privacy on SNS from the individual's perspective.

1.1 Problem Area

On SNS, users often enhance their profile and engage in activities that include sharing and exchanging information with other members. A study by Jones and Soltren (2005) states that privacy on SNS is breached due to the users disclosing too much information, with third parties getting hold of it. The risk of information disclosure has been repeatedly associated with identity theft, stalking and various forms of cyberattacks (Gross and Acquisti, 2005). This exposure of sensitive information may cost people their career and personal relationships as well as public embarrassment in the society (Tuunainen, et al., 2009). Advertisement organizations may also collect and use personally identifiable information to deliver tailored ads, without explicit consent from the user (Hoy and Milne, 2010). Other organizations are also interested in the information about individuals that may be found on these sites. Ofcom (2008a) gives examples of educational institutions examining details of prospective and current students and employers and recruitment agents screening the SNS profiles of candidates and current employees. In addition, several studies have indicated that SNS users are lacking in the awareness of potential threats as well as lacking in adequate initiative to engage in privacy protection behavior. For example, a majority of users do not pay attention to the SNS' terms and conditions and privacy policy agreements (Jones and Soltren, 2005; Govani and Pashley, 2005; Tuunainen, et al., 2009; Mohtasebi and Borazjani, 2010) and are furthermore not using the privacy settings provided in the SNS to protect the accessibility of their profiles (Gross and Acquisti, 2005; Govani and Pashley, 2005; Mohtasebi and Borazjani, 2010). The magnitude of the mentioned concerns becomes more and more significant as the SNS continue to gain an even more massive audience.

In examining the research conducted within this area, we find that this area is not adequately explored. More specifically, the links between users' perceptions and their actions on SNS are not fully understood (see Tufekci, 2008; Fogel and Nehmad, 2009; Tuunainen, et al., 2009). Consequently, in our study, we first seek to explore users' general attitudes and perceptions towards these websites in regards to privacy concerns, particularly as they pertain to information disclosure, awareness and privacy protection behavior. This leads to our two first research questions:

RQ1: What are the overall prevailing attitudes towards privacy as they relate to social networking sites?

RQ2: What are the relationships between these privacy attitudes and their manifested behaviors?

Second, we find it worthwhile to analyze if there are any differences between demographic groups in regards to privacy concerns on the Internet and on SNS, particularly related to the aforementioned areas of information disclosure, awareness and privacy protection behavior. This can be argued because previous research has hinted at the possibility of there existing demographical differences within this area (see Fogel and Nehmad, 2009; Tufekci, 2008; Hoofnagle, et al., 2010). Thus, we extend our research area by examining differences based on gender, age groups and geographical backgrounds. From this, our second research question is stated as:

RQ3: How do these privacy attitudes differ between genders, age groups and geographical backgrounds?

1.2 Purpose

The aim of this study is to assess the attitudes related to privacy and information sharing on SNS as well as to further explore the relationships between these areas and how they differ in relation to demographical backgrounds.

1.3 Delimitations

Since we take Boyd's (2006) definition of social networks into consideration, SNS in this study refers to those sites that offer general profile-building functionalities while not necessarily including other characteristics of social networking services such as microblogging, Really Simple Syndication (RSS), photoblogging or Wikis. More specifically, we have limited ourselves to studying one of the SNS in depth (Facebook[2]), a choice which we motivate further in the methodology section.

When studying geographical backgrounds we limit ourselves to assessing differences between continents as opposed to between countries. The reason for us doing this is related to the data analysis, which necessitates a certain number of data points. This, too, will be further elaborated on in the methodology section.

1.4 Motivation and Approach

As previously stated, the area of risk-taking and privacy on SNS is a rather new phenomenon that has not been explored enough. Therefore, we find it worthwhile to build on other researchers' research by performing our own study within this field. Our study will give insights into the social science field regarding SNS users' general perception of risk-taking and privacy associated with their use of these sites, and also how the perception may differ between different demographic groups. This topic is worth investigating because the findings can assist and inform organizations in any way

[2] This study includes notes and references to Facebook's terms and conditions as well as its privacy policy. We base these on the revision dated April 22, 2010. The excerpt of this can be found in the Appendix.

involved in or affected by SNS by taking into consideration the attitudes and the behaviors of their users in general, and a specific demographical group (based on age, gender or geographical background) in particular. From studies evaluating the area of online shopping, we already know that users place a high value on privacy and security (Seock and Chen-Yu, 2007) of such web sites. This could be the case for SNS as well, as more and more sensitive information is being stored on these sites. Such knowledge, we argue, will become more and more necessary for being able to create a successful SNS. As an increasing number of organizations compete with each other in this area by trying to create the most attractive site to attract users, we argue that knowledge concerning this area is essential.

But even organizations operating chiefly within other industries not primarily related to the Internet are creating their own SNS in the form of, for example, forums on Intranets. Having knowledge of users' attitudes within this area may, for example, help them create a SNS better tailored to the users' privacy needs. As a consequence, the users would feel safer, and information that would not have been shared otherwise would now be shared. This, in turn, would have a natural effect on collaboration. We also note that our findings may serve as public information concerning the possible need for awareness of privacy and information sharing on SNS by encouraging reflection on part of the users, eventually leading to a change in their perceptions regarding these areas.

On an academical level, we find this topic worthy of study as previous studies have been severely limited regarding their research methodology. In contrast to these, we do not restrict our survey to only including university (college) students with detrimental results for the sample quality as a consequence. Rather, we expand it to include a wider range of demographic characteristics, especially as they relate to heterogeneity in age, gender and geographical backgrounds. We assume that by basing our study on such demographic heterogeneity, different perceptions of the area, in comparison to what other researchers have found, will be made visible. In our methodology chapter we will elaborate further on the characteristics of our sample and its possible implications. Furthermore, we dare to say that most previous studies have not been as strict or, similarly, highly limited in their

treatment of statistical tests, with the implication that their results may not be providing sufficient insights into this area. Lastly, researchers within this area have, overall, found contradictory evidence highlighting the fact that this is a new area and therefore in need of exploration. We consequently argue that our study can help explore it further and, in combination with other studies, continue to form a basis on which to proceed studying this field.

1.5 Structure of the Report

The report is organized as follows:

Chapter 2 contains our literature review introducing the concept of SNS in general and Facebook in particular. We follow up by highlighting previous works related to privacy concerns in the use of SNS and, surrounding our discussions of the aspect of information disclosure, third parties' interest in users' information and users' awareness of privacy as well as their privacy protection behavior. In addition, we present other studies that report differences in privacy perception depending on age, gender and geographical regions as they relate to online activities in general and SNS in particular.

Chapter 3 includes our theoretical framework which is based on the social exchange theory. We relate this theory to the information exchange relationship that takes place when the users actively engage in SNS activities.

In Chapter 4, our methodology chapter, we elaborate on our research approach and how we constructed the questions for our questionnaire. We present our data collection strategy, foresee sampling and non-sampling errors and proceed to discuss ensuring the reliability and validity of our measurements. Ethical issues and biases are also considered and addressed. We end the chapter by summarizing the various statistical tests that will be performed as part of our analysis, along with motivating our choices.

Chapter 5 contains the presentation and discussion of our analysis and results for the studied variables based on the collected responses. Findings based on descriptive statistics, correlation analyses, linear regression and tests for differences across demographic characteristics are cross-referenced with the tables and graphs in the Appendix.

2. Literature Review

2.1 Social Networking Sites

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. As of this writing, there are hundreds of SNS offering different types of services to individuals and groups with shared interests[3]. These SNS display great diversity in user bases across genders, age groups and specific geographical regions. Boyd and Ellison (2007) present the history of SNS since 1997 when SixDegrees.com was launched. They document the timeline up to late 2006 including 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. Among the SNS found in the list, Facebook, MySpace, LinkedIn, Hi5, and Friendster are notable and well-known sites. Also, taking a closer look at these SNS, it is not surprising that many of them resemble each other in the design and layout, as well as by offering similar features to their users.

SNS provide users with an efficient way of setting up new relationships and managing existing ones as well as catching up with old friends (Ofcom 2008a). Ofcom (2008b) categorizes SNS adopters into five distinct groups based on how they make use of the SNS (see Table 1). These sites are made convenient for the users with friendly interfaces and easy-to-follow instructions. In no time, a novice user will get acquainted with the pattern of use and receive hands-on experience with respect to various functionalities. For communicating and maintaining relationships, the user engages in activities such as updating others on his whereabouts, sharing pictures and archiving events, noticing updates from 'friends' activities, communicating using private messages as well as posting comments and public testimonials (Dwyer, et al., 2007). In SNS, people in one's connection are often designated as 'Friends'. Boyd (2004) notes that "*When traversing the*

[3] http://traffikd.com/social-media-websites/

network, there is no way to determine what metric was used or what the role or weight of the relationship is. While some people are willing to indicate anyone as Friends, and others stick to a conservative definition, most users tend to list anyone who they know and do not actively dislike. This often means that people are indicated as Friends even though the user does not particularly know or trust the person" (Boyd, 2004, p. 2). It is important, then, to clarify that the term 'Friend' used in the context of SNS is unlike the conventional definition of a 'Friend' we use in the real world. Thus, throughout this report, we will refer to the term 'Friend' as anyone who has been permitted to join one's group of friends on a SNS.

Group	Style of use	Typical sites
Alpha socialisers	Flirting, searching and meeting new people (usually of the opposite sex)	Bebo, MySpace, Hi5
Attention seekers	Posting photos portraying lifestyles	Bebo, MySpace, ICQ
Followers	Following trends and keeping up with friends, peers	Bebo, MySpace, Facebook, Hi5, ICQ
Faithfuls	Finding old friends and keeping in touch	Facebook
Functionals	Looking for people with shared interests and hobbies	Facebook, MySpace, Bebo

Table 1: Annex 3: Social Networking Qualitative Research Report (Ofcom, 2008b)

Ofcom (2008b) points out that SNS allow some users to boost their confidence while others simply find the activities on SNS entertaining and fun. Some sites, such as MySpace and Friendster, even allow their users to customize and decorate their own profile, changing the layout and background theme with easy-to-use editors and customization tools. However, users may get addicted to the sites and distracted from work (Dickinson, 2010) and studies (Patel, 2007). Other concerns relate to the previously stated and highly debated privacy and safety issues. Moreover, Ofcom (2008b) has found that factors such as age, gender, personality type, status of relationship, Internet access and geography are affecting the users' behavior pertaining to the use of SNS.

One of the most prominent and up-to-date SNS is Facebook. Facebook was founded in February 2004 and initially not made available to everyone. It was originally developed for the students at Harvard College and within a month, most of the undergraduate population already had a profile there. A few months later, the site had gradually expanded to most of the universities in North America. In 2005, a new domain name, Facebook.com, was obtained and soon it started to allow its membership to include US high schools as well as UK universities. Finally, in September 2006, Facebook was made open to anyone of the age 13 or older with a registered e-mail address (Phillips, 2007)[4]. Like many other SNS, the site remains free to join. It also continues to dominate the Internet in terms of its growing number of visitors. As such, Facebook can also be used to funnel visitors to one's website or blog (Taylor, 2010). Ofcom (2008a) moreover reports that some users may use their profile for small-scale business purposes, including commercial products and services.

Similar to the concept of other SNS, Facebook is a tool that helps people to communicate effectively with friends, families and peers. Users can navigate the core functions of the site including managing their 'Profile', checking and replying to 'Messages' as well as accepting friend 'Requests'. Users are free to post status updates and share links, photos and videos with their connections. Each user's profile page has a 'Wall' space that allows friends to write messages to the user and see the user's recent activities on the site. On top of these functions, Facebook provides first-party applications such as uploading 'Photos' and 'Videos', tagging people in them, joining 'Groups', participating in 'Events' and composing 'Notes'. Over time, Facebook introduces and adds new features to its site to create an even richer user experience. The Facebook 'Chat' offers an alternative way for users to interact with friends in real-time while Facebook's 'Gift' feature enables virtual gift giving among users. The Facebook 'Marketplace' feature allows users to post free classified ads for selling items and properties as well as finding job vacancies. The functions and features mentioned above are among the users' favorite features and represent some of the many available that encourage interactive activities on Facebook.

[4] A complete walkthrough of Facebook's journey is available at http://www.facebook.com/press/info.php?timeline

In addition, the overall activity on Facebook has been increasing due also to the site being made accessible through the users' mobile devices. Ever since that, mobile operators have helped to promote and support Facebook's mobile products.

2.2 Privacy within SNS

SNS appear to provide significant value to the users, in ways which have been described in the previous sections. But at the same time they also raise privacy concerns. There have been previous studies examining social networks that have inquired into the privacy area. In this chapter, they will be showcased in their respective segments, based on their significance to our research questions. In general, these studies have embraced the exploration of 'privacy risks', 'awareness', 'privacy concerns', 'trust', 'information revelation', 'security' and 'privacy protection'. We adopt several findings from these previous studies of SNS as a basis for discussing and analyzing our own findings. Therefore, areas that will be included are the over-disclosure of information and third parties' interest in the users' information as well as the lack of users' awareness of threats and privacy protection behavior.

2.2.1 Information Disclosure

To be granted membership on a SNS, the user is required to provide at least some basic information. Facebook, for instance, asks users to fill in their name, e-mail address and birth date. Upon successful registration, the user can complete his profile with more detailed personal information such as interests, relationship status, political views and so on. What information the user wants to show in his profile is entirely up to his preference and decision. Tufekci (2008) reports that Facebook users are predominantly using their real name in their profile and studies by Tuunainen, et al., (2009) and Christofides, et al., (2009) reveal that users are very likely to have a profile picture on their Facebook profile and also show information such as their hometown, birth date, e-mail address and educational background. Tuunainen, et al., (2009) also finds that the street or home

address and contact phone number is the information that is least likely to be disclosed. On hosting public profiles on SNS, Utz and Krämer (2009) notice that people tend to try to make a good impression in front of others, for example to impress potential employers or dates by displaying information that reflect *"highly socially desirable identities"* (p. 2). Thus, for all we know, some of the profiles of other members that we as SNS users view are likely to be exaggerated to make them look more appealing. In addition, the need to be popular is shown to be one of the key motivations for people to share information with others on SNS (Christofides, et al., 2009). Other factors that may cause the phenomenon of information revelation include changing cultural trends and rising confidence levels when it comes to technology as well as herding behavior and peer pressure (Acquisti and Gross, 2006).

SNS have become increasingly versatile by inventing new functionalities, and have been doing well to retain their users in doing this. These sites have been enhanced to support multimedia content such as tagging people in photos and uploading videos. Some of the features have facilitated and encouraged information exchange among the participants, but at the same time the idea has been panned with criticism from the public. For instance, Facebook caused controversy when it first introduced the 'News Feed' feature in 2006. This is due to the feature pelting the user with undesired information as well as the detrimental effects on personal privacy it caused. The design is such that when a user logs into his Facebook account, he will be directed to an alternative home page with the 'News Feed' displaying the current information about his friends' whereabouts and their Facebook activity. This information is most often willingly provided by the individual's friends and thus intended to be shared and distributed for others to be able to catch up with their latest updates. Similarly, whenever a user wants to acknowledge 'friends' of his new updates, he may do so upon giving his consent to Facebook that his updated or new information will subsequently be published to his connections' 'News Feed'. The issue here is that the information is disseminated so rapidly and broadly, in a sense flying all over the SNS that one may not realize the risk level of exposure of the information revelation. In addition, Facebook (2010a) gives a figure of as much as 25 billion pieces of content being shared each month.

Thus, when an individual has a profile on a SNS, he knowingly and unknowingly may have shared information with potentially hundreds or even thousands of the other registered members. For example, whenever you post a comment or message on your friend's wall, other people in your friend's friends connection get to see it. Another example could be you being in one of the pictures taken at a party and the photo uploader (who may or may not be in your 'friend' list) is able to tag you and to include your name in the photo description, meaning that your photo identity becomes visible to a plethora of people. Also, SNS users have no control when it comes to the persistence and durability of their information on the site. Here, we also want to highlight that when an individual removes information from his Facebook profile or delete his account, copies of the information may remain viewable elsewhere (Facebook, 2010c). But it does not end there; the information might actually be reshared or copied by other users (Facebook, 2010c). The Get Safe Online Report (2007) discovered that people do indeed post other people's information and photos as well as pass on contact details without the original owner's consent.

Gross and Acquisti (2005) enumerate several privacy risks pertaining to information disclosure, including real-world and online stalking, data re-identification (based on demographic information or face recognition) and substantial risks of identity theft (phishing). Information like the full birth date can be used by other people to gain access to bank or credit card accounts (ConsumerReports.org, 2010a) and a user's Facebook profile picture can be used by somebody else in a dating site profile (ConsumerReports.org, 2010b). Moreover, a report published by Legal and General (2009) named 'The Digital Criminal' explains that SNS are opening up opportunities for burglars to get to know their target simply by studying the victim's public profile (home address information) and monitoring his social networking activity (online stalking). The report furthermore provides the same advice as many others have; that social networkers should avoid posting status updates and details about them going on vacation or leaving their house unattended**.** To some people, this may sound excessive, even paranoid. Nevertheless, that such easily available information invites both digital and ordinary crime is not hard to imagine. The Get Safe Online (2007) report also highlighted that

through SNS, 29% of the users look up their ex-boyfriends, ex-girlfriends, coworkers, employers, or bosses to learn what is going on in their life. In addition, Gross and Acquisti (2005) emphasize that the privacy implication of sharing sensitive information such as sexual orientation and political views may not have an immediate impact on the users. But that in few years from now, the exposure of this information may jeopardize their career and public perception in the society. Indeed, privacy loss and poor control over personal information may cause serious consequences that are socially irreparable (Tuunainen, et al., 2009). SNS have also been criticized for being misused to exacerbate cyberbullying, as the case of a 15-year-old schoolgirl Megan Gillan who committed suicide after being teased on the SNS Bebo (Moore, 2009).

At first glance, users may seem naïve when seeing no potential harm in disclosing basic information to others. But might there be a difference in disclosure depending on how 'sensitive' the information is? Then again, the definition of 'sensitive' is subjective to how a user values the privacy of that information. After all, according to Lang, et al., (2009), people are still less likely to post 'sensitive' information about themselves. Finally, Tufekci (2008) finds that in general the privacy concerns of a user is not of much relevance to his decision to disclose personal information. Tufecki (2008) instead suggests that the information disclosure on SNS is affected by the demographic characteristics of the users. Details on the demographic differences towards privacy concerns will be provided in the forthcoming part of this chapter.

2.2.2 Third-Party Interest in Information

Gross and Acquisti (2005) state that the SNS and its third parties have the capability to access the participants' information. They also see the possibility of third parties building a digital dossier to store information pertaining to the SNS' participants. This information could be personally identified, extended and shared for use among the social networking organization's client companies. Advertisers have seen the huge increase in SNS adoption and are utilizing the information available in the user profiles to deliver

personally tailored ads to the users based on their unique individual interests and demographics (Hoy and Milne, 2010). They can capitalize on the 'friends of connections' tactic to expand their target to Facebook users whose connections are also linked to specific pages, groups or applications (Hoy and Milne, 2010). As of this date, no protection of information is guaranteed on Facebook as *"Facebook is not responsible for the actions, content, information, or data of third parties"* (Facebook, 2010d). Exacerbating the problem is that the users generally seem to assume that their privacy is looked after by the SNS (Ofcom, 2008b).

Facebook users may notice plenty of applications available to them that come in great varieties of forms and purposes. Many of them are third-party applications, meaning that they are not developed or maintained by the Facebook organization. Some of these applications are quizzes and games which can be downloaded by any user. Likewise, any user may create applications for all other users to install and run. Facebook (2010a) reports that there are about 550,000 active applications currently on the platform, and more than 70% of all users engage with the applications monthly. Despite this, one might not know until one examines Facebook's terms and conditions that *"when you use an application, your content and information is shared with the application"* (Facebook, 2010d). While some of these applications may not seem harmful to add to one's profile, they can be malicious programs disguising to invade the user's computer. As a case in point, BBC Click managed to show a security flaw in Facebook by means of a data mining application that was able to steal the personal details of a person and all of his Facebook friends without him knowing (Kelly, 2008).

In addition, there have been numerous examples of organizations using information found on SNS for their own interest to the detriment of the particular user in question (TT 2009, 2010a, b; Jacobsson, 2009). A study by CareerBuilder (2009) found that as many as 45% of all employers are using SNS to screen potential employees, with sites such as Facebook and LinkedIn being the most frequently checked. Out of all employers, 35% stated that they had found information when searching through these pages that did, in fact, contribute to the person in question not being hired. The reasons for not being hired

ranged from having inappropriate photographs in one's profile to sharing sensitive information and showing poor writing skills. At the opposite end, only 18% of all employees reported that they had hired a person based on the information found on SNS (CareerBuilder, 2009). This would suggest that, all other things equal, an individual is better off sharing less information on SNS when it comes to maximizing employability.

2.2.3 Awareness and Privacy Protection

Like in most online communities, before participating in a SNS, a user is required to agree on its terms and conditions as well as its privacy policy. By accepting the terms, the user abides to ground his behavior on the SNS on these terms, including respecting other users' rights (Facebook, 2010d). The privacy policy usually outlines how the company collects and can use the user's content and information. However, studies such as Jones and Soltren (2005), Tuunainen, et al. (2009) and Mohtasebi and Borazjani (2010) have found that most users do not read the SNS' terms and conditions and privacy policy. For instance, according to a study of users' awareness of privacy on Facebook, over 70% of the respondents were actually not aware that Facebook can share the users' information with third parties, and even those 61% who had read Facebook's privacy policy were not aware of this fact (Tuunainen, et al., 2009). This indicates that people still have inadequate knowledge and understanding regarding where and how their information can be used and exploited. In any case, Facebook's terms and privacy policy alone do not promise the users immunity from breach of their privacy. It is stated in the most recent Facebook terms that Facebook *"do not guarantee that Facebook will be safe or secure"*, and that the users *"use it at [their] own risk"* (Facebook, 2010d). Also, over the years, Facebook's privacy policy has gone through numerous revisions and recently it has been spotted that these changes have actually eroded the users' privacy (Opsahl, 2010).

As has been implied earlier, the relationship established through a SNS is not necessarily a 'friend' relationship (Boyd, 2004). People that are barely recognized by the user and possibly even those that the user has never met before will be considered 'friends' in the

user's profile once they have been added to the user's 'friend list'. With this, the SNS has given liberty to the users to initiate a connection with whomever the users intend to befriend. Adding people as new connections means that you allow these people to view your profile and that you share your personal information with them. Despite the SNS providing an easy way for the users to establish relationship with people, studies such as Jones and Soltren (2005) and Lang, et al. (2009) have shown that most of the users would never accept a 'Friend' invitation or request from a stranger, indicating that people are generally insecure of expanding their network to include unknown persons and that they are certainly not comfortable being 'seen' by strangers. Thus, a user's strategy of being selective in befriending can be seen not only as sense of awareness, but also as a form of privacy protection behavior.

In addition to privacy protection, SNS like Facebook provide privacy settings that enable the users to control the visibility of their information. A user can control who can see his profile, who can post on his wall and who can interact with him on Facebook. He can also edit his profile to hide all (or some) information fields such as birthday or gender from other users. Though as an exception, the user name and profile picture do not have privacy settings (Facebook, 2010c), even if it is possible to include a fake picture as well as a nickname. Facebook (2010b) offers privacy settings based on the three basic levels of privacy: Friends, Friends of Friends, and Everyone. There is no clear cut or optimal privacy setting scheme for each individual, it lays on the users to decide which setting that is best suited for their needs. Utz and Krämer (2009) argue that choosing the appropriate settings is *"a dynamic process"* (p.8). Facebook (2010b) recommends that basic information such as 'About Me' and posts (photo albums and status updates) are allowed to be viewed by 'Everyone', while recommending the settings 'Friends of Friends' or 'Friends' for more personal information such as birthday, religious and political views, and contact information.

Interestingly, there have been mixed findings concerning users' attitudes toward the privacy settings provided by SNS. Gross and Acquisti (2005), Govani and Pashley (2005) and Mohtasebi and Borazjani (2010) reveal that only a small percentage of users make

use and configure the privacy settings in their profile while other studies (Jones and Soltren, 2005; Get Safe Online, 2007; Tuunainen, et al., 2009; Utz and Krämer, 2009) report that a vast majority of the users are familiar with these options and have utilized them accordingly. We argue that the privacy settings are necessary and, thus, users should at least make an informed decision regarding their privacy settings, although they may end up neither making any changes from the default settings nor using the feature to its fullest extent. As an example supporting our argument, when a SNS user wants to look up other users within the SNS' database, he can conveniently perform a search query using terms like a name or an e-mail address. If these users in the search results have not changed their privacy settings for all of their information from the default level ('Everyone'), their full profiles are accessible. Practically, the inquirer does not even need to be in the specific user's connections (group of friends) in order to access his personal information. Facebook (2010b) also states that *"any information that is visible to Everyone may be seen by everyone on the Internet"*. This includes being visible in search engines and through RSS feeds as well as being accessible by Facebook Platform applications and websites that the user visits.

2.3 Demographic Differences Related to SNS and Privacy Concerns

2.3.1 Gender

Royal Pingdom's (2009) observations on a number of SNS using demographical data from the United States show that LinkedIn, MySpace, Friendster, Hi5 have more women than men among their users. Particularly, based on the latest data from Facebook's self-reported statistics on the US market (Smith, 2009), women still represent 57% of the overall Facebook audience. However, these statistics also report that the recent rapid growth rate among the men is closing the gender gap. On the pattern of usage and motivation for the time spent on Facebook, a study suggests that social connectivity and perpetual contact are motivating the women to use SNS (Joinson, 2008). Joinson (2008) also notes that women tend to visit the site more frequently for social connection, status

updates, and for posting photographs. This may somewhat relate to Thelwall (2008) reporting that women tend to have more friends on social networks than men, while both men and women share the same commonality in having a majority of female friends.

Numerous studies have found gender differences regarding general online privacy concerns (Sheehan, 1999; Rodgers and Harris, 2003; Cho, et al., 2009). These studies suggest that women are more concerned than men about their online privacy. This also extends to women's concerns about cyberbullying and cyberstalking (Salaway and Caruso, 2008). Sheehan (1999) examines gender differences in attitudes and concerns toward information collected through online marketing. One of the differences she finds concerns the secondary use of information, as in receiving unsolicited e-mails. Here, women show more concern than men, and they are also more questioning of how the e-mails reached their address. In an international sample study of online consumers, Bellman, et al., (2004) confirm this finding about women's perception of the unauthorized secondary use of information. When registering for websites, women are more likely to provide incomplete information than men, while men provide inaccurate information more often than women as their privacy concerns increase (Sheehan, 1999). As for Internet shopping, men reported having greater trust in online shopping, and have more positive attitudes towards the Internet when it comes to it being able to provide a convenient shopping venue, compared to women (Rodgers and Harris, 2003). In addition, men also display a greater risk-taking attitude than women (Fogel and Nehmad, 2009). Similarly, Garbarino and Strahilevitz (2004) also find that women perceive more risks in purchasing online; more specifically they perceive more severe consequences to their loss of privacy compared to men.

Whether these differences in privacy concerns are also pertaining to SNS have been studied by Salaway and Caruso (2008), Fogel and Nehmad (2009) and Hoy and Milne (2010), to name a few. Overall, they reveal that women have greater privacy concerns than men. Female users display more concern than men regarding how their personal information could be used, and they do not agree to the same extent as men that SNS have made an effort to protect their privacy (Hoy and Milne, 2010). Concerning the

latter, women need to be reassured about the privacy protection policy before creating a social networking profile (Fogel and Nehmad, 2009). This finding is similar to Milne and Culnan's (2004) in that men are less likely than women to read privacy notices. Hoy and Milne (2010) also highlight the fact that in using Facebook, women are more likely than men to be proactive in protecting their privacy by controlling their privacy settings, including untagging pictures and removing messages from their profile 'wall'. Similarly, women are more likely to make their profiles private compared to men (Thelwall, 2008; Joinson, 2008; Lewis, et al., 2008). With regards to information disclosure, although we find that one study points to women sharing more information about themselves (Jones and Soltren, 2005), most studies reveal that women are less likely to disclose personal information than men (Acquisti and Gross, 2006; Salaway and Caruso, 2008; Fogel and Nehmad, 2009). These studies have reported that men are more likely than women to provide their phone numbers, personal addresses, instant messenger addresses and their sexual orientation on their SNS profiles. Finally, when it comes to adding new connections, women are more careful than men about whom they befriend (Hoy and Milne, 2010). On the other hand, Jones and Soltren (2005) find that both genders are equally unlikely to add a stranger to their 'friends' list.

2.3.2 Age

Some studies have attempted to conclude that age is associated with the level of online privacy concern (Campbell 1997; Milne, et al., 1996; Paine, et al., 2007). These studies have shown that older age groups have higher privacy concerns than younger age groups. Likewise, Paine, et al., (2007) adds that as age increases, the privacy concerns also seem to increase. On the subject of data collection, younger consumers are less concerned over unauthorized secondary use of their information (Campbell 1997). Young adolescents show few concerns over the negative consequences of information disclosure and, as such, their perceptions of privacy and self-efficacy are not motivating them to protect their privacy (Youn, 2009). However, contrary evidence can also be found. A recent study by Hoofnagle, et al., (2010) using a sample from the American population reveals

that there is no statistical difference in either attitudes, practices or policy preferences towards privacy between young and older adults, indicating that young adults care about their privacy just as much as older ones. Even so, young adults appear to have a lack of knowledge of privacy laws and are more likely to trust the law to protect their privacy (Hoofnagle, et al., 2010).

With regards to the adoption of SNS, Royal Pingdom (2010) provides findings on the age distribution of usage across various SNS. It is noted that MySpace and Friendster are most popular among users under 17 years old, at Hi5 the 25-34 age group is most numerous, while the age groups of 35-44 and 45-54 are dominating LinkedIn and Facebook. Not a single one of the mentioned sites is dominated by users 55 years old or above. It should also be noted that the average user of MySpace, Facebook, LinkedIn is 31, 38, and 44 years old, respectively, and that these figures may indicate that the social media is not dominated by younger people; rather they are dominated by middle-aged people (Royal Pingdom, 2010). It may appear that age is not necessarily a predictor for membership of a SNS, taking into consideration the focus of those sites as another critical element. LinkedIn, for instance, with its business and work relationship focus, generate little interest among teenagers who seek friendships rather than business connections.

Age is also found to be associated with the number of ‘friends’ one has, with younger age groups having more ‘friends’ than older people, which may be explained by the time spent on the sites and the frequency of visits to the sites (Joinson, 2008). It may also be explained due to the status seeking that is prevalent among teenagers (Pfeil, et al., 2009). In a study on MySpace, Pfeil, et al., (2009) note that older people are less enthusiastic than teenagers to engage in site activities and less often use the ‘comments’ feature as a way of communicating. They further suggest that older people are less concerned with working on their profile page; instead they deliver a more formal self-presentation compared to teenagers who reveal lots of personal and emotional information. The Get Safe Online (2007) report noted similar findings related to younger adults; 34% of 18-24 year olds post personal details on their profile. The report furthermore speculated that the likelihood of this group’s contact details being passed on by other people is higher

compared to other age groups. Even so, young users are more likely to make use of privacy settings on SNS (Get Safe Online Report, 2007; Joinson, 2008) which is somewhat in line with young people indeed being concerned about the protection of their privacy, as found by Hoofnagle, et al. (2010).

In addition, we comprehend that age as a demographic characteristic is not conventionally base-fixed, different from gender that has two base elements (male and female). Different researchers make up their own classes of age groups and their interpretation of their findings are subject to the age classification. The terms 'old' and 'young' are relative and when trying to interrelate both terms in various studies, we encounter overlapping among the defined age groups. Even so, we managed to grasp the essence of those studies in order to help us when defining our own age groups.

2.3.3 Geographical Background

In the early 2000s, the novel concept behind social networks started to attract media attention beginning in the U.S. and spreading to other parts of the world. This was quickly followed by the release of numerous SNS across the globe. MySpace, for instance, achieved success in America while Friendster earned popularity on the Asian continent. Other SNS also embraced the market in certain countries such as LunarStorm and Bilddagboken in Sweden, Mixi in Japan, Orkut and Hi5 in Brazil, Bebo in the U.K., Ireland, Australia and New Zealand, and Hyves in the Netherlands. Among all, the most rapidly proliferating SNS has been Facebook, which has seen a significant increase in unique visitors every year since the opening of its ports to the public in 2006. As of 2010, the top ten countries represented on Facebook are the U.S. (leading with over 100 million users), the U.K., Indonesia, Turkey, France, Italy, Canada, the Philippines, Spain and Mexico (Digital Buzz Blog, 2010). Despite worldwide domination, there have also been cases of the site being banned in several countries mostly due to political reasons. Blocked access to the site in Syria (Aune, 2007), China (MacDonald, 2009), Vietnam (EarthTimes, 2009), and Iran (BBC News, 2009) are examples of this.

Several researchers are being active in the field of geographical background in relation to online privacy concerns, though their studies have not been entirely global. Some have managed to highlight a few countries only, including the U.S., which is quite often included. According to a survey of 7 countries conducted by The Harris Poll (2010), 61% of the US respondents in combination with over 50% of the respondents from France, China, Spain, and the U.K. as well as over 40% of Germans and Italians are in general concerned about the possibility of their personal online data being accessible by search engines such as Google or Bing. A great majority of them are worried about being victims of cybercriminals and about their data being hacked. The survey also reports that Italians and Brits are most willing to share personal details on a website, whereas the Americans and the Chinese are more sensitive about this. Germans are in general more aware of privacy policies and tend to read the terms and conditions stated on the websites. In another study, the U.S. respondents were found less concerned about privacy issues compared to the Japanese (Maynard and Taylor, 1996). Also, people in most Asian countries have less affinity for the Internet and a greater fear of online shopping than the North Americans who tend to trust these sites for making purchases (Lynch and Beck, 2001). Additionally, Bellman, et al., (2004) collected responses from 38 countries and suggested that the level of privacy concerns is related to the national regulation of information privacy. They point out that consumers from countries with privacy regulations generally express fewer concerns about online privacy and transaction security than those from countries with a less-developed regulation framework.

In regard to privacy concerns in relation to SNS, little research has been done that also takes into account the geographical backgrounds of the respondents. The Harris Poll (2010) again shows that majorities in Spain, Germany, France, the U.S., Italy and the U.K. agree that SNS like Facebook increase their vulnerability to cyberattacks. In IBM's (2010) Global Innovation Outlook report about Web 2.0 applications, a majority of respondents from Brazil and Russia perceive that the benefits of participating in these applications outweigh the privacy risks. Respondents from Germany, Sweden and the U.S. believe that they benefit from exchanging information with other members, which

serves as their reasons for engaging in the use of these applications. The survey also states that the Chinese and Singaporean assume that their personal information is well protected by Web 2.0 applications. Furthermore, these respondents along with the U.S. ones show considerably low levels of privacy awareness and privacy protection. Conclusively, regarding this area of study, we find that our research may be one of the first attempts to test differences based on geographical background (continents).

3. Theoretical Framework

3.1 Social Exchange Theory

We adopt the social exchange theory as a framework for analyzing our findings. However, we will not solely be relying on it; instead, we see it as a valuable perspective to adopt when hypothesizing around the results of our findings. The social exchange theory proposes that social interactions consist of exchange relationships and states that the exchange is perceived in terms of its costs and rewards (benefits). Costs refer to factors that cause inhibition and deterrence to act or behave, while rewards are valued in the pleasure, satisfaction or gratification that a person obtains from the experience (Thibaut and Kelley, 1959). If the rewards outweigh the costs, then an individual is likely to commit to the exchange relationship (Metzger, 2004). This social exchange relationship will not be abandoned if it is reinforced or rewarded in some way (Thibaut and Kelley, 1959). Homans (1958) originally described the phenomenon as: *"Persons that give much to others try to get much from others, and persons that get much from others are under pressure to give much to others. This process of influence tends to work out to an equilibrium, balancing the exchanges"* (Homans 1958, p. 606).

The evidence of social exchanges on the Internet becomes more apparent with the rise of social media such as collaboration tools (Web 2.0), social network services, dating sites and job sites. These technologies support social exchanges through interactive web based interfaces, enabling online users to engage in a series of social exchanges. The phenomena consisting of SNS members implicitly exchanging and sharing information can be seen as a social interaction, and thus, we find that this theory is well suited for our research area. For example, a Facebook user can post his updates and share the information with his 'friends'. He can post comments on others' walls, join a group and invite people to events. Based on the social exchange theory, those actions and many other interactions that can be performed using the features available in Facebook are stimulating some course of social exchanges within the user's network. Previous studies,

presented below, have attempted to explain the social exchange theory in relation to privacy concerns.

An individual's reward components may be produced from his behavior or others' behavior (Thibaut and Kelley, 1959), as in the SNS context of this research where people seek to be in the process of seeing and being seen (Tufekci, 2008). When using the SNS, these people receive benefits in a variety of ways, where gratifications range from areas such as expanding one's social capital to 'social searching' and 'social browsing', and gain satisfaction from the content of the media and from the actual experience of using the SNS (Joinson, 2008). Another interesting motivation for being a member of a SNS is to present an idealized persona (Dwyer, et al., 2007; Utz and Krämer, 2009). A person who seeks to gain social acceptance among others tries to make himself attractive and impress others with his persona and qualities. This point is also noted by Boyd (2007) and Pfeil, et al., (2009) who find that teenagers are willing to put in significant effort to personalize their profile and form their identity hoping that they will be approved by their peers. Interestingly, Blau (1964) has argued that to earn social rewards such as approval, respect and satisfaction one should have the courage to take risks.

Arguably, as has been brought up earlier, one of the costs of adopting a SNS is the privacy risk. Perceptions of privacy risks are prone to users' judgments and personal impressions and experiences from the SNS engagement. What drives an individual to willingly provide personal information may be due to the perceived benefits of revealing information to strangers being greater than the perceived costs of potential privacy invasions (Gross and Acquisti, 2005). A person who perceives that the privacy risks outweigh the value received on the SNS is more likely to be deterred from joining the SNS, which is shown by the fact that non-users of SNS have higher levels of privacy concerns (Tufekci, 2008). Those who see the benefits of participating, yet are aware of the risks, may, however, not actively engage in the social exchanges. Youn (2009) also puts forward an interesting argument, arguing that, for individuals, the greater level of risk perceptions due to information disclosure, the greater the concerns over privacy. Similarly, the greater the perceptions of the benefits from the information exchange, the

less the concerns for privacy. For instance, people that strive for popularity may indeed be concerned about their privacy, but *"they may not be willing to sacrifice their popularity by implementing privacy controls"* (Christofilde, et al., 2009, p. 344).

In addition, trust has been noted as one of the most important requirements in the exchange relationship as it reduces the perceived risk of self-disclosing information (Steel, 1991). Trust *"leads to risk-taking in a relationship"* (Mayer, et al., 1995, p. 724) and higher trust results in lower risk perception (Ratnasingham, 1999). As it relates to SNS, trust will be seen as trust towards other members of the site and trust towards the site itself. First, when it comes to trust in other members ('friends'), the user has no real control but instead an expectation that the other members will follow appropriate conduct and commitment when participating in the SNS. Users also have no way of censoring and controlling what information about themselves that could appear on a friend's profile. This could be information in the form of negative comments, false statements or embarrassing photos of themselves. Regarding trust towards the site, users need to be assured that the site's privacy policy is adequate and trustworthy in order for them to establish a transactional relationship with the other parties (Pan and Zinkhan, 2006). Studies (Dwyer, et al., 2007; Tuunainen, et al., 2009) reveal that a majority of users trust Facebook with their personal information. Moreover, in a comparison study between Facebook and MySpace members, Dwyer, et al., (2007) reports that the level of trust in Facebook is significantly greater than the trust in MySpace. Though SNS may have attempted to give a signal of assurance through their privacy policy to their users, the users may not be entirely convinced that the SNS would not use their personal information for other purposes. Ultimately, not all users completely understand the terms of the bargain (Jones and Soltren, 2005), since they may be too overwhelmed with the usability of the site. Weighing in this factor, the cost of privacy risks turns out to be tolerable at some point.

4. Methodology

4.1 Overall Work Process

Bryman and Bell (2007) illustrate the ideal path to follow when conducting quantitative research (see Figure 1). However, they clearly state that this work process is an ideal one which is rarely followed by researchers in practice. Indeed, the actual process followed by researchers may include going back and forward between these steps (Bryman and Bell, 2007). Instead, they argue that the illustration should serve as a presentation of the most important steps to incorporate when performing quantitative research.

We note that our work process has not followed the ideal path outlined. Instead it has been highly iterative, with us as researchers going back and forward between the different stages in the quantitative research process. In doing this, we have ensured that all stages have in fact been included and this process model thus helped us to ensure that all parts were sufficiently covered and connected to each other.

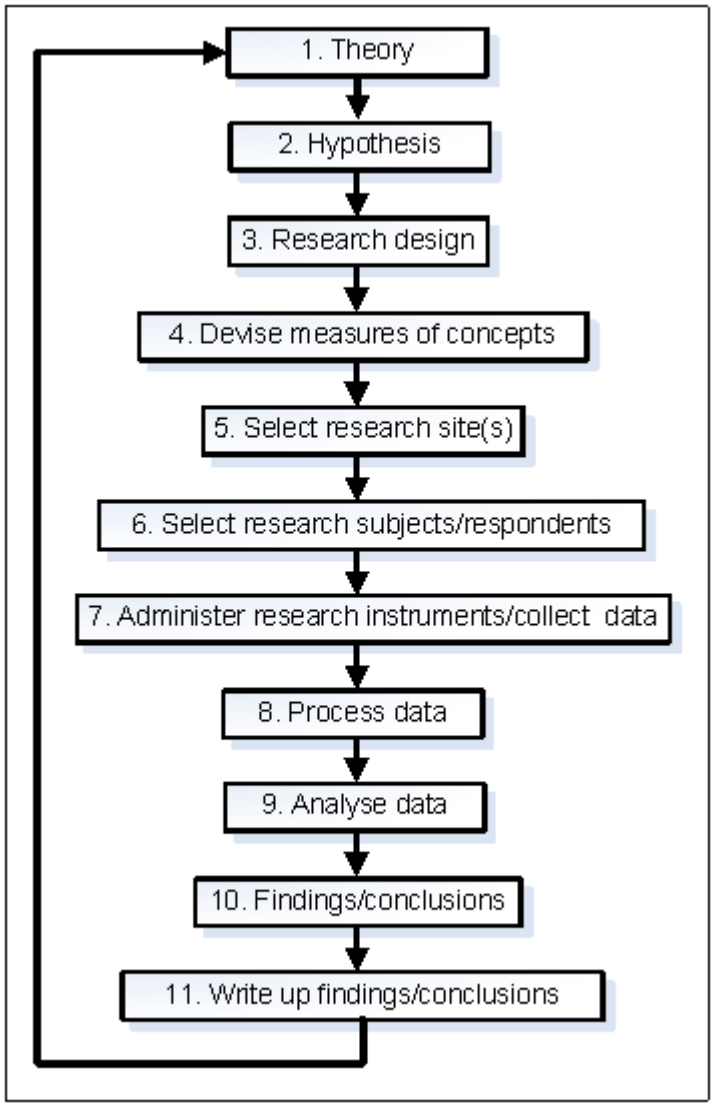


Figure 1: The Process of Quantitative Research (Bryman and Bell, 2007)

4.2 Philosophical Paradigm and Research Approach

We have used a positivistic paradigm when conducting our research, in which measurement and quantification was emphasized in the striving for objective knowledge (Seale, 1999; Wallén, 1996). This is a scientific approach in which the researcher works logically and in which the data collection and data analysis parts of the research are seen as highly important (Creswell, 2007). We argue that this paradigm suits our research questions well as we have tried to make visible relationships between our variables of

interest, presented in Table 2. By using quantitative research methods we were able to perform statistical testing thereby allowing for a higher level of generalizability than what would be possible using qualitative research methods (Seale, 1999). We do, however, agree on part of the criticism of the positivistic paradigm, most notably stemming from researchers with a postpositivistic perspective (see Fischer, 1998). In this criticism, the positivistic paradigm is described by the postpositivists as naïve as there is no one absolute truth that can be unraveled by relying on positivistic research methods. Rather, reality is constructed and dependent on the perspective of the individual (Fischer, 1998). But even if this criticism pertains especially to researchers within the social science area, we argue that our choice of paradigm and research method has been in line with postpositivistic researchers' emphasis on multiple methods of inquiry (Fischer, 1998). In this way, our research can be seen as one piece of the puzzle, which combined with other types of research can build up to form some kind of truth.

The more specific approach of this study was to build on previous research regarding risk-taking and privacy concerns related to SNS. Consequently, we started off with a theoretical background, meaning that an overall deductive approach was used (Bryman and Bell, 2007). The deductive approach is one in which hypotheses are commonly stated based on previous research and then tested using statistical methods (Bryman and Bell, 2003). 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. In line with this, we have noted that since our field of research is quite new, we have instead stated research questions having a wide scope which permitted us to explore relationships not foreseen before conducting our data analysis.

4.3 Questionnaire Design

The overall design of our questionnaire was highly inspired by Fogel and Nehmad's (2009) design. Like them, we found that to be able to answer our research questions, our questionnaire had to be divided into several parts. The first part revolves around demographic information. The second part concerns general attitude to risk and privacy. The third part relates to the use of social networking websites in general and the fourth and final part concerns the use of Facebook in particular. Two additional questions were also included at the end of the questionnaire, the placement of which will be further elaborated on below. Overall, the table below presents the questions asked in our questionnaire and the scientific background pertaining to them. It should be noted, however, that since this area of research is fairly new, there are no agreed upon measurements to use. As such, it was up to our judgment as researchers to construct relevant measurements. Partly because of this, the scientific background mentioned in the table in some cases refer to researchers who have used a similar question to assess attitudes within the realm of risk-taking and privacy concerns on SNS.

Similar to a range of other researchers (Acquisti and Gross, 2006; Tufekci, 2008; Tuunainen, et al., 2009; Fogel and Nehmad, 2009) we chose to include Facebook as a significant part of our questionnaire. This was due to several factors; First, Facebook was at the time of writing becoming massively adopted by the general public. According to comScore (2008), by mid-2008, the site had become the frontrunner of its leagues, followed by MySpace. By February 2010, Facebook (2010a) declared that the site had already garnered more than 400 million active users worldwide (70% of them were outside the U.S). It also stated that half of all the users log on to Facebook in any given day and that a user would have an average of 130 friends there. The site had been translated into more than 70 languages to accommodate a global audience. Similar reports have been found in Kazeniac (2009) who reported that Facebook was the overall largest SNS and Schonfeld (2009) who reported that Facebook was the fourth largest website in the world. Second, there was a considerable presence of resources and information in the media about Facebook – information found in blogs, online articles,

published articles, reports and in statistical data. Overall, we saw these facts as evidence that using Facebook as an object of study permitting generalization to other SNS was legitimate. Indeed, many researchers have been using Facebook as a source for research within this area, including researchers studying privacy and risk-taking, which was the focus of our study. These researchers' research was published relatively recently and often contained cross references to others' works. With this material building the foundation of our study, we sought to point out and demonstrate the relevance of those independent findings to our own findings. Third, based on the first assertion, we argue that the participants in our sample survey were more likely to have an account on Facebook and were therefore able to relate to most of the Facebook-specific questions and respond them accordingly. In making this choice, we were also hoping that the outcome of our study would be able to reach larger audiences.

Question/Statement	Scientific Background	Possible values/Coding scheme	Variable Scale	Variable Abbreviation
Age	Fogel and Nehmad (2009); Acquisti and Gross (2006); Lang, et al., (2009)	Any reasonable age	Interval/ratio	Age
AgeGroup		1=less than or equal to 20 2=21-25 3=26-30 4=31+	Ordinal	AgeGroup
Gender	Fogel and Nehmad (2009); Hoy and Milne (2010); Acquisti and Gross (2006); Manago, et al.. (2008); Lang, et al., (2009); Lewis, et al., (2008)	0=Man 1=Woman	Nominal	Gender
Nationality		Any reasonable nationality	Nominal	Nationality
ContinentGroup		1=Asia 2=Europe 3=North America 4=Africa	Nominal	ContinentGroup
To achieve something in life, one has to take risks	Fogel and Nehmad (2009)	Likert scale (Strongly disagree=1 to strongly agree=5)	Ordinal	Achieve_risks
If there is a great chance of a reward, I will take high risks	Fogel and Nehmad (2009)	Likert scale (Strongly disagree=1 to strongly agree=5)	Ordinal	Reward_risks
It is important for me to protect my identity information	Fogel and Nehmad (2009); Stutzman (2006)	Likert scale (Strongly disagree=1 to strongly agree=5)	Ordinal	Important_protect
In general, I am concerned about my privacy when using the Internet	Fogel and Nehmad (2009)	Likert scale (Strongly disagree=1 to strongly agree=5)	Ordinal	Concerned_privacy
I believe that my information is well-protected online	Fogel and Nehmad (2009)	Likert scale (Strongly disagree=1 to strongly agree=5)	Ordinal	Information_protected
Do you have a profile on a social networking website?	Fogel and Nehmad (2009): Dwyer, et al., (2007); Tufekci (2008)	0=No 1=Yes	Nominal	Profile_SNS

Question/Statement	Scientific Background	Possible values/Coding scheme	Variable Scale	Variable Abbreviation
Roughly for how long have you been using social networking websites?	Fogel and Nehmad (2009)	0=less than 1 year 1=1-2 years 2=2-3 years 3=3-4 years 4=4-5 years 5=5+ years	Ordinal	SNS_how_long
How frequently are you being active on social networking websites?	Fogel and Nehmad (2009); Dwyer, et al., (2007)	Several times per day(4)/week(3)/month(2)/year(1) Even less frequently(0)	Ordinal	Frequently_active
Roughly how many friends do you have in all of your social networking websites combined?	Fogel and Nehmad (2009); Lewis, et al., (2008); Ellison, et al., (2007)	0=0-49 1=50-99 2=100-199 3=200-299 4=300-399 5=400-499 6=500+	Ordinal	Number_friends_SNS
I have my own profile on:	Fogel and Nehmad (2009); Tufekci (2008)	0=No, 1=Yes Friendster (Yes/No) Hi5 (Yes/No) MySpace (Yes/No) LinkedIn (Yes/No) Bilddagboken (Yes/No)	Nominal	Profile_Friendster Profile_Hi5 Profile_MySpace Profile_LinkedIn Profile_Bilddagboken
Nbr_SNS		0 to 6	Interval/ratio	Nbr_SNS
Do you have a Facebook account?	Fogel and Nehmad (2009)	0=No 1=Yes	Nominal	Profile_Facebook
Which of the following information do you include in your Facebook profile? [list of information]	Fogel and Nehmad (2009); Gross and Acquisti (2005); Tuunainen, et al., (2009); Christofides, et al., (2009)	0=No, 1=Yes Name (Yes/No) Birthday (Yes/No) Profile picture (Yes/No) Email (Yes/No) Hometown (Yes/No) Address (Yes/No)	Nominal	FB_Name FB_Birthday FB_Profpic FB_Email FB_Hometown FB_Address FB_IM FB_Phone

Question/Statement	Scientific Background	Possible values/Coding scheme	Variable Scale	Variable Abbreviation
		IM (Yes/No) Phone (Yes/No) Religious views (Yes/No) Relationship status (Yes/No) Sexual orientation (Yes/No) Interests (Yes/No) Education/Work information (Yes/No) Photos of yourself (Yes/No)		FB_Relviews FB_Relstatus FB_Sex_or FB_Interests FB_Edu_Work FB_Photo_yrslf
Sum_Info_Reveal		0 to 14	Interval/ratio	Sum_Info_Reveal
Roughly how often do you update your status message on Facebook?		Several times per day(4)/week(3)/month(2)/year(1) Even less frequently(0)	Ordinal	Freq_stsupdate
Roughly how many third-party applications have you added to your Facebook account?		0=0 1=1-4 2=5-9 3=10-14 4=15-19 5=20+	Ordinal	Nbr_apps
I am concerned about the information submitted to Facebook	Tuunainen, et al.,(2009); Dwyer, et al., (2007)	Likert scale (Strongly disagree=1 to strongly agree=5)	Ordinal	FB_Concern_Info
I feel that the privacy of my personal information is well protected by Facebook	Dwyer, et al., (2007); Tuunainen, et al., (2009)	Likert scale (Strongly disagree=1 to strongly agree=5)	Ordinal	FB_Info_Wellprot
I am aware of Facebook's privacy settings	Tuunainen, et al., (2009); Strater and Richter (2007)	Likert scale (Strongly disagree=1 to strongly agree=5)	Ordinal	FB_Aware_privsett
I have made a conscious decision regarding my Facebook account's privacy settings	Tuunainen, et al., (2009)	Likert scale (Strongly disagree=1 to strongly agree=5)	Ordinal	FB_Consc_privsett
I will accept a friend request from an unknown person on Facebook	Mohtasebi and Borazjani (2010)	Likert scale (Strongly disagree=1 to strongly agree=5)	Ordinal	FB_Friend_Unknwn
I am aware of who can see my profile and the information in it on	Tuunainen, et al., (2009)	Likert scale (Strongly disagree=1 to strongly agree=5)	Ordinal	FB_Aware_Info

Question/Statement	Scientific Background	Possible values/Coding scheme	Variable Scale	Variable Abbreviation
Facebook				
Adding third-party applications in Facebook is not likely to be harmful		Likert scale (Strongly disagree=1 to strongly agree=5)	Ordinal	FB_Apps_Harmful
I am aware of Facebook's terms and conditions regarding my information	Tuunainen, et al., (2009); Mohtasebi and Borazjani (2010); Jones and Soltren (2005); Gross and Acquisti (2005); Acquisti and Gross (2006)	Likert scale (Strongly disagree=1 to strongly agree=5)	Ordinal	FB_Aw_Terms
Facebook's terms and conditions affect my decision regarding whether or not to participate in it	Murados (2008)	Likert scale (Strongly disagree=1 to strongly agree=5)	Ordinal	FB_Terms_Part
I have changed my Facebook account's privacy settings (from the default settings)	Tuunainen, et al., (2009); Gross and Acquisti (2005); Acquisti and Gross (2006)	0=No 1=Yes	Nominal	FB_Chg_Privsett
After completing this questionnaire, I have become more conscious of my use of social networking websites	Murados (2008); Tuunainen, et al., (2009); Acquisti and Gross (2006)	Likert scale (Strongly disagree=1 to strongly agree=5)	Ordinal	More_Consc_use
You are given a choice between the following two scenarios: 1. You receive an amount of money M wih 100% certainty. 2. A coin is flipped to decide whether you receive $100 or nothing (50% certainty each). What amount of money M is required for you to choose the first scenario?	Karmarkar (1978)	Any reasonable value (i.e. 1-100)	Interval/ratio	Equat_risk_av

Table 2: Questionnaire Items and Variable Coding

4.4 Data Collection

Examining Internet users' risk-taking and privacy concerns as well as their behavior translated into our target population including all Internet users. Consequently, if we were to have used a probabilistic sampling method, it would have required us to construct a selection procedure in which all Internet users would have the same likelihood of being selected to participate in our study (Anderson, et al., 2009). Regardless of how the probabilistic sampling method would be performed in practice (simple, stratified or cluster), this requirement was simply not possible to fulfill due to the limited time available for our study.

Due to these limitations, we had to resort to using the other sampling method available: the non-probabilistic sampling method. In this method, the probability of selecting each possible sample is unknown, which is a disadvantage compared to the probabilistic sampling method. Resulting from this choice of sampling method is that statistically valid statements cannot be made about the estimates. However, the method has frequently been used in practice (see for example Gefen and Straub, 2000; Wixom and Watson, 2001) because it is often the only feasible one. (Anderson, et al., 2009)

In our study, we chose to employ a combination of the two non-probabilistic sampling methods convenience sampling and judgment sampling. Convenience sampling is a method in which the researcher chooses samples because of accessibility whereas in judgment sampling samples are chosen based on the knowledge of the researcher or another person specialized within the field of study. (Anderson, et al., 2009)

To collect data, then, we posted posts on different web forums calling for help with our study. The forums were selected based on who its visitors were, a type of judgment sampling. We were careful to choose forums whose visitors would, to a significant extent, include persons displaying the same diversity in attitudes as the general public. Consequently, general forums such as those related to education (high school as well as university) were most prominent in our sample, whereas forums related to individuals

with special interests were specifically omitted. The reason being that persons active on forums that are narrowly focused may display characteristics not representative of the whole population. We also used our judgment to ensure that the forums selected were characterized by an adequate level of seriousness, thereby reducing the risks of conscious input errors. One could argue that selecting forums related to education results in a sample with a significant portion of younger individuals. This is true, but we found it important to keep in mind that at the time of writing, SNS in general were still dominated by the younger audience. Consequently, forums visited by older individuals also fulfilling the two goals of adequate seriousness and not being too niched were very hard to find.

Another data collection method that could have been used is handing out questionnaires in paper form. Even if this method may have made the subject feel more 'invested' in the research, our assessment is that it would neither have reduced the risks of conscious input errors nor made certain that a higher proportion of the participants would have completed the whole questionnaire. However, it would have enabled participants to ask us questions about the questionnaire questions, possibly resulting in higher level of correctness of the data.

Related to this decision was our choice not to focus on students at Lund University. Even if that would have possibly increased our sample size, the detrimental effects on the generalizability of our findings would, in our view, have been too significant. Overall, we argue that the data collection methods actually employed by us ensured that we received a sample that was more diverse than what would be the case using any other available method.

4.5 Sampling Error

Sampling error is defined as *"the difference between an unbiased point estimate calculated from the sample and the population parameter"* (Anderson, et al., 2009, chapter 22, p. 5). This error stems from the fact that not every element in the population is surveyed (Anderson, et al., 2009). As previously mentioned, we have used a non-probabilistic

sampling method, which does indeed increase the level of sampling error. However, we argue that this is an inevitable problem that researchers face when doing research within a short time-frame, highlighted by the fact that numerous researchers have been using this method in published articles in peer-reviewed journals, as previously exemplified. Furthermore, to reduce the impact of sampling errors, we ensured that our sample was demographically diverse, as was further elaborated on in the preceding section. Building from a demographically diverse sample results in the unbiased point estimate being less different from the population parameter than what would otherwise have been the case (Anderson, et al., 2009).

4.6 Non-sampling Error

Non-sampling error is defined as all other types or errors that might occur when conducting a survey (Anderson, et al., 2009). The first type of sampling error that can occur is an incorrect measurement of the phenomenon of interest. This will be elaborated on in the proceeding sections on validity and reliability. Another type of non-sampling error is the non-response error, which is when some units choose not to answer or when they answer the survey only partially (Anderson, et al., 2009). This can create a bias as the units not responding may have similar characteristics, especially if the characteristic is in any way important to the study (Anderson, et al., 2009). To reduce non-response error, we have explained how many questions our questionnaire contains as well as the average time it will take to complete it, both in the forum posts and in the beginning of our questionnaire. We have also designed the questionnaire placing questions that are easy to answer in the beginning and questions that may appear more tedious to answer at the end. Both of these design features lessen the risk of non-response error. The first one by providing information to the surveyed resulting in the uncertainty regarding the length of the questionnaire being reduced. The second by making the surveyed individual feel invested in the questionnaire, reducing the risk of the surveyed leaving the questionnaire page before all of the questions are answered. As we have collected data on the number of people who have visited our questionnaire as well as the number of people who have completed it, an assessment can be made regarding this type of non-response error. We

noted that 255 people visited our questionnaire and 240 people answered it completely, consequently 14 persons visited the questionnaire but did not submit answers to it. Out of these 14 persons who visited the questionnaire but did not answer it, we ourselves counted for roughly five of these visits while checking the correctness of the questionnaire. Consequently, roughly 9 individuals having visited our questionnaire without having completed it, which corresponds to a completion rate of roughly 95%. This value has to be seen as an indication of good questionnaire design.

Another type of non-response is when people saw our questionnaire (or more specifically our forum post) but chose not to answer it. Conducting a survey in this setting, we had a hard time assessing how significantly this type of non-response affected our study. We noted that 240 collected answers during a 29 day time period indicates that people's reluctance to answer our questionnaire cannot have been very high. This in combination with the diversity of our sample regarding our demographical characteristics of choice translated into our assessment that non-response did not have a significant negative effect on our study.

Anderson, et al., (2009) argue that non-sampling errors due to lack of knowledge is especially common in technical surveys. This was a concern for us, partly because the people most active on SNS are teenagers who may not understand some of the questions posed. To remedy this problem we tried to phrase our questions in a way that permitted scientific analysis while still making them easily understandable. We did note from the beginning of creating our questionnaire that question 17 would be hard to understand for some, which was why it was placed at the very end of the questionnaire. Its inclusion was motivated by the fact that it provides an alternative measure of risk-aversion, which we hypothesized could be included with measurements of risk-taking to create a construct.

Other types of non-sampling errors that may occur are selection error and processing error. Selection error is an error in selecting the units to participate in the survey whereas processing error involves an error when recording, coding or transferring data (Anderson, et al., 2009). In our case, selection error was not present as we were interested in all

people who are active on the Internet, to some extent also the people who are not active on SNS. To diminish the risk of processing error we used an online questionnaire where data was stored automatically. Subsequently it was also transferred to our software for data analysis automatically (using Google Docs' export function). Another action taken by us to reduce processing errors was that both of us researchers were present when transforming and recoding the data as well as when performing the statistical testing. Indeed, the transformation and recoding of the final data set were conducted by each researcher independently and then compared using Excel Compare version 2.2 beta. Together, these actions reduced the risk of processing error by adding an additional error-checking mechanism. Furthermore, backups were created at regular intervals and stored at different locations during the data collection period, reducing the risk of our data being lost or manipulated.

4.7 Reliability

Reliability is often divided into several parts, with some researchers dividing it into internal and external reliability. Internal reliability is then a measurement of to which extent other researchers are able to find the same constructs as the original researchers and external reliability is the extent to which other researchers are able to replicate the entire study (Seale, 1999). On the other hand, some researchers divide reliability into two other parts: test-retest reliability and internal consistency (Pallant, 2007). Here, test-retest reliability is a measurement assessing to which extent the test scale is stable over time. That is, the test is administered to the same individuals during two points that differ in time. If the results are significantly different to each other, the test is said to have low test-retest reliability. Internal consistency, then, is a measurement assessing if items making up an attribute are measuring the same underlying construct. The most common way to check for this is using Cronbach's alpha or the mean inter-item correlation between the items (Pallant, 2007).

We have dealt with internal and external reliability as thoroughly as possible by describing our research method in detail. Furthermore, we have chosen to include lots of

data and motivated the choices behind our questionnaire items as well as our tests based on the most up-to-date scientific material available. These actions in combination will facilitate researchers both being able to find the same constructs and also being able to replicate the study as a whole.

Regarding test-retest reliability, we found that it could not be ensured due to the very limited time-frame that we had available for our study. However, we have had no reason to expect that the results gathered at the beginning of our data collection period deviates from the results gathered at the end of our data collection period. Furthermore, as our data collection period was a month in length, it could be argued that some of the possible differences have cancelled each other out. That is, there is reason to believe that compared to data collected during a very short time-period, a slightly longer time period is not as likely to exhibit strange deviations. Conclusively, we found that our research has not been significantly negatively affected by the time factor.

Internal consistency is only pertaining to constructs, which have been checked using the common Cronbach's alpha measurement in combination with the inter-item correlation measurement. The reason for us using both measurements is that Cronbach's alpha values generally are too small if too few items (less than 10) are included in a construct (Pallant, 2007), whereas inter-item correlations may in those cases be more accurate. That is, one of the problems with Cronbach's alpha is that its value can be made higher by simply including additional variables (Streiner and Norman, 1989).

It should be noted that we also took advantage of other measurements provided by the computer software used, information which some researchers include in their discussions of reliability. More specifically, the relevant information that we used included but was not limited to R-squared and Adjusted R-squared values, p-values and relative frequencies. Furthermore, in line with Seale's (1999) and Anderson, et al.'s (2009) reasoning, computer software was not used mechanically, but in combination with a large portion of human judgment. That is, we were active in critically examining the computer output.

4.8 Validity

Like reliability, validity is often divided into different parts, sometimes into what is called internal validity and external validity (Bryman, 2008). Internal validity in a quantitative study refers to the extent that a scale measures what it is supposed to measure (Pallant, 2007). To ensure this, we used previous studies within our research area as a basis for constructing our questionnaire. This means that similar wording has been used, as well as the ubiquitous Likert scale. Together, these choices contributed to some level of internal validity, even if we noted that internal validity is, no doubt, harder to achieve when conducting research within a relatively new research area. We also found that this definition of internal validity pertains more to studies relying heavily on constructs, as constructs are assumed to measure a hidden variable. Our study, on the other hand, included only a very limited number of constructs. The rest of our questionnaire items could be characterized as relevant in their own right and, as such, the question of whether they measured what they were supposed to measure became largely moot.

External validity, on the other hand, refers to the extent that the study's findings are applicable in other situations and is thus a question of generalization (Seale, 1999). External validity is therefore highly related to several parts of the study, from the questionnaire design to the sample and the statistical tests used. In this way, the final verdict of external validity is up to the reader, as Seale (1999) argues. We as researchers can only clearly communicate our choices and the motivations behind them to facilitate easier assessment of the external validity of our study. Our opinion is that our sample diversity and size in combination with significant methodological awareness have contributed to a high level of external validity. Indeed, the notion that a diverse and large sample strongly affects the generalizability positively is frequently described in the methodology literature (see for example Bryman and Bell, 2007).

Another aspect of validity is face validity, which is ensuring that the questionnaire is understandable (Litwin, 1995). As previously mentioned, we achieved a significant completion rate for our questionnaire, which could be taken as evidence that it was easy enough to understand. However, we were given feedback relating to our questionnaire from individuals in the forums as well as in the questionnaire itself, where some individuals reported that they did not understand question 17. This was expected, as the inclusion of question 17 was considered highly experimental. Apart from reactions to this question specifically, we received no further feedback related to our questionnaire being hard to understand. Instead, we received encouraging comments from participants wishing us good luck and stating that this area of research seemed interesting.

4.9 Overall Bias

We find it important to note that however transparent we try to make our methodological and theoretical choices and frameworks, we were still affected by unconscious processes of hidden assumptions and biases (Ehrlinger, et al., 2005; Norris, 1997; Hammersley and Gomm, 1997). Consequently we find that our data analysis and conclusion parts, even though they are based on quantitative data, may have been especially colored by these biases. A solution to this 'problem' is not to be found as the notion of researchers having no biases is highly naïve. Instead we argue in line with postpositivistic researchers (see Fischer, 1998) that there is no 'one real truth' and that our results are to be interpreted as one result of many eventually building up to form a collective version of the 'truth'. This ultimately places demands on our readers to use their critical thinking skills, where they themselves have to assess the truth factor of our research. It also translates into us following Seale's (1999) advice to trust that our readers possess this skillset.

4.10 Ethical Considerations

Throughout our research, we have taken great care to ensure a high level of ethical conduct. When collecting data pertaining to individuals, there is always a risk that the data may be used for unethical purposes (Israel and Hay, 2006). As our study involves

collecting rather large amounts of data of this sort, we have taken steps to minimize the risk of the data being abused in any way. One part of this is ensuring that participants in our study have had the possibility of being anonymous. This has been ensured by us not recording any information with which it would be possible to relate a questionnaire answer to a certain individual (not even IP addresses). Furthermore this includes the fact that our participants did not, in any way, have to register or provide any kind of information to be able to access our online questionnaire. Israel and Hay (2006) argue that not recording any information in the first place effectively protect participants' confidentiality by also guarding the data against theft and accidental disclosure. That is, if the data would be stolen, a specific individual would not be traceable anyway. Moreover, an advantage of using Google Documents as our online questionnaire tool was its ability to support Hypertext Transfer Protocol Secure (HTTPS), raising the level of information security and anonymity further by facilitating an encrypted connection to Google's servers.

In discussing ethical considerations, further questions regarding the safeguarding of data have to be addressed as well (see Brady et al., 2001 in Israel and Hay, 2006). As we have chosen to use Google's service Google Documents for our questionnaire, a discussion of Google's data policy is relevant. Google states that they do not share information to third-parties without consent and that they take necessary precautions to protect against *"unauthorized access to or unauthorized alteration, disclosure or destruction of data"* (Google, 2009). Personal information is only collected to *"operate, develop or improve [their] services"* (Google, 2009), however this has limited relevance to questionnaire respondents as no information with which one could be able to identify a person is collected in the first place. Regarding the respondents IP address, which might in fact be collected for this purpose by Google, the relevance of it as an identifier of an individual must be questioned. This is especially true given the ubiquity of dynamic IP addresses in combination with open wireless networks, other public networks and Network Address Translation (NAT) devices.

Israel and Hay (2006) and Kvale and Brinkmann (2009) both address the issue of voluntariness, arguing that individuals who are put under pressure are unlikely to be able to make an informed, voluntary choice (informed consent) regarding whether or not to participate in a study. We note that we as researchers have not in any way pushed people to participate in our study, not even by using prizes or rewards for completing our survey, which could by some be seen as an indirect push. Instead, we have in our forum posts as well as in the beginning of our questionnaire described our area of study with our concern for anonymity and the possibility to opt-out of the study at any time. Consequently, our assessment is that as the participant has completed and submitted the questionnaire, informed consent has been achieved.

4.11 Sample Profile

Data was collected during the time period 1st of April 2010 until the 29th of April 2010. This period supplied us with 240 answers, where 238 of them were deemed to be valid. This means that in performing the check for incorrect values mentioned in Argyrous (2005) and Bryman and Bell (2007), two of the responses were deleted right away. Both of them because they displayed obvious signs of being invalid. Furthermore, some of the respondents did not answer all of the questions, partly due to the second part of our questionnaire being tailored for individuals who have an account on Facebook. A consequence of this is that some of the statistical tests performed have not include all of the 238 respondents. The number of respondents included in each test is clearly stated in close proximity to the specific test. In all of the cases we took great care to ensure that the number of cases included exceeded the minimum requirement for the test in question.

Analyzing the gender distribution of our sample, we find that roughly 51% are men and 49% are women (Table A1, Graph G1). This is close to an optimal distribution as subsequent tests are reliant on the two groups being represented by an adequate number of respondents. We note that one respondent was able to submit the questionnaire without including gender information. This response will nonetheless be kept as the individual in

question did respond to the last part of our questionnaire, giving out information that can still be used in the analyses.

Overall, our respondents display a wide range of demographic characteristics. The age of our respondents range from 14 to 60 years with a mean value of 27.3 years and a standard deviation of around 9 years, displayed in Table A2. A large part of our sample is between 21 and 31 years old, with some outliers noticeable at the upper range of the age scale, as seen in Graph G2.

We also find a significant diversity regarding geographical backgrounds. More specifically, we have 42 different countries represented, which we have divided into four continents: Asia, Europe, North America and Africa. This segmentation can be motivated using the same argument as above; that a group needs to consist of enough individuals to be able to perform statistical tests of differences between groups. Dividing our individuals based on the continent that they belong to allowed us to do this. Examining Table A3 and Graph G3 it can be noted that the lion's share of our respondents come from Europe, accounting for roughly 38 % of the answers. This is contrasted with Africa, with only about 13% of the answers. North America and Asia are accounting for roughly 22% and 23% of the all the respondents respectively. It should also be noted that some participants came from a country that could not be included in the aforementioned categories. These answers were simply omitted from the tests pertaining to continents.

Overall, we argue that this level of demographic diversity partly validates our study's significance as we have found no other study within this realm displaying such heterogeneity.

4.12 Methods for Data Analysis

To conduct our data analysis, the data was first exported from Google Docs to Microsoft Excel 2003 using Google Docs' export function. In Excel, the data was transformed into a format allowing for subsequent analysis, including transforming all variables into

numerical ones as well as creating new variables. It was then imported into SPSS version 17.0 where the actual data analysis was performed. SPSS is the most widely used software for conducting statistical analyses (Howitt and Cramer, 2005). For some of the statistical tests we instead used Gretl version 1.8.7 as one of us authors felt more familiar with this software. SPSS' and Excel's ubiquity are considered to be assurances of quality, whereas the high quality of Gretl is thoroughly discussed in Yalta and Yalta (2007). Consequently, we as researchers have no reason to doubt the output generated from these software packages.

More specifically, the data analysis performed in Excel involved coding all of our variables into numerical values. For example, the variable Gender was coded into 0 indicating a man and 1 indicating a woman and Likert scale variables were encoded into 1 for Strongly disagree to 5 for Strongly agree. Questions corresponding to ordinal scales but not Likert scales were coded in a similar fashion, with 0 displaying the lowest amount and the maximum value being 5 or 6. This was done to enable subsequent analysis using SPSS and Gretl. A more thorough table displaying the possible values for all of the questionnaire items can be found in Table 2.

Having input fields in our questionnaire permitting free text obviously resulted in answers that were dissimilar in their formatting. As an example, some individual responded to the nationality question by including more than one nationality. Others did not input a valid nationality but something else. As for resolving the multiple nationalities problem, we chose a nationality which seemed to be the correct one. For example, a nationality value of British Indian was corrected to England and values of African American were changed to USA. The invalid values, on the other hand, could not be corrected and were thus omitted from the tests pertaining to continents. It should be noted that no tests were performed on individual countries, rather all of them were performed on continents. This reduced some potential problems, including some respondents reporting their nationality as being British – a response that does not pinpoint a specific country.

In Excel we also created new variables, for example the variable Continent was created using country information. This was necessary as some of the statistical tests performed require a sample size that is big enough. Using continents as opposed to countries allowed us to perform these statistical tests. Likewise, the variable Age having the scale of interval/ratio was used as a basis to create the variable AgeGroup, which grouped the individuals into certain age categories. The argument for doing this is also that it enabled us to perform some additional statistical tests otherwise not possible to perform. It should be noted, however, that following good practice within the area of statistics, we always sought to use as high a scale as possible when performing tests. In practice, this meant using interval/ratio scale variables instead of ordinal ones when possible.

The specific methodology for finding relationships between the variables included us using the demographic data collected and testing it against the rest of the data. In practice, this translated into us starting with testing the gender variable followed by the age variable and lastly the continent variable. In each instance, proper statistical tests were used, guided by the nature of the variables.

Constructs were created when we found (using applicable tests for correlation) that several variables were measuring an underlying phenomenon (hidden variable). The validity of the constructs were tested using Cronbach's alpha with a threshold of 0.6 deemed as sufficient and 0.7 deemed as good. This is in line with researchers' perceptions of valid alpha values within exploratory research (Robinson, et al., 1991; Nunnally, 1978). As this area of research is new and therefore in need of exploration, we argue that it makes sense to use these thresholds. Similarly, mean inter-item correlations were calculated adding all correlation coefficients together and dividing the sum by the number of correlation coefficients added. Here, values between 0.2 and 0.4 were judged as optimal, as advised by Briggs and Cheek (1986). As previously stated, mean inter-item correlation is more suitable when testing constructs including 10 or fewer variables. Thus we relied on this measurement in the case of contrary test results. In practice, the constructs used were created by simply adding variables from ordinal scales together. The resulting variable representing a construct was then treated as having the scale of

interval/ratio, permitting a more complete range of statistical tests to be performed (Pallant, 2007; Argyrous, 2005).

As opposed to many researchers using Likert scales we have chosen a conservative, more scientific approach to analyze the data gathered using them. As the distance between values on a Likert scale cannot be assumed to be equal, describing them with means and standard deviations makes no sense (Jamieson, 2004). Indeed, as Argyrous (2005) states, *"this is not a correct procedure"* (Argyrous, 2005, p. 344) as *"what a score of 5.6 is meant to signify, however, and whether this is different in any meaningful way from a score of say 5.3, is not very obvious"* (Argygous, 2005, p. 344). Jamieson (2004) makes a similar argument stating that *"[when having a Likert scale] the intervals between values cannot be presumed equal"* (Jamieson, 2004, p. 1217) and continuing with the argument that a researcher may ultimately come to the wrong conclusion by using the wrong tests based on using the wrong scale (Jamieson, 2004).

Based on these persuasive arguments, we have chosen to follow the advice that both Jamieson (2004) and Argyrous (2005) give – that the appropriate way to treat Likert scales is as ordinal level data and consequently to use non-parametric tests. Argyrous (2005) furthermore presents a plethora of tests that are possible to conduct based on what scale the variable in question is measured in. In cases of doubt, we have followed Argyrous' (2005) advice, noting that it is not uncommon for authors of books within statistics or quantitative research methods to give slightly different advice within this area. The motivation behind following Argyrous' (2005) advice is that in comparison to other texts, his was found to be the most comprehensive and explained areas that other writers simply left out. The tests that we have chosen to perform are collectively presented in Table 3.

Variable types	Test	Description	Scientific motivation
At least one nominal	Chi-square test for independence	Tests independence	Argyrous (2005) pp. 316-334; Howitt and Cramer (2005) pp. 93-105; Pallant (2007) pp. 214-218
At least one nominal	Goodman and Kruskal tau	Asymmetric measure of association, ranges from 0-1.	Argyrous (2005) pp. 83, 92
Both at least ordinal	Spearman's rho	The non-parametric equivalent of Pearson's r. Gives correlation coefficient from -1 to 1.	Argyrous (2005), pp. 179-182; Howitt and Cramer (2005). p. 60; Pallant (2007) pp. 123, 126, 130.
Both at least ordinal	Mann-Whitney U (Wilcoxon W)	Non-parametric equivalent of the t-test. Tests for difference in rankings.	Argyrous (2005) pp. 343-353; Howitt and Cramer (2005) pp. 123-126; Pallant (2007) pp. 220-223
All at least ordinal	Kruskal-Wallis H	Non-parametric equivalent of the ANOVA test. Tests for difference in rankings.	Argyrous (2005) pp. 357-358; Pallant (2007) pp. 226-228
One categorical, one interval/ratio	Point biserial correlation	Gives correlation coefficient from -1 to 1	Gravetter and Wallnau (2009) pp. 548-549
Independent variable categorical, dependent variable interval/ratio	Eta	Asymmetric measure of association, ranges from 0-1.	Argyrous (2005), p. 182
Independent variables categorical or interval/ratio, dependent variable interval/ratio	Linear regression (OLS)	Describing changes in the dependent variable based on changes in the independent variables.	Argyrous (2005) pp. 187-199; Pallant (2007) pp. 146-165

Table 3: Statistical Tests

The observant reader may note that we have deviated from the scientific rigorosity described previously when we have added together several ordinal scales to create a construct which is assumed to be of interval/ratio scale. It should also be noted that when performing linear regression using the ordinary least squares (OLS) method, two requirements first and foremost need to be fulfilled. First, error terms should follow a normal distribution given a specific combination of values (Argyrous, 2005), which will be examined using the Chi-square test. Second, the error terms should be homoskedastic (of equal variance) (Argyrous, 2005), which will be assessed using the White test (see White, 1980). Whether or not our regression analyses have fulfilled these criteria will be reported in relation to the specific test being reported in the data analysis section. It is

worth noticing that it is not uncommon for none of these requirements to be fulfilled when performing linear regression, even though passing these tests is an indicator of quality. Resulting from this discussion is that the parts of our data analysis dealing with created constructs from variables with ordinal scales as well as the ones including linear regression where the above requirements are not fulfilled should be particularly critically scrutinized by the reader. The reason for using these methods in spite of the, arguably, limited scientific rigorousness is that they have, nonetheless, provided insights into relationships between variables and constructs that would otherwise have remained completely hidden.

Furthermore, we note that the kind of quantitative research we are involved in, including relatively simple statistical tests, does not allow us to state that causal relationships exist. As Anderson, et al., (2009) and Bryman and Bell (2007) argue, when using statistical tests and methods such as the Chi-square test for independence, linear regression and others, researchers can only be certain that a correlation between variables exist, not that the relationship is causal. It is therefore up to us as researchers to elaborate on the possible cause and effect relationships based on previous research as well as good judgment. The reader should therefore also be especially critical of statements that include us ascertaining cause and effect relationships based on these tests.

In summary, we argue similar to Seale (1999) that it is ultimately up to the reader to assess the truth value of our findings. However, by being aware of potential shortcomings in our study we were able to criticize our own method and clearly communicate these findings to our audience. We found that this, apart from creating a bond of trust with the reader, has made our reasoning become more transparent.

5. Results and Analysis

5.1 Descriptive Statistics

By examining the descriptive statistics regarding the questions that assessed attitudes towards general risk-taking, represented in Table A4 and A5, we found that our sample is mostly positive towards risk-taking. Indeed, more than three quarters agree or strongly agree that in order to achieve something in life, one has to take risks. When it comes to taking action based on this attitude, the results are somewhat lower with around 30% answering neutrally and 45% agreeing when asked if they will take high risks in order to receive a high reward.

Not surprisingly, an overwhelming majority of our sample think that it is important to protect one's personal information (Table A6). Only about 13% answered this question being neutral or disagreeing. Responses were divided relatively equally between agreeing and strongly agreeing. The importance of protecting one's personal information closely mirrors the findings by Fogel and Nehmad (2009) and Stutzman (2006). Respondents also answered that they are concerned about their privacy when using the Internet, with more than 70% agreeing or strongly agreeing to this statement (Table A7). This concern was reflected as skepticism highlighted in the answers to the question of whether our participants thought that their data was well-protected online. Only one quarter of our respondents agree or strongly agree with this statement (Table A8), and 37% are stating that they disagree. We found that this result is in line with Fogel and Nehmad's (2009) findings when asking a similar question.

Regarding the number of people who have profiles on SNS, we found that around 90% state that they do (Table A9), with Facebook being the overwhelmingly most popular site – around 85% of our respondents agreed on having a profile there (Table A10). This result is similar but slightly higher compared to what other researchers have found (cf. Stutzman, 2006; Fogel and Nehmad, 2009; Acquisti and Gross, 2006). Two other SNS

that are relatively popular in our sample is MySpace (Table A13) and LinkedIn (Table A14), with 27% respectively 16% reporting having a profile there. This confirmed our initial assumptions; that when studying SNS, it is a good idea to focus on the overwhelmingly most popular one: Facebook.

There is a wide difference regarding for how long our respondents have used SNS (Table A16). Around 25% report that they have been using SNS for more than 5 years, while around 22% report that they have been using these sites for 2-3 years. This result was to be expected, as the 2-3 years answer could be reflected by the time period in which Facebook became popular for the masses. Individuals who have used SNS for more than 5 years are what could be called early adopters within this area. Overall, this result differs slightly from Fogel and Nehmad's (2009), as they reported an average time of usage of around 2 years. We assume that this discrepancy is due to the nature of their study, which only included Facebook and MySpace as examples of SNS. Indeed, neither Facebook nor MySpace is to be considered an old SNS, thereby affecting their measurements downwards.

Out of all the SNS we had specified, we found that most individuals are active on only one or two of them, with only one being the most common answer (Table A17). Around 12% are not active on any of them whereas 2% are active on four of them. This reflects the users concentrating on one or a few SNS, probably due to the large network effects affecting these types of websites.

Users who are involved in SNS report being highly active on these sites (Table A18). Around half of our sample report being active on SNS several times per day, and more than 85% of the SNS users are active on these sites several times per week. Even if Fogel and Nehmad (2009) and Dwyer, et al., (2007) asked slightly different questions pertaining to activity, they also found that users of SNS are what must be described as very active on these sites.

We found no surprises regarding the number of friends SNS users have on all of their profiles combined (Table A19). These results almost follow the normal distribution with 100-199 and 200-299 friends being the most frequent answers totaling around 50%. 12% of our respondents report to having more than 500 friends whereas 14% have 0-49 friends. This is in line with Fogel and Nehmad (2009) reporting an average number of friends on MySpace and Facebook combined of around 240 and also in line with Ellison, et al. (2007) and Lewis, et al. (2008) who have reported an average number of friends on Facebook only of 150-200 and around 150, respectively.

Information disclosure differs in relation to the specific type of information being disclosed. Around 75% report that they are sharing accurate information regarding their real name (Table A20) and their birthday (Table A21) and 69% report sharing their e-mail (Table A22). A slightly higher amount (~80%) report sharing information about their hometown (Table A23), having an accurate profile picture (Table A24) as well as sharing photos of themselves on their SNS account (Table A25). Information such as one's relationship status (Table A26), interests (Table A27) and where one works or goes to school (Table A28) is not seen as controversial either, with roughly 63% reporting that they are sharing this kind of information. Slightly more controversial is sharing information about one's religious views (Table A29) and sexual orientation (Table A30), resulting in only 42% displaying this information. The most sensitive information to share seems to be one's instant messenger address (Table A31), phone number (Table A32) and actual home address (Table A33), with 29%, 13% and 8% displaying this information, respectively.

Our results on information disclosure are highly similar to Tuunainen, et al.,'s (2009) and Christofides, et al.,'s (2009) results regarding which type of information that is most commonly shared. However, we found two significant differences between our results. First, Tuunainen, et al., (2009) report higher values for the items most commonly disclosed, such as real name, profile picture, birthday and hometown, all shared by 90-100% of their sample. Similarly, Christofides, et al., (2009) report higher values for birthday (96%), e-mail address (85%) hometown (85%) and relationship status (81%).

We argue that this may be due to us including an option in our questionnaire of answering that the information in question was shared, but in fact not accurate. As such, our study may better assess the amount of accurate information that is being shared. We also noted that our sample is less reluctant to share their religious views compared to Tuunainen, et al.,'s (2009). An answer to both of these discrepancies may be found in the proceeding analysis, as our sample is broken down and the answers are analyzed based on demographic characteristics.

Different from Gross and Acquisti (2005) who found that around 10% do not provide their correct full name on Facebook, we found that as many as 24% do not provide their correct full name. Further differences from Gross and Acquisti (2005) include us finding a lower percentage of individuals who share their phone number (40% vs. 13%), profile picture (91% vs. 83%) and birth date (88% vs. 76%). We argue that the differences may be due to increased awareness on behalf of SNS users, who during the last years have become more enlightened regarding what information that may be appropriate to share on SNS.

When comparing our results with Fogel and Nehmad's (2009) we found similarities regarding certain information that is shared, such as full name (82% vs. 76%), profile picture (86% vs. 83%), home address (9% vs. 8%) and phone number (9% vs. 13%). We also noted dissimilarities regarding certain items, namely instant messenger (49% vs. 29%) and interests (83% vs. 64%). We argue that the dissimilarities are due to the fact that our sample's demographical characteristics are highly different from theirs. Proceeding tests performed with respect to demographical characteristics will show that this is the case.

Respondents show signs of more moderate SNS use when reporting how frequently their status message on Facebook is updated (Table A34). Almost 70% stated that they update their status message several times per week or several times per month. Only 5% update their status message several times per day.

Another risk-taking measurement that we devised ourselves is the question of whether or not adding third-party applications to one's Facebook account is likely to be harmful. As third-party application providers have a right to access the users' data (Tuunainen, et al., 2009), we argue that this was a relevant measure to include. Also, as third-party applications on Facebook may include harmful code, with basically no way for the user to assess the safety of the applications, a lower number of applications added may indicate a higher awareness of privacy and security. We found that Facebook users do not seem to install more than a few third-party applications to their account (Table A35), with 75% responding that they have installed four applications or less. Out of them, 30% respond that they have not installed any third-party applications at all. Only 3.5% respond that they have installed 20 applications or more.

Users of SNS express some concerns regarding the information submitted to Facebook. Around 50% agree or strongly agree when asked a question about this (Table A36), which is similar to Tuunainen et al.'s (2009) findings. Furthermore, users are in doubt whether their information is actually well protected by Facebook (Table A37). The answers to this question almost follow the normal distribution, with neutral being the most common answer, accounting for 35% of all participants. The answers 'disagree' and 'agree' both count for an equal amount of the answers, with 27% each. Only 2% strongly agree that their information is well protected by Facebook. In assessing the answers to this question, we found that our sample is a bit more skeptical than Tuunainen, et al.,'s (2009), possibly due to demographic differences between the samples. It could also be the result of increased user skepticism towards Facebook, due to the negative publicity it has received during the last months in particular.

More than 75% agree or strongly agree when asked if they are aware of Facebook's privacy settings (Table A38), different from Strater and Richter (2007) who report that most college students are not familiar with the privacy settings. We also found that more than 80% agree or strongly agree that they have made a conscious choice regarding their privacy settings (Table A39). This was also shown when our respondents were asked whether they had changed their privacy settings from the default ones (where everything

is visible to everyone), with more than 85% answering that they had, in fact, changed their privacy settings (Table A40). These results are in line with Tuunainen, et al.,'s (2009) results when asking questions about the awareness and usage of privacy settings, even if their sample scores a bit higher on the awareness question (94%). The results are, however, different from Gross and Acquisti's (2005) and Acquisti and Gross' (2006) results, showing that few Facebook members change the default privacy settings. We note that Tunnainen, et al.,'s (2009) and our higher scores pertaining to this question may, again, be due to the increased awareness of the general public regarding the possible harms of leaving all information open for everyone to see, made possible by an increase in media coverage during the recent years.

We furthermore asked our respondents if they were aware of who could see their profile and the information in it (Table A41). Here, too, more than 80% responded with agree or strongly agree, communicating a strong awareness of this area. Around 10% disagreed or strongly disagreed to the question. Tuunainen, et al., (2009) received similar results, with 75% agreeing to the same question. Strong privacy protection behavior was also visible when respondents were asked whether they would add an unknown person as a friend (Table A42). Almost 80% disagreed or strongly disagreed, communicating that they would not add an unknown person as a friend. Only 8% agreed or strongly agreed. We here found a puzzling difference to Mohtasebi and Borazjani's (2010) findings, which report that 48% will accept friend requests from unknown people. The difference between the findings, we argue, must lie in the sample as Mohtasebi and Borazjani's (2010) sample includes only Malaysian students.

We have already noted that the vast majority of Facebook users have added four third-party applications or less to their account, with only 30% reporting that they have not added any third-party application. Is this because they see a risk in adding more of them? In doing our analysis, we found that yes, this may be the case. We stated that adding applications in Facebook is not likely to be harmful, and found that 36% of the respondents disagreed and 18% strongly disagreed with us (Table A43). As few as 15% agreed or strongly agreed to our statement. However, an unusually high amount of our

respondents were being neutral (32%), possibly indicating that they were not able to see the relationship between risk-taking and third-party application adding at all.

We then asked questions pertaining to Facebook's terms and conditions and privacy policy. In the first question, our respondents were simply asked whether they were aware of the terms and conditions (Table A44). Almost 50% agreed or strongly agreed. Slightly more than 25% disagreed or strongly disagreed. However, out of the 50% that agreed or strongly agreed, only 7% were in the strongly agree category, most certainly indicating that the majority of them probably only had some vague idea regarding what is stated in them. This can be argued because there is reason to believe that if one really knows the terms and conditions, then the answer to the question is most probably strongly agree. For example, we can compare our answers with Tuunainen, et al.,'s (2009) who ask a yes or no question based on if the respondents have actually read the terms of use/privacy policy. Only 15% respectively 21% answer positively. Similar grim results have been found by numerous researchers (Mohtasebi and Borazjani, 2010; Acquisti and Gross, 2006; Gross and Acquisti, 2005; Jones and Soltren, 2005), strengthening our argument that the part of our sample that responded with agree has most likely received some slight information about the terms and conditions from a secondary source or have themselves only skimmed through it.

Interesting results were found when our sample was asked whether or not Facebook's terms and conditions affected if they would participate in it (Table A45). As many as 25% disagreed with us, with 32% being neutral. Thus, the majority of Facebook users do not seem to care much regarding what their terms and conditions are. Indeed, we found that only 6% strongly agreed to this question. This, we argue, is in line with the social exchange theory. The users seem to find that the benefits of using Facebook outweigh the possible risks/costs in doing so, even if the terms and conditions and the privacy policy is highly unfavorable for them.

Lastly, we asked our respondents if they had become more aware of their use of SNS after answering our questionnaire (Table A46). Around 40% agreed or strongly agreed

whereas only 19% disagreed or strongly disagreed. We take this as evidence that our questionnaire has helped at least some individuals understand the possible risks associated with sharing information on SNS. Similar results have been found by Acquisti and Gross (2006) and Tuunainen, et al., (2009), both presenting indications that survey participants have gained insights into this area by taking part of a survey.

In addition, it should be noted that the answers to question 17 were all over the map. That is, a significant part of our sample did not understand the question and consequently responded either with an unrealistic value or with a bogus value. Out of 239 valid answers to our questionnaire overall, we found that only 136 individuals had responded with a value that could be deemed somewhat realistic. However, we chose not to continue performing data analysis on the answers to this question, partly due to the uncertainty regarding the truth value of these findings. One conclusion that can be drawn is that this type of question may not be suitable to ask in an online questionnaire, where individuals have limited possibilities of posing questions about a specific question. Another conclusion is that the question may not be suitable to ask based on the relatively low average age of our sample, which may have limited the understanding of the question.

5.2 Demographical Differences

In respect to the following analyses, including those pertaining to demographical differences, we have chosen to emphasize results that have been found statistically significant using a 10% alpha (α) level as our minimum threshold. This includes highlighting results that oppose other researchers' findings. We will base our conclusions on the overall pattern formed by our results in combination with the results from previous studies considering demographical differences.

5.2.1 Gender Differences

The Goodman and Kruskal Tau's measurement of association was used to explore the relationship between gender and our variables. For testing differences between genders, Mann-Whitney U tests were conducted between gender and the ordinal variables, while

the Chi-square test for independence was similarly used in the case of nominal variables. Specifically for the Mann-Whitney test, we also report the mean rank for each group in order to help describe the direction of the difference. For measuring association between gender and ratio variables, we used the eta (η) measure.

First, our analysis showed that regarding general online privacy, women are more concerned than men (p=.003 Table B1 and B2:Concerned_privacy). This actually adds to a compilation of other previous studies (Sheehan, 1999, Rodgers and Harris, 2003, Cho, et al., 2009) that have come to the same conclusion. However, what lies behind this difference remains an intriguing question. We also found that there was no significant difference between the genders on general attitudes towards risk-taking (p=.582 on Achieve_risks and p=.218 on Reward_Risk Table B2). This is opposed to Fogel and Nehmad (2009) who suggest that men have a greater risk-taking attitude than women. This discrepancy could be due to the small number of items in our scale which may not provide a sufficient measurement for assessing risk-taking. Expectedly, no association was found between gender and the majority of characteristics and activities; neither on SNS in general, nor on Facebook in particular (Table B3).

For the Facebook users, we found that women are more concerned about submitting information to the site (p=.009 Table B1 and B2:FB_Concern_Info). When closely observing the piece by piece information that is provided to Facebook, we noticed further differences between the genders. We found that as many as 30% of the women in our sample do not provide their actual or full name on their profile (p=.007 Table B4). A similar question was posed by Fogel and Nehmad (2009) who found no gender differences. However they did report that 24% of the women were reluctant to use their real name. Though both genders largely choose not to reveal their instant messenger account and phone number, women are less likely than men to provide such information (p=.005 Table B5, p=.052 Table B6), mirroring the results of Fogel and Nehmad (2009). This difference could be due to a number of reasons. First, based on the social exchange theory, women seem to understand the importance of keeping their contact details private as they perceive risks related to this information-sharing. For example, they may see risks

with their instant messenger address, phone number, or real name being used by cyberstalkers or cyberbullies (Salaway and Caruso, 2008). From another point of view, the result could be explained by the fact that men are using instant messaging more than women (Chung and Nam, 2007). And as Fogel and Nehmad (2009) suggest, it is more common in offline settings (face-to-face conversations) that men give out their phone numbers to others. Also, with the possibility of developing and extending new online relationships through SNS (Dwyer, et al., 2007) combined with the fact that men have used SNS to find dates (Salaway and Caruso, 2008), we argue that men could be more motivated to make contact or to make themselves contactable using other communication channels (instant messenger and phone). Thus, their decision to share contact details makes sense according to the social exchange theory.

On top of these differences, more men than women disclose other types of potentially sensitive information, such as their relationship status (p=.024 Table B7), sexual orientation (p=.000 Table B8), and personal interests (p=.002 Table B9). Furthermore, 50% of the men indicate their religious views, whereas only about 35% of the women share this information with others (p=.042 Table B10). However, we may not be able to suggest why there is a gender divergence on these four information items. We speculate that these differences in information disclosure may be attributed to the differences found regarding privacy concerns. They may also be related to other personal characteristics, such as one's self-esteem, which was found by Dolgin, et al., (1991). Ending our analysis of information disclosure, we found that there is a relationship between gender and the overall amount of information shared (η=.260 Table B11).

In respect to awareness, we found that the women are more aware of who can access their Facebook profiles and the information in it (p=.046 Table B1 and B2: FB_Aware_Info). Although a majority comprised of both genders report that they would not accept a friend request from an unknown person on Facebook, the difference lies in almost 30% of the men (compared to 12% of the women) being neutral or positive about it (p=.000 Table B2 and B12). This is in line with Hoy and Milne's (2010) findings about women being more careful in befriending on SNS and it is also an interesting finding considering that a

study by Jones and Soltren (2005) has reported that such 'stranger-befriending' difference does not occur between the genders. Accordingly, due to the argument about women and cybercrimes (see Salaway and Caruso, 2008), and based on our results on women's attitudes towards information disclosure, it may be fair to reason that the women are not comfortable sharing their personal information with strangers, and therefore, perceive more risk of adding them to their connections (friend list). In addition, a majority of both men and women show relatively strong awareness of Facebook's privacy settings and at least 85% of each gender have changed their settings from the default settings in Facebook (Table B13). Even so, from the selective befriending strategy we could partially conclude that the women in our sample have shown more proactive behavior as it relates to protecting their online information. Lastly, we found that more women than men agree that Facebook's terms of usage and privacy policy is a factor influencing their decision whether or not to join the site (p=.052 Table B1 and B2: FB_Terms_Part). This may be because women are more prone to seek for assurance that their privacy is being protected (Fogel and Nehmad, 2009).

5.2.2 Age Differences

To analyze the age differences, we performed several analyses using the variables Age (continuous) and AgeGroup (ordinal). Both variables will be referred to differently in this report. We classified the variable age into the following four groups (AgeGroup); respondents 20 years old or below are in the first group, ages 21 to 25 are in group two, from 26 to 30 are in group three, and above 30 years old in group four (see Chapter 4 Table 2). Spearman's rho and the point biserial correlation coefficient were calculated accordingly to explore the relationship between Age and our study variables while Goodman and Kruskal's tau was used to measure the associations pertaining to the AgeGroup variable. The Kruskal-Wallis H test was used to compare the age groups with the ordinal variables while the Chi-square test for independence was similarly used for tests including a nominal variable. When the Kruskal Wallis H test detected differences across these four age groups, we further performed Mann-Whitney U tests on each pair of

groups in the AgeGroup variable to identify if there was a significant difference between the specific pairs of age groups too. Specifically for the Mann-Whitney test, we also report the mean rank for each group in order to describe the direction of the difference. For measuring association between age group and ratio variables, we used the eta (η) measurement.

First, our results show that age is neither associated with general risk-taking attitude (Table C1:p=.188 Achieve_risks; p=.604 Reward_risks) nor with general online privacy concerns (p=.262 Table C1: Concerned_privacy). Similarly, tests performed on the AgeGroup variable also detected no differences using both measurements. Particularly for privacy concerns, this finding is opposed to Paine, et al., (2007) who finds that age and privacy concerns are positively related. Instead, our results support Hoofnagle, et al., (2010) who finds that young adults and old adults are equally concerned about their privacy.

Our analysis showed that there is a correlation between the respondent's age and whether the respondent is having any profile on a SNS or not (r=-.128, n=237, p=.049 Table C1:Profile_SNS), with an increase in age translating into a decrease in the likelihood of having a SNS profile. Furthermore, we found that the older a user is, the more likely it is that the user will have profiles on several SNS (r=.156, n=208, p=.025 Table C1:Nbr_SNS). Continuing our analysis, we noted that people between 26 and 30 years old are more likely than the youngest group to have profiles on multiple SNS (p=.005 Table C3). Also, age is positively related to having a LinkedIn profile (r=.321, n=208, p=.000 Table C1:Profile_LinkedIn). The latter is also supported by Royal Pingdom's (2010) statistics which state that LinkedIn is dominated by older adults (35-54 years old) with an average age of 31 years.

Nevertheless, regarding SNS characteristics and activities, we discovered that higher age is related to being less frequently active on SNS (r=-.227, n=208, p=.001, Table C1:Frequently_active). Moreover, age is also negatively related to the number of friends a user has on SNS (r=-.276, n=208, p=.000 Table C1:Number_friends_SNS). In other

words, the older a person is, the less active he is and the less number of friends he probably has on SNS. We also found evidence from the Kruskal-Wallis (Table C2) and the Mann-Whitney test that the oldest group (30+) are significantly less active (p=.002, p=.000 and p=.000 against group 1, 2 and 3 respectively Table C4) and have less friends on SNS (p=.000, p=.000 and p=.000 against group 1, 2 and 3 respectively Table C5). Based on Joinson's (2008) findings, we argue that the amount of time spent and the frequency of visits to SNS is affecting young people to make new connections more extensively compared to older people. In addition, we noted that the respondents between 21 and 25 years old have been able to adopt SNS for a longer time period compared to the adopters from the youngest (p=.004) and oldest (p=.033) group (Table C6).

With regard to information disclosure, we found that age is negatively associated with revealing information about one's birthday (r=-.257, n=201, p=.000 Table C1:FB_Birthday), instant messenger address (r=-.144, n=201, p=.042 Table C1:FB_IM), sexual orientation (r=-.157, n=201, p=.026 Table C1:FB_Sex_or) and education and work background (r=-.202, n=201, p=.004 Table C1:FB_Edu_Work). A similar relationship between age and sexual orientation disclosure is reported by Tufekci (2008). However, when we conducted tests for independence across the age groups, we no longer encountered any association between age and sexual orientation, education or work background. Instead we detected correlation in religious views (tau=.040, p= .046 Table C7: FB_Relviews). Accordingly, the Chi-square test for independence showed age group differences in disclosing birthday (p=.012 Table C8), instant messenger address (p=.004 Table C9) and religious views (p=.045 Table C10). Over 75% of respondents less than 30 years old reveal their Birthday information in contrast to 60% of the oldest group (Table C8). The majority of people above 20 years old report not having provided their instant messenger account, however half of the youngest group claim otherwise (Table C9). Interestingly, our results revealed that users between 26 and 30 years old are unlikely to disclosure their religious views compared to the other groups, who are being equally divided on this question (Table C10). Despite a few dissimilar results from the tests on information sharing depending on whether we used Age or AgeGroup, we still confirm that one's likelihood to disclose information is related to one's age. In this respect, we see

that the tendency to provide information lessens as a person gets older. The numerical measurement of the relationship between age and the overall sum amount of information disclosed was found to be η=.235 (Table C11), which expresses a slight association.

For Facebook users, we found that there is a negative relationship between age and thinking that one's personal information being well protected by Facebook (r=-.251, n=201, p=.000 Table C1:FB_Info_Wellprot). Moreover, our Kruskal-Wallis (p=.006 Table C12: FB_Info_Wellprot) and Mann-Whitney test (Table C13) confirmed that individuals over 30 years old are showing less trust in Facebook to protect their privacy information compared to the groups including individuals 25 years old or less (p=.000 and p=.019 against group 1 and 2 respectively). This is consistent with the literature, for example Hoofnagle, et al., (2010) who points to the naiveté among young people when it comes to assuming that their privacy is protected by law. An additional finding related to differences in age demographics is the positive correlation between one's age and whether Facebook's terms of use has affected one's decision regarding Facebook membership (r=.173, n=201, p=.014 Table C1: FB_Terms_Part). Based on these results, it seems that as people turn older and mature, they are more likely to consider a range of variables before making an informed decision. This includes examining the benefits and costs of agreeing to something (in this case, the terms and conditions and privacy policy). Finally, we found that as many as 93% of the individuals under 25 years old claim to have changed their Facebook privacy settings (Table C14). This coincides with Joinson (2008) who has previously concluded that young users are in the majority when it comes to using privacy settings.

5.2.3 Geographical Differences

Similarly, for performing analyses based on the geographical background of the respondents, we used the variable ContinentGroup (nominal). The nationalities of the respondents were first classified into the following four groups; respondents from Asia are in the first group, Europeans are in group two, North Americans are in group three and Africans are in group four (see Chapter 4 Table 2). Based on Goodman and Kruskal Tau's coefficient, Table D1 presents the measures of the relationships between several of the studied variables as they depend on the continent. The Kruskal-Wallis H test was used to compare the continent groups with the ordinal variables while the Chi-square test for independence was similarly used for the nominal variables. When the Kruskal Wallis test detected differences, we further performed Mann-Whitney U tests on each pair of groups in the ContinentGroup to identify between which ones there were differences. Specifically for the Mann-Whitney test, we also report the mean rank for each group in order to describe the direction of the difference. For measuring association between continent and ratio variables, we used the eta (η) measurement.

First, we found that one's continent is not associated with one's perception of risk-taking attitude (Table D1: p=.575 Achieve_risks; p=.797 Reward_risks). However, when asked to rate their general online privacy concerns, respondents from Asia exhibit higher concerns compared to those from other continents (p=.003 Table D2:Concerned_privacy), especially compared to respondents from Europe (p=.000) and North America (p=.005) (Table D3). This result can be partially linked to Lynch and Beck (2001) who suggest that people from Asia are more apprehensive compared to North Americans towards Internet shopping. We then studied their SNS characteristics and their engagement in Facebook activities (Table D2 SNS_how_long; Number_friends_SNS; Nbr_SNS; Freq_stsupdate). Asians report having used SNS for a longer period of time than Europeans (p=.006) and Africans (p=.001) (Table D4). This may be due to SNS like Friendster which have majorly dominated Asia during the early years of SNS. Hence, these sites have been giving Asians an early and wide exposure to SNS which has allowed them to follow the trend by continuing to use them ever since.

Based on our list of SNS in the questionnaire, we found that Europeans have the least number of profiles on SNS (Table D5). Subsequently, we detected correlations between continent and specific SNS membership, such as Friendster (tau=.233;p=.000), Hi5 (tau=.116;p=.000) and MySpace (tau=.055;p=.013) (Table D1: Profile_Friendster; Profile_Hi5; Profile_MySpace). According to our results, Asians have a greater number of friends in all of their SNS profiles combined as compared to Europeans (p=.000), North Americans (p=.036), and Africans (p=.039) (Table D6).

Comparing Asians with Europeans (p=.018) and Africans (p=.012) (Table D7), it appears that the former are more likely to share their whereabouts by frequently posting status updates on the site. Asians have also got significantly more third-party applications added to their profile compared to people from other continents (p=.000 Table D8:Nbr_apps), showing that they may be seeking even more social contact and amusement, permitted by these applications, which goes outside of what is seen as limited Facebook features and its first-party applications. This tendency may be explained by the fact that 30% of our Asian respondents (compared to 8% Europeans, 11% North Americans, and 15% Africans) agree to the statement that adding third-party applications in Facebook is not likely to cause any harm (Table D9). Based on the social exchange theory, we suggest that Asians may have installed more applications since their perception is that the benefits gained outweigh the potential risks associated with these applications.

Furthermore, we noted that there are some relations between the continent and the likelihood of disclosing specific profile information. More specifically we found associations between continent and birthday (tau=.045; p=.035), profile picture (tau=.105; p=.000), e-mail address (tau=.051; p=.021), home address (tau=.060; p=.009), instant messenger address (tau=.066; p=.006) and posting photos of oneself (tau=.108; p=.000) (Table D1: FB_Birthday; FB_Profpic; FB_Email; FB_Address; FB_IM; FB_Photo_yrslf). 90% of the Asians reveal their birthday details in contrast to 63% of the Africans (p=.034 Table D10). More than 80% of the respondents from Asia, Europe and North America have a profile picture on Facebook, yet only around 50% Africans have one (p=.000 Table D11). This is followed by more than 50% of the African users who

respond not having included any photos of themselves other than their profile picture (p=.000 Table D12). Europeans and North Americans seem less enthusiastic about disclosing their e-mail addresses, compared to at least 80% of the Asians and Africans who are comfortable displaying this information (p=.021 Table D13). Interestingly, almost all (76 out of 77) Europeans in our sample do not want to state their home address in the profile (Table D14). Also, only around 15% of the Europeans share their instant messenger account information compared to 43% of the North Americans (p=.005 Table D15). Drawing from the above patterns, it seems that the Europeans consider their e-mail address, home address, and instant messenger account very private information. As for the relationship between continent and the overall sum of information disclosed, we calculated an eta value of η=.261 (Table D16). Similar to the gender and age characteristics, this eta (η) value indicates a slight association between geographical background (continent) and overall information-sharing.

When probed about their perception regarding whether their personal information is being well-protected by Facebook, we found that Asians (p=.001) and North Americans (p=.038) are more likely than the Europeans to assume that Facebook is protecting their privacy (Table D17). Over 50% of the European respondents show disagreement related to this view compared to only 18% of the Asians and 27% of the North Americans (Table D18). In IBM's (2010) Global Innovation Outlook report, Asian countries in particular, like Singapore and China, have been reported reflecting similar beliefs towards Web 2.0 applications in general.

Though most of the respondents state that they have made some form of conscious decision before regarding their Facebook account privacy settings, 44% of the Africans have not or answer neutrally (Table D19). However, regardless where the respondents are from, we found no difference concerning their likelihood to change their privacy settings (Table D20). This could include the other 56% of the Africans, for instance, who are aware of their decisions towards privacy settings but may intentionally have left their settings in the default or 'everyone' mode. Another interesting finding is the significant geographical differences regarding accepting strangers as friends (p=.004 Table D8:

FB_Friend_Unknwn). Close to 30% of the Asians and 40% of the Africans are fine with allowing an unknown person into their group of connections as opposed to less than 15% of Europeans and North Americans (Table D21 and D22). Based on the earlier result pertaining to the number of friends one has on SNS, we assume that the likelihood of the Asians adding unknown people may have contributed their higher number of SNS friends (in comparison with the Europeans and the North Americans).

5.3 Correlations and Constructs

From the outset we noted that some of our questionnaire items could possibly be measuring the same hidden variable (construct). However, with a serious limitation on the number of questions that our respondents would feasibly answer, a limitation regarding construct creation, we noted, would be found as well. Indeed, to create constructs, one often should have a number of questions pertaining to that specific construct as this makes often-used measurements related to constructs have higher values (Pallant, 2007). Even if this limitation was noted it did not deter us from examining the correlations between questionnaire answers to find relationships between questionnaire items as well as make possible analyses involving constructs as opposed to single questionnaire items.

To examine correlations between variables we calculated the Spearman's rho correlation coefficients between all of the variables having ordinal scales (Table E1). Some of the more obvious relationships we found were between how long a person has used SNS and the total number of friends one has on SNS (r=.473, n=201, p=.000), how frequently one is active on these sites (r=.205, n=201, p=.003) as well as how many SNS one is active on in total (r=.323, n=201, p=.000). Individuals who reported overall concerns about their privacy when using the Internet were also responding that it is important for them to protect their identity information (r=.418, n=201, p=.000), greater concerns about the information submitted to Facebook (r=.396, n=201, p=.000) and that Facebook's terms and conditions affect their decision whether or not to participate in it (r=.259, n=201,

p=.000). They were also more prone to respond that they had become more conscious of their use of SNS after completing our questionnaire (r=.242, n=201, p=.001). Likewise, individuals who thought that their information was well-protected on the Internet in general also thought that their information was well-protected on Facebook (r=.416, n=201, p=.000) and were also less concerned about the information submitted to Facebook (r=-.223, n=201, p=.001). Individuals who are more aware of the information they display on Facebook also show a higher awareness of privacy settings (r=.432, n=202, p=.000), a higher level of having made a conscious decision regarding their privacy settings (r=.497, n=202, p=.000) as well as being aware of (r=.269, n=202, p=.000) and affected by (r=.196, n=202, p=.005) Facebook's terms and conditions and privacy policy. And even if more awareness of the information displayed on Facebook was found to be positively related to the number of third-party applications added (r=.186, n=202, p=.008), it was also positively related to thinking that third-party applications were harmful (r=-.171, n=202, p=.015, note the negated question). This is contradictory and suggests that those individuals may have performed a cost and benefit analysis to come to the conclusion that adding applications will result in a higher rewards compared to the cost of possible harm of doing this, in line with the social exchange theory.

We used the items showing the highest correlations to form constructs. This resulted in the creation of our first construct named Awareness (Constr_aw), which was created based on the questionnaire items found in Table 4. This construct measured the level of overall awareness of the possible risks of information sharing. It displayed sufficient reliability, with a value for Cronbach's alpha value of .719 (Table E2) and a mean inter-item correlation of .31. A second construct, Activity (constr_act), was created including the variables found in Table 5. This construct represented the overall activity on SNS by an individual. We found that this construct had a Cronbach's alpha value of .645 (Table E3) and a mean inter-item correlation of .27. It is also worth noting that a variable Sum_Info_Reveal was created by summing all of the information shared on Facebook together. More specifically, as every question pertaining to a specific type of information shared on Facebook could have the values yes or no (0 or 1), this allowed an

interval/ratio variable to be created from binary ones. This variable was then treated as a measurement of the total amount of information shared.

Construct	
Awareness	**Activity**
FB_Aware_Info	SNS_how_long
FB_Aware_privsett	Frequently_active
FB_Consc_privsett	Number_friends_SNS
FB_Aw_Terms	Freq_stsupdate
FB_Terms_Part	Nbr_SNS

Table 4: Constructs

5.4 Linear Regression

Linear regression using the OLS method with Sum_Info_Reveal as the dependent variable and Age and Gender as the independent variables was performed. Both variables were found significant with Age having a slightly negative (B=-.079, p=.001) relationship and Gender also displaying a negative relationship (B=-1.421, p=.000) (Table F2), meaning that older individuals, all other things equal, share less information on SNS and that women generally share less information than men. The explanatory power of this model, however, was found to be pretty low, with R-squared and Adjusted R-squared values of .116 and .107 (Table F1), respectively. When testing if the error term in this model had a constant variance, we found that this was indeed the case (p=.097 Table F3). Similarly, we found that its residuals were normally distributed (p=.10 Graph G4). However, we note that the relationship between the continuous variable Age and the amount of information revealed is not straight-forward to interpret (Graph G5) as our sample has a high concentration of individuals roughly between 20-30 years old. Considering the difficulty of interpreting this graph, the preceding tests on information sharing using age groups should be taken into consideration as well.

It has been suggested by Tuunainen, et al., (2009) that the more details an individual provides, the more active of a user of SNS the individual is. Similarly, Lampe, et al.,

(2006, 2007) found a positive association between the level of information disclosure and the number of friends. Consequently, we sought to test whether the amount of information revealed is related to how active an individual is on SNS. When testing the relationship between the amount of information revealed and our Activity construct, we found that activity indeed seems to be related to the amount of information revealed (Graph G6). Performing a linear regression with the amount of information revealed as the dependent variable and the construct activity as an independent variable (more on this below), we received proof that our initial assumption was correct; the variables seem to be positively related to each other (B=.315, p=.000) (Table F5) with a higher activity being correlated with more information revealed. This model has some degree of explanatory power, with R-squared and Adjusted R-squared values of .21 and .206 (Table F4), respectively. It also passed the test for heteroskedasticity (p=.43 Table F6), meaning that the error term is constant over time. Moreover we found that its residuals follow the normal distribution (p=.12 Graph G7).

It is worth noticing that Tuunainen, et al., (2009) explains the relationship between activity and information sharing as *"the more detail is provided in the profile, the more active user of Facebook the respondent is"* (Tuunainen, et al., 2009, p. 10) whereas we consider this argument of causality to be backwards. If one wants to speculate as to which causal relationship exists between the variables, a more logical conclusion would be that the more active a user is on SNS, the more information the user generally also provides on SNS. This would furthermore be somewhat akin to Christofides, et al., (2009) who find that *"General tendency to disclose and need for popularity were the only significant predictors of information disclosure on Facebook"* (Christofides, et al., 2009, p. 343).

Further elaborating on this model, we found that by including both Age and Gender into the model, its explanatory power increased, R-squared to .297 and Adjusted R-squared to .286 (Table F7). Moreover, we found that all of the variables were significant at the 5% level and that their coefficients were consistent with common-sense. Thus, Activity was still positively correlated (B=.300, p=.000) with the amount of information revealed whereas Age (B=-.045, p=.043) and Gender (B=-1.498, p=.000) (Table F8) were still

negatively correlated. This model passed one of the elementary tests pertaining to regression models; the test for heteroskedasticity (p=.296 Table F9). In contrast, it barely failed the test for normally distributed residuals at the 5% level (p=.0487 Graph G8). However, again we would like to point out the relationship between Age and the amount of information revealed which does not have an obvious interpretation (Graph G5), leading us to be somewhat skeptical of the inclusion of this variable in the model.

We also sought to test the relationship between Awareness and the amount of information revealed as there is reason to believe that the more aware an individual is of the potential harms of revealing information, the less information the individual would then choose to reveal. However, examining Graph G9, we find that there is no relationship at all between these two items. Tufekci (2008) and Dwyer, et al., (2007) have tested a similar relationship by examining if online privacy concerns are related to information disclosure on SNS. The results from these tests were, similarly, that no relationship could be found. Likewise, Acquisti and Gross (2006) were not able to find a relationship between privacy attitudes and the likelihood of providing certain information to SNS. We speculate that these results may be due to the cost and benefit analysis that individuals perform, as posited by the social exchange theory. Thus, an individual may be highly aware of the risks of sharing information, but may choose to take these risks due to the potential benefits in doing so. Furthermore, explanations such as herding behavior or peer pressure, as provided by Acquisti and Gross (2006), cannot be ruled out.

6. Conclusions

Overall, individuals seem to find it important to protect their identity information online as well as on SNS. They also exhibit great concerns over the information shared, both on the Internet in general and on SNS in particular. In line with this, they are also highly skeptical regarding whether or not their personal information is actually protected both on the Internet in general and on SNS in particular.

When studying their actual behavior, we found that users are generally very active on SNS and share a plethora of information. However, the information is most often protected using the sites' available privacy protections. But there is reason to believe that individuals display naiveté when relying on these privacy controls, especially since many of them are oblivious regarding these sites' terms and conditions and privacy policy. By analyzing the amount of information that is possible to share on SNS in relation to the amount of information that users actually share, we found that information that may be regarded by the users as sensitive is less likely to be shared. This points to a manifestation of the previously noted concerns. When comparing our results to the results of previous studies, we also found that individuals seem to have evolved their knowledge of privacy and information-sharing over the last years as our measures of information-sharing generally score lower compared to earlier studies. We speculate that the increased awareness may be due to increased attention on these areas from the media.

We also found that individuals who display high awareness concerning privacy are, in fact, equally likely as their peers to share information on SNS. In contrast, individuals who are more active on SNS generally also share more information on these sites. Furthermore, individuals do not seem to take the terms and conditions and privacy policy into consideration when deciding whether or not to participate in a SNS. These results are in line with the social exchange theory. Indeed, individuals seem to be performing cost and benefit analyses related to their actions on SNS, which may help explain why they are participating in the face of great concerns as well as why they would continue to do so somewhat regardless of the SNS' terms and conditions and privacy policy.

Based on our analysis, we also found several demographical differences. Similar to their attitudes towards the Internet in general, women are more concerned than men about submitting information to SNS. This is also shown in their reluctance to disclose specific information, for example their contact details. Women also appear to have a higher sense of awareness about privacy related matters as well as stronger privacy protection behavior. For example, they are more careful about whom to befriend and they take the SNS' terms and conditions into more significant consideration.

Our study furthermore shows that older individuals tend to disclose less personal information. This is especially true for people above 30 years old, who are, in general, not convinced that their privacy is being protected by SNS. Somewhat counterintuitively then, we found that younger users are generally making more use of the available privacy settings compared to older users. This could be related to the amount of information that younger users choose to disclose where more information, everything else equal, requires stronger privacy settings. It would mean that a significant level of trust is placed on these privacy settings being able to safeguard their information. Older users may be skeptical of the idea that it is possible to safeguard information entered into the system in the first place, regardless of the privacy settings applied. Thus, their solution to the dilemma is rather not to enter any information that could be sensitive and therefore in need of applied privacy settings. Related to the social exchange theory, it could also be the case that older individuals' cost and benefit analyses related to subsequent social exchanges include less perceived benefits compared to the perception of younger individuals. Consequently, their choice of disclosing less information makes sense.

In comparing continents, we found that Europeans tend to make more careful judgments regarding information-sharing on SNS and generally perceive that they need to protect their information 'on their own' (that is, they do not trust the SNS to protect their information). Despite Asians showing higher concerns regarding general online activities, it appears that the concerns do not completely carry through when it comes to their use of SNS. There is a great proportion of Asians who do not mind accepting unknown 'friend'

requests, as well as a significant proportion assuming that third-party applications are harmless. We find these results strange as Asians display more overall concern related to the Internet compared to other groups, even if the same concern is not apparent when it comes to SNS. Asians have also, in general, had a longer experience of SNS which should logically be related to more privacy awareness. Our hypothesis is that many of these discrepancies may be related to differences in news reporting, where Western newspapers have treated SNS with more skepticism. It may also be due to other cultural differences skewing the cost and benefit analysis, such as the perception that more friends and more applications are weighed higher in terms of benefits for the Asians.

Conclusively, we note that the social exchange theory is suitable for analyzing this area. It seems as though individuals behave rationally when being active on SNS, even if their rationality is limited by their assessment of the costs and benefits, ultimately depending on their knowledge. This implies that public information regarding this area will still be vital for informing individuals of the potential costs of sharing information on the Internet in general and, arguably, on SNS in particular. As the benefits are highly visible, highlighting the costs will eventually push organizations in any way involved with SNS to tailor their offerings to better meet the standards of the general public.

6.1 Limitations and Future Research

As mentioned throughout the text, our study has several limitations. First, the sample used does not include individuals in equal proportions based on our demographical characteristics of choice. Second, the data used and its related statistical tests do not allow us to make causal statements. Third, the constructs created display values sufficient for exploratory research, however the relatively low values for the reliability tests suggest that more relevant constructs measuring the same phenomena could be created. These are obvious areas that could be improved in future research.

Furthermore, as we have found differences based on demographical characteristics, an evident area for future research would be to investigate in-depth why these differences

exist. This may include performing qualitative research in the form of, for example, interviews.

Likewise, as we have noted that individuals tend to perform cost and benefit analyses related to their activities on SNS, it would be interesting to understand more specifically how they assess and weigh these expected costs and benefits. This, too, would probably best be examined using qualitative research methods.

Appendix A: Descriptive Statistics

Table A1

Gender

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	122	51,3	51,5	51,5
	1	115	48,3	48,5	100,0
	Total	237	99,6	100,0	
Missing		1	,4		
Total		238	100,0		

Table A2

Age Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Age	237	14,0	60,0	27,312	8,9795
Valid N (listwise)	237				

Table A3

ContinentGroup

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	55	23,1	24,3	24,3
	2	90	37,8	39,8	64,2
	3	52	21,8	23,0	87,2
	4	29	12,2	12,8	100,0
	Total	226	95,0	100,0	
Unspecified		12	5,0		
Total		238	100,0		

Table A4

Achieve_risks

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	1	,4	,4	,4
	2	10	4,2	4,2	4,6
	3	24	10,1	10,1	14,8
	4	135	56,7	57,0	71,7
	5	67	28,2	28,3	100,0
	Total	237	99,6	100,0	
Missing		1	,4		
Total		238	100,0		

Table A5

Reward_risks

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	2	,8	,8	,8
	2	21	8,8	8,9	9,7
	3	71	29,8	30,0	39,7
	4	108	45,4	45,6	85,2
	5	35	14,7	14,8	100,0
	Total	237	99,6	100,0	
Missing		1	,4		
Total		238	100,0		

Table A6

Important_protect

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	3	1,3	1,3	1,3
	2	5	2,1	2,1	3,4
	3	24	10,1	10,1	13,5
	4	98	41,2	41,4	54,9
	5	107	45,0	45,1	100,0
	Total	237	99,6	100,0	
Missing		1	,4		
Total		238	100,0		

Table A7

Concerned_privacy

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	4	1,7	1,7	1,7
	2	28	11,8	11,8	13,5
	3	34	14,3	14,3	27,8
	4	88	37,0	37,1	65,0
	5	83	34,9	35,0	100,0
	Total	237	99,6	100,0	
Missing		1	,4		
Total		238	100,0		

Table A8

Information_protected

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	17	7,1	7,2	7,2
	2	87	36,6	36,7	43,9
	3	67	28,2	28,3	72,2
	4	55	23,1	23,2	95,4
	5	11	4,6	4,6	100,0
	Total	237	99,6	100,0	
Missing		1	,4		
Total		238	100,0		

Table A9

Profile_SNS

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	29	12,2	12,2	12,2
	1	208	87,4	87,8	100,0
	Total	237	99,6	100,0	
Missing		1	,4		
Total		238	100,0		

Table A10

Profile_Facebook

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	36	15,1	15,1	15,1
	1	202	84,9	84,9	100,0
	Total	238	100,0	100,0	

Table A11

Profile_Friendster

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	215	90,3	90,3	90,3
	1	23	9,7	9,7	100,0
	Total	238	100,0	100,0	

Table A12

Profile_Hi5

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	206	86,6	86,6	86,6
	1	32	13,4	13,4	100,0
	Total	238	100,0	100,0	

Table A13

Profile_MySpace

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	174	73,1	73,1	73,1
	1	64	26,9	26,9	100,0
	Total	238	100,0	100,0	

Table A14

Profile_LinkedIn

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	199	83,6	83,6	83,6
	1	39	16,4	16,4	100,0
	Total	238	100,0	100,0	

Table A15

Profile_Bilddagboken

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	237	99,6	99,6	99,6
	1	1	,4	,4	100,0
	Total	238	100,0	100,0	

Table A16

SNS_how_long

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	14	5,9	6,7	6,7
	1	31	13,0	14,8	21,5
	2	49	20,6	23,4	45,0
	3	29	12,2	13,9	58,9
	4	30	12,6	14,4	73,2
	5	56	23,5	26,8	100,0
	Total	209	87,8	100,0	
Missing		29	12,2		
Total		238	100,0		

Table A17

Nbr_SNS

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	,00	29	12,2	12,2	12,2
	1,00	92	38,7	38,7	50,8
	2,00	87	36,6	36,6	87,4
	3,00	25	10,5	10,5	97,9
	4,00	5	2,1	2,1	100,0
	Total	238	100,0	100,0	

Table A18

Frequently_active

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	1	,4	,5	,5
	1	5	2,1	2,4	2,9
	2	20	8,4	9,6	12,4
	3	75	31,5	35,9	48,3
	4	108	45,4	51,7	100,0
	Total	209	87,8	100,0	
Missing		29	12,2		
Total		238	100,0		

Table A19

Number_friends_SNS

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	30	12,6	14,4	14,4
	1	25	10,5	12,0	26,3
	2	50	21,0	23,9	50,2
	3	47	19,7	22,5	72,7
	4	21	8,8	10,0	82,8
	5	11	4,6	5,3	88,0
	6	25	10,5	12,0	100,0
	Total	209	87,8	100,0	
Missing		29	12,2		
Total		238	100,0		

Table A20

FB_Name

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	48	20,2	23,8	23,8
	1	154	64,7	76,2	100,0
	Total	202	84,9	100,0	
Missing		36	15,1		
Total		238	100,0		

Table A21

FB_Birthday

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	47	19,7	23,3	23,3
	1	155	65,1	76,7	100,0
	Total	202	84,9	100,0	
Missing		36	15,1		
Total		238	100,0		

Table A22

FB_Email

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	63	26,5	31,2	31,2
	1	139	58,4	68,8	100,0
	Total	202	84,9	100,0	
Missing		36	15,1		
Total		238	100,0		

Table A23

FB_Hometown

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	41	17,2	20,3	20,3
	1	161	67,6	79,7	100,0
	Total	202	84,9	100,0	
Missing		36	15,1		
Total		238	100,0		

Table A24

FB_Profpic

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	35	14,7	17,3	17,3
	1	167	70,2	82,7	100,0
	Total	202	84,9	100,0	
Missing		36	15,1		
Total		238	100,0		

Table A25

FB_Photo_yrslf

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	41	17,2	20,3	20,3
	1	161	67,6	79,7	100,0
	Total	202	84,9	100,0	
Missing		36	15,1		
Total		238	100,0		

Table A26

FB_Relstatus

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	83	34,9	41,1	41,1
	1	119	50,0	58,9	100,0
	Total	202	84,9	100,0	
Missing		36	15,1		
Total		238	100,0		

Table A27

FB_Interests

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	72	30,3	35,6	35,6
	1	130	54,6	64,4	100,0
	Total	202	84,9	100,0	
Missing		36	15,1		
Total		238	100,0		

Table A28

FB_Edu_Work

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	70	29,4	34,7	34,7
	1	132	55,5	65,3	100,0
	Total	202	84,9	100,0	
Missing		36	15,1		
Total		238	100,0		

Table A29

FB_Relviews

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	117	49,2	57,9	57,9
	1	85	35,7	42,1	100,0
	Total	202	84,9	100,0	
Missing		36	15,1		
Total		238	100,0		

Table A30

FB_Sex_or

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	118	49,6	58,4	58,4
	1	84	35,3	41,6	100,0
	Total	202	84,9	100,0	
Missing		36	15,1		
Total		238	100,0		

Table A31

FB_IM

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	144	60,5	71,3	71,3
	1	58	24,4	28,7	100,0
	Total	202	84,9	100,0	
Missing		36	15,1		
Total		238	100,0		

Table A32

FB_Phone

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	175	73,5	86,6	86,6
	1	27	11,3	13,4	100,0
	Total	202	84,9	100,0	
Missing		36	15,1		
Total		238	100,0		

Table A33

FB_Address

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	186	78,2	92,1	92,1
	1	16	6,7	7,9	100,0
	Total	202	84,9	100,0	
Missing		36	15,1		
Total		238	100,0		

Table A34

Freq_stsupdate

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	27	11,3	13,4	13,4
	1	25	10,5	12,4	25,7
	2	66	27,7	32,7	58,4
	3	74	31,1	36,6	95,0
	4	10	4,2	5,0	100,0
	Total	202	84,9	100,0	
Missing		36	15,1		
Total		238	100,0		

Table A35

Nbr_apps

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	61	25,6	30,2	30,2
	1	92	38,7	45,5	75,7
	2	30	12,6	14,9	90,6
	3	10	4,2	5,0	95,5
	4	2	,8	1,0	96,5
	5	7	2,9	3,5	100,0
	Total	202	84,9	100,0	
Missing		36	15,1		
Total		238	100,0		

Table A36

FB_Concern_Info

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	6	2,5	3,0	3,0
	2	30	12,6	14,9	17,8
	3	65	27,3	32,2	50,0
	4	71	29,8	35,1	85,1
	5	30	12,6	14,9	100,0
	Total	202	84,9	100,0	
Missing		36	15,1		
Total		238	100,0		

Table A37

FB_Info_Wellprot

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	18	7,6	8,9	8,9
	2	55	23,1	27,2	36,1
	3	70	29,4	34,7	70,8
	4	55	23,1	27,2	98,0
	5	4	1,7	2,0	100,0
	Total	202	84,9	100,0	
Missing		36	15,1		
Total		238	100,0		

Table A38

FB_Aware_privsett

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	3	1,3	1,5	1,5
	2	12	5,0	5,9	7,4
	3	32	13,4	15,8	23,3
	4	110	46,2	54,5	77,7
	5	45	18,9	22,3	100,0
	Total	202	84,9	100,0	
Missing		36	15,1		
Total		238	100,0		

Table A39

FB_Consc_privsett

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	2	,8	1,0	1,0
	2	8	3,4	4,0	5,0
	3	28	11,8	13,9	18,8
	4	91	38,2	45,0	63,9
	5	73	30,7	36,1	100,0
	Total	202	84,9	100,0	
Missing		36	15,1		
Total		238	100,0		

Table A40

FB_Chg_Privsett

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	27	11,3	13,4	13,4
	1	175	73,5	86,6	100,0
	Total	202	84,9	100,0	
Missing		36	15,1		
Total		238	100,0		

Table A41

FB_Aware_Info

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	4	1,7	2,0	2,0
	2	17	7,1	8,4	10,4
	3	18	7,6	8,9	19,3
	4	94	39,5	46,5	65,8
	5	69	29,0	34,2	100,0
	Total	202	84,9	100,0	
Missing		36	15,1		
Total		238	100,0		

Table A42

FB_Friend_Unknwn

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	93	39,1	46,0	46,0
	2	67	28,2	33,2	79,2
	3	26	10,9	12,9	92,1
	4	13	5,5	6,4	98,5
	5	3	1,3	1,5	100,0
	Total	202	84,9	100,0	
Missing		36	15,1		
Total		238	100,0		

Table A43

FB_Apps_Harmful

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	36	15,1	17,8	17,8
	2	72	30,3	35,6	53,5
	3	64	26,9	31,7	85,1
	4	27	11,3	13,4	98,5
	5	3	1,3	1,5	100,0
	Total	202	84,9	100,0	
Missing		36	15,1		
Total		238	100,0		

Table A44

FB_Aw_Terms

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	12	5,0	5,9	5,9
	2	39	16,4	19,3	25,2
	3	53	22,3	26,2	51,5
	4	83	34,9	41,1	92,6
	5	15	6,3	7,4	100,0
	Total	202	84,9	100,0	
Missing		36	15,1		
Total		238	100,0		

Table A45

FB_Terms_Part

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	12	5,0	5,9	5,9
	2	40	16,8	19,8	25,7
	3	65	27,3	32,2	57,9
	4	73	30,7	36,1	94,1
	5	12	5,0	5,9	100,0
	Total	202	84,9	100,0	
Missing		36	15,1		
Total		238	100,0		

Table A46

More_Consc_use

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	14	5,9	6,9	6,9
	2	24	10,1	11,9	18,8
	3	83	34,9	41,1	59,9
	4	61	25,6	30,2	90,1
	5	20	8,4	9,9	100,0
	Total	202	84,9	100,0	
Missing		36	15,1		
Total		238	100,0		

Appendix B: Gender

Table B1

Ranks

	Gender	N	Mean Rank	Sum of Ranks
Concerned_privacy	0	122	106,74	13022,00
	1	115	132,01	15181,00
	Total	237		
FB_Concern_Info	0	99	90,54	8963,50
	1	102	111,15	11337,50
	Total	201		
FB_Friend_Unknwn	0	99	115,47	11432,00
	1	102	86,95	8869,00
	Total	201		
FB_Aware_Info	0	99	93,30	9237,00
	1	102	108,47	11064,00
	Total	201		
FB_Terms_Part	0	99	93,28	9234,50
	1	102	108,50	11066,50
	Total	201		

Table B2

Test Statistics[a]

	Achieve_risks	Reward_risks	Concerned_privacy	Important_protect
Mann-Whitney U	6756,500	6407,000	5519,000	6199,500
Asymp. Sig. (2-tailed)	,582	,218	,003	,091

	FB_Concern_Info	FB_Friend_Unknwn	FB_Aware_Info	FB_Terms_Part
Mann-Whitney U	4013,500	3616,000	4287,000	4284,500
Asymp. Sig. (2-tailed)	,009	,000	,046	,052

a. Grouping Variable: Gender

Table B3

Directional Measures

Goodman and Kruskal tau (Gender)		Value	Approx. Sig.
	SNS_how_long Dependent	,003	,697[a]
	Frequently_active Dependent	,001	,941[a]
	Number_friends_SNS Dependent	,004	,573[a]
	Freq_stsupdate Dependent	,005	,380[a]
	Nbr_apps Dependent	,009	,119[a]

a. Based on chi-square approximation

Table B4

Crosstab

			Gender		
			0	1	Total
FB_Name	0	Count	15	32	47
		% within Gender	15,2%	31,4%	23,4%
	1	Count	84	70	154
		% within Gender	84,8%	68,6%	76,6%
Total		Count	99	102	201
		% within Gender	100,0%	100,0%	100,0%

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	7,379	1	,007
N of Valid Cases	201		

Table B5

Crosstab

			Gender		
			0	1	Total
FB_IM	0	Count	62	82	144
		% within Gender	62,6%	80,4%	71,6%
	1	Count	37	20	57
		% within Gender	37,4%	19,6%	28,4%
Total		Count	99	102	201
		% within Gender	100,0%	100,0%	100,0%

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	7,805	1	,005
N of Valid Cases	201		

Table B6

Crosstab

			Gender		
			0	1	Total
FB_Phone	0	Count	81	93	174
		% within Gender	81,8%	91,2%	86,6%
	1	Count	18	9	27
		% within Gender	18,2%	8,8%	13,4%
Total		Count	99	102	201
		% within Gender	100,0%	100,0%	100,0%

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	3,784	1	,052
N of Valid Cases	201		

Table B7

Crosstab

			Gender		
			0	1	Total
FB_Relstatus	0	Count	33	50	83
		% within Gender	33,3%	49,0%	41,3%
	1	Count	66	52	118
		% within Gender	66,7%	51,0%	58,7%
Total		Count	99	102	201
		% within Gender	100,0%	100,0%	100,0%

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	5,099	1	,024
N of Valid Cases	201		

Table B8

Crosstab

			Gender		
			0	1	Total
FB_Sex_or	0	Count	43	74	117
		% within Gender	43,4%	72,5%	58,2%
	1	Count	56	28	84
		% within Gender	56,6%	27,5%	41,8%
Total		Count	99	102	201
		% within Gender	100,0%	100,0%	100,0%

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	17,506	1	,000
N of Valid Cases	201		

Table B9

Crosstab

			Gender		
			0	1	Total
FB_Interests	0	Count	25	47	72
		% within Gender	25,3%	46,1%	35,8%
	1	Count	74	55	129
		% within Gender	74,7%	53,9%	64,2%
Total		Count	99	102	201
		% within Gender	100,0%	100,0%	100,0%

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	9,478	1	,002
N of Valid Cases	201		

Table B10

Crosstab

			Gender		
			0	1	Total
FB_Relviews	0	Count	50	66	116
		% within Gender	50,5%	64,7%	57,7%
	1	Count	49	36	85
		% within Gender	49,5%	35,3%	42,3%
Total		Count	99	102	201
		% within Gender	100,0%	100,0%	100,0%

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	4,151	1	,042
N of Valid Cases	201		

Table B11

Directional Measures

			Value
Nominal by Interval	Eta	Sum_Info_Reveal Dependent	,260

Table B12

Crosstab

			Gender		
			0	1	Total
FB_Friend_Unknwn	1	Count	34	59	93
		% within Gender	34,3%	57,8%	46,3%
	2	Count	36	30	66
		% within Gender	36,4%	29,4%	32,8%
	3	Count	16	10	26
		% within Gender	16,2%	9,8%	12,9%
	4	Count	10	3	13
		% within Gender	10,1%	2,9%	6,5%
	5	Count	3	0	3
		% within Gender	3,0%	,0%	1,5%
Total		Count	99	102	201
		% within Gender	100,0%	100,0%	100,0%

Table B13

Crosstab

			Gender		
			0	1	Total
FB_Chg_Privsett	0	Count	13	13	26
		% within Gender	13,1%	12,7%	12,9%
	1	Count	86	89	175
		% within Gender	86,9%	87,3%	87,1%
Total		Count	99	102	201
		% within Gender	100,0%	100,0%	100,0%

Appendix C: Age

Table C1

Correlation

			Age
Spearman's Rho	Achieve_risks	Correlation Coefficient	,086
		Sig. (2-tailed)	,188
		N	237
	Reward_risks	Correlation Coefficient	,034
		Sig. (2-tailed)	,604
		N	237
	Concerned_privacy	Correlation Coefficient	,073
		Sig. (2-tailed)	,262
		N	237
	Frequently_active	Correlation Coefficient	-,227**
		Sig. (2-tailed)	,001
		N	208
	Number_friends_SNS	Correlation Coefficient	-,276**
		Sig. (2-tailed)	,000
		N	208
	Nbr_SNS	Correlation Coefficient	,156*
		Sig. (2-tailed)	,025
		N	208
	FB_Info_Wellprot	Correlation Coefficient	-,251**
		Sig. (2-tailed)	,000
		N	201
	FB_Terms_Part	Correlation Coefficient	,173*
		Sig. (2-tailed)	,014
		N	201

Pearson	Profile_SNS	Pearson Correlation	-,128*
		Sig. (2-tailed)	,049
		N	237
	Profile_LinkedIn	Pearson Correlation	,321**
		Sig. (2-tailed)	,000
		N	208
	FB_Birthday	Pearson Correlation	-,257**
		Sig. (2-tailed)	,000
		N	201
	FB_IM	Pearson Correlation	-,144*
		Sig. (2-tailed)	,042
		N	201
	FB_Sex_or	Pearson Correlation	-,157*
		Sig. (2-tailed)	,026
		N	201
	FB_Edu_Work	Pearson Correlation	-,202**
		Sig. (2-tailed)	,004
		N	201

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

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

Table C2

Ranks

	AgeGroup	N	Mean Rank
SNS_how_long	1	44	97,02
	2	63	121,33
	3	51	106,81
	4	50	87,51
	Total	208	
Frequently_active	1	44	109,58
	2	63	110,87
	3	51	122,02
	4	50	74,13
	Total	208	
Number_friends_SNS	1	44	115,05
	2	63	118,86
	3	51	115,09
	4	50	66,33
	Total	208	
Nbr_SNS	1	44	87,45
	2	63	103,23
	3	51	119,77
	4	50	105,52
	Total	208	

Test Statistics[a,b]

	SNS_how_long	Frequently_active	Number_friends_SNS	Nbr_SNS
Chi-Square	10,086	22,197	27,527	8,152
df	3	3	3	3
Asymp. Sig.	,018	,000	,000	,043

a. Kruskal Wallis Test

b. Grouping Variable: AgeGroup

Table C3

Ranks

	AgeGroup	N	Mean Rank	Sum of Ranks
Nbr_SNS	1	44	40,13	1765,50
	3	51	54,79	2794,50
	Total	95		

Test Statistics[a]

	Nbr_SNS
Mann-Whitney U	775,500
Asymp. Sig. (2-tailed)	,005

a. Grouping Variable: AgeGroup

Table C4

Ranks

	AgeGroup	N	Mean Rank	Sum of Ranks
Frequently_active	1	44	55,94	2461,50
	4	50	40,07	2003,50
	Total	94		
Frequently_active	2	63	66,10	4164,50
	4	50	45,53	2276,50
	Total	113		
Frequently_active	3	51	62,25	3174,50
	4	50	39,53	1976,50
	Total	101		

Test Statistics[a]

	Frequently_active (group 1 & 4)	Frequently_active (group 2 & 4)	Frequently_active (group 3 & 4)
Mann-Whitney U	728,500	1001,500	701,500
Asymp. Sig. (2-tailed)	,002	,000	,000

a. Grouping Variable: AgeGroup

Table C5

Ranks

	AgeGroup	N	Mean Rank	Sum of Ranks
Number_friends_SNS	1	44	59,10	2600,50
	4	50	37,29	1864,50
	Total	94		
Number_friends_SNS	2	63	70,13	4418,00
	4	50	40,46	2023,00
	Total	113		
Number_friends_SNS	3	51	62,20	3172,00
	4	50	39,58	1979,00
	Total	101		

Test Statistics[a]

	Number_friends_SNS (group1 & 4)	Number_friends_SNS (group 2 & 4)	Number_friends_SNS (group 3 & 4)
Mann-Whitney U	589,500	748,000	704,000
Asymp. Sig. (2-tailed)	,000	,000	,000

a. Grouping Variable: AgeGroup

Table C6

Ranks

	AgeGroup	N	Mean Rank	Sum of Ranks
SNS_how_long	1	44	46,55	2048,00
	2	63	59,21	3730,00
	Total	107		
SNS_how_long	2	63	64,66	4073,50
	4	50	47,35	2367,50
	Total	113		

Test Statistics[a]

	SNS_how_long (group 2 & 4)	SNS_how_long (group 2 & 1)
Mann-Whitney U	1092,500	1058,000
Asymp. Sig. (2-tailed)	,004	,033

a. Grouping Variable: AgeGroup

Table C7

Directional Measures

Goodman and Kruskal tau (AgeGroup)		Value	Approx. Sig.
	FB_Birthday Dependent	,055	,012[a]
	FB_IM Dependent	,067	,004[a]
	FB_Relviews Dependent	,040	,046[a]
	FB_Chg_Privsett Dependent	.065	,005[a]

a. Based on chi-square approximation

Table C8

Crosstab

			AgeGroup				
			1	2	3	4	Total
FB_Birthday	0	Count	6	14	8	19	47
		% within AgeGroup	14,3%	22,2%	16,3%	40,4%	23,4%
	1	Count	36	49	41	28	154
		% within AgeGroup	85,7%	77,8%	83,7%	59,6%	76,6%
Total		Count	42	63	49	47	201
		% within AgeGroup	100,0%	100,0%	100,0%	100,0%	100,0%

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	10,969	3	,012
N of Valid Cases	201		

Table C9

Crosstab

			AgeGroup				
			1	2	3	4	Total
FB_IM	0	Count	21	50	35	38	144
		% within AgeGroup	50,0%	79,4%	71,4%	80,9%	71,6%
	1	Count	21	13	14	9	57
		% within AgeGroup	50,0%	20,6%	28,6%	19,1%	28,4%
Total		Count	42	63	49	47	201
		% within AgeGroup	100,0%	100,0%	100,0%	100,0%	100,0%

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	13,495	3	,004
N of Valid Cases	201		

Table C10

Crosstab

			AgeGroup				
			1	2	3	4	Total
FB_Relviews	0	Count	20	32	36	28	116
		% within AgeGroup	47,6%	50,8%	73,5%	59,6%	57,7%
	1	Count	22	31	13	19	85
		% within AgeGroup	52,4%	49,2%	26,5%	40,4%	42,3%
Total		Count	42	63	49	47	201
		% within AgeGroup	100,0%	100,0%	100,0%	100,0%	100,0%

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	8,041	3	,045
N of Valid Cases	201		

Table C11

Directional Measures

			Value
Nominal by Interval	Eta	Sum_Info_Reveal Dependent	,235

Table C12

Ranks

	AgeGroup	N	Mean Rank
FB_Info_Wellprot	1	42	121,21
	2	63	106,09
	3	49	96,40
	4	47	80,91
	Total	201	

Test Statistics[a,b]

	FB_Info_Wellprot
Chi-Square	12,490
Df	3
Asymp. Sig.	,006

a. Kruskal Wallis Test

b. Grouping Variable: AgeGroup

Table C13

Ranks

	AgeGroup	N	Mean Rank	Sum of Ranks
FB_Info_Wellprot	1	42	51,87	2178,50
	3	49	40,97	2007,50
	Total	91		
FB_Info_Wellprot	1	42	54,68	2296,50
	4	47	36,35	1708,50
	Total	89		
FB_Info_Wellprot	2	63	61,40	3868,00
	4	47	47,60	2237,00
	Total	110		

Test Statistics[a]

	FB_Info_Wellprot (group 1 & 3)	FB_Info_Wellprot (group 1 & 4)	FB_Info_Wellprot (group 2 & 4)
Mann-Whitney U	782,500	580,500	1109,000
Asymp. Sig. (2-tailed)	,040	,000	,019

a. Grouping Variable: AgeGroup

Table C14

Crosstab

			AgeGroup				
			1	2	3	4	Total
FB_Chg_Privsett	0	Count	2	4	13	7	26
		% within AgeGroup	4,8%	6,3%	26,5%	14,9%	12,9%
	1	Count	40	59	36	40	175
		% within AgeGroup	95,2%	93,7%	73,5%	85,1%	87,1%
Total		Count	42	63	49	47	201
		% within AgeGroup	100,0%	100,0%	100,0%	100,0%	100,0%

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	13.120	3	.004
N of Valid Cases	201		

Appendix D: Geographical Background (Continent)

Table D1

Directional Measures

Goodman and Kruskal tau (ContinentGroup)		Value	Approx. Sig.
	Achieve_risks Dependent	,012	,575[a]
	Reward_risks Dependent	,009	,797[a]
	Concerned_privacy Dependent	,026	,028[a]
	SNS_how_long Dependent	,033	,005[a]
	Profile_Friendster Dependent	,233	,000[a]
	Profile_Hi5 Dependent	,116	,000[a]
	Profile_MySpace Dependent	,055	,013[a]
	Number_friends_SNS Dependent	,025	,047[a]
	Nbr_SNS Dependent	,062	,000[a]
	Freq_stsupdate Dependent	,029	,032[a]
	Nbr_apps Dependent	,044	,000[a]
	FB_Birthday Dependent	,045	,035[a]
	FB_Profpic Dependent	,105	,000[a]
	FB_Email Dependent	,051	,021[a]
	FB_Address Dependent	,060	,009[a]
	FB_IM Dependent	,066	,006[a]
	FB_Photo_yrslf Dependent	,108	,000[a]
	FB_Info_Wellprot Dependent	,034	,012[a]
	FB_Consc_privsett Dependent	,054	,000[a]
	FB_Friend_Unknwn Dependent	,030	,027[a]

a. Based on chi-square approximation

Table D2

Ranks

	ContinentGroup	N	Mean Rank
Concerned_privacy	1	55	137,72
	2	90	100,40
	3	52	104,68
	4	29	124,03
	Total	226	
SNS_how_long	1	50	120,83
	2	80	92,36
	3	41	106,05
	4	28	75,79
	Total	199	
Frequently_active	1	50	113,65
	2	80	91,53
	3	41	92,94
	4	28	110,18
	Total	199	
Number_friends_SNS	1	50	125,72
	2	80	86,46
	3	41	98,29
	4	28	95,27
	Total	199	
Nbr_SNS	1	50	124,38
	2	80	78,86
	3	41	107,44
	4	28	105,96
	Total	199	
Freq_stsupdate	1	50	113,89
	2	78	91,60
	3	37	95,89

	4	27	79,30
	Total	192	

Test Statistics[a,b]

	Concerned_privacy	SNS_how_long	Number_friends_SNS	Nbr_SNS	Freq_stsupdate
Chi-Square	14,267	13,936	15,130	24,636	8,885
df	3	3	3	3	3
Asymp. Sig.	,003	,003	,002	,000	,031

a. Kruskal Wallis Test

b. Grouping Variable: ContinentGroup

Table D3

Ranks

	ContinentGroup	N	Mean Rank	Sum of Ranks
Concerned_privacy	1	55	87,93	4836,00
	2	90	63,88	5749,00
	Total	145		
Concerned_privacy	1	55	61,66	3391,50
	3	52	45,89	2386,50
	Total	107		

Test Statistics[a]

	Concerned_privacy (group 1 & 2)	Concerned_privacy (group 1 & 3)
Mann-Whitney U	1654,000	1008,500
Asymp. Sig. (2-tailed)	,000	,005

a. Grouping Variable: ContinentGroup

Table D4

Ranks

	ContinentGroup	N	Mean Rank	Sum of Ranks
SNS_how_long	1	50	76,78	3839,00
	2	80	58,45	4676,00
	Total	130		
SNS_how_long	1	50	45,68	2284,00
	4	28	28,46	797,00
	Total	78		

Test Statistics[a]

	SNS_how_long (group 1 & 2)	SNS_how_long (group 1 & 4)
Mann-Whitney U	1436,000	391,000
Asymp. Sig. (2-tailed)	,006	,001

a. Grouping Variable: ContinentGroup

Table D5

Ranks

	ContinentGroup	N	Mean Rank	Sum of Ranks
Nbr_SNS	1	50	83,55	4177,50
	2	80	54,22	4337,50
	Total	130		
Nbr_SNS	2	80	54,76	4380,50
	3	41	73,18	3000,50
	Total	121		
Nbr_SNS	2	80	50,89	4071,00
	4	28	64,82	1815,00
	Total	108		

Test Statistics[a]

	Nbr_SNS (group 1 & 2)	Nbr_SNS (group 2 & 3)	Nbr_SNS (group 2 & 4)
Mann-Whitney U	1097,500	1140,500	831,000
Asymp. Sig. (2-tailed)	,000	,002	,021

a. Grouping Variable: ContinentGroup

Table D6

Ranks

	ContinentGroup	N	Mean Rank	Sum of Ranks
Number_friends_SNS	1	50	82,11	4105,50
	2	80	55,12	4409,50
	Total	130		
Number_friends_SNS	1	50	51,19	2559,50
	3	41	39,67	1626,50
	Total	91		
Number_friends_SNS	1	50	43,42	2171,00
	4	28	32,50	910,00
	Total	78		

Test Statistics[a]

	Number_friends_SNS (group 1 & 2)	Number_friends_SNS (group 1 & 3)	Number_friends_SNS (group 1 & 4)
Mann-Whitney U	1169,500	765,500	504,000
Asymp. Sig. (2-tailed)	,000	,036	,039

a. Grouping Variable: ContinentGroup

Table D7

Ranks

	ContinentGroup	N	Mean Rank	Sum of Ranks
Freq_stsupdate	1	50	73,68	3684,00
	2	78	58,62	4572,00
	Total	128		
Freq_stsupdate	1	50	43,44	2172,00
	4	27	30,78	831,00
	Total	77		

Test Statistics[a]

	Freq_stsupdate (group 1 & 2)	Freq_stsupdate (group 1 & 4)
Mann-Whitney U	1491,000	453,000
Asymp. Sig. (2-tailed)	,018	,012

a. Grouping Variable: ContinentGroup

Table D8

Ranks

	ContinentGroup	N	Mean Rank
Nbr_apps	1	50	122,83
	2	78	87,49
	3	37	93,62
	4	27	77,70
	Total	192	
FB_Concern_Info	1	50	109,04
	2	78	94,64
	3	37	76,24
	4	27	106,41
	Total	192	

FB_Info_Wellprot	1	50	115,86
	2	78	82,42
	3	37	103,89
	4	27	91,19
	Total	192	
FB_Aware_privsett	1	50	92,09
	2	78	95,69
	3	37	116,28
	4	27	79,91
	Total	192	
FB_Consc_privsett	1	50	87,02
	2	78	104,43
	3	37	112,72
	4	27	68,93
	Total	192	
FB_Friend_Unknwn	1	50	110,58
	2	78	85,74
	3	37	85,07
	4	27	117,17
	Total	192	
FB_Aware_Info	1	50	91,26
	2	78	101,49
	3	37	112,18
	4	27	70,31
	Total	192	
FB_Apps_Harmful	1	50	119,09
	2	78	87,40
	3	37	79,89
	4	27	103,70
	Total	192	

Test Statistics[a,b]

	Nbr_apps	FB_Info_Wellprot	FB_Consc_privsett	FB_Friend_Unknwn
Chi-Square	18,853	13,034	14,838	13,229
Df	3	3	3	3
Asymp. Sig.	,000	,005	,002	,004

a. Kruskal Wallis Test

b. Grouping Variable: ContinentGroup

Table D9

Crosstab

			ContinentGroup				
			1	2	3	4	Total
FB_Apps_Harmful	1	Count	5	16	11	3	35
		% within ContinentGroup	10,0%	20,5%	29,7%	11,1%	18,2%
	2	Count	13	32	14	10	69
		% within ContinentGroup	26,0%	41,0%	37,8%	37,0%	35,9%
	3	Count	17	24	8	10	59
		% within ContinentGroup	34,0%	30,8%	21,6%	37,0%	30,7%
	4	Count	13	5	4	4	26
		% within ContinentGroup	26,0%	6,4%	10,8%	14,8%	13,5%
	5	Count	2	1	0	0	3
		% within ContinentGroup	4,0%	1,3%	,0%	,0%	1,6%
Total		Count	50	78	37	27	192
		% within ContinentGroup	100,0%	100,0%	100,0%	100,0%	100,0%

Table D10

Crosstab

			ContinentGroup				Total
			1	2	3	4	
FB_Birthday	0	Count	5	22	9	10	46
		% within ContinentGroup	10,0%	28,2%	24,3%	37,0%	24,0%
	1	Count	45	56	28	17	146
		% within ContinentGroup	90,0%	71,8%	75,7%	63,0%	76,0%
Total		Count	50	78	37	27	192
		% within ContinentGroup	100,0%	100,0%	100,0%	100,0%	100,0%

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	8,657	3	,034
N of Valid Cases	192		

Table D11

Crosstab

			ContinentGroup				Total
			1	2	3	4	
FB_Profpic	0	Count	6	13	3	13	35
		% within ContinentGroup	12,0%	16,7%	8,1%	48,1%	18,2%
	1	Count	44	65	34	14	157
		% within ContinentGroup	88,0%	83,3%	91,9%	51,9%	81,8%
Total		Count	50	78	37	27	192
		% within ContinentGroup	100,0%	100,0%	100,0%	100,0%	100,0%

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	20,186	3	,000
N of Valid Cases	192		

Table D12

Crosstab

			ContinentGroup				
			1	2	3	4	Total
FB_Photo_yrslf	0	Count	7	16	3	14	40
		% within ContinentGroup	14,0%	20,5%	8,1%	51,9%	20,8%
	1	Count	43	62	34	13	152
		% within ContinentGroup	86,0%	79,5%	91,9%	48,1%	79,2%
Total		Count	50	78	37	27	192
		% within ContinentGroup	100,0%	100,0%	100,0%	100,0%	100,0%

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	20,804	3	,000
N of Valid Cases	192		

Table D13

Crosstab

			ContinentGroup				
			1	2	3	4	Total
FB_Email	0	Count	10	30	15	4	59
		% within ContinentGroup	20,0%	38,5%	40,5%	14,8%	30,7%
	1	Count	40	48	22	23	133
		% within ContinentGroup	80,0%	61,5%	59,5%	85,2%	69,3%
Total		Count	50	78	37	27	192
		% within ContinentGroup	100,0%	100,0%	100,0%	100,0%	100,0%

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	9,781	3	,021
N of Valid Cases	192		

Table D14

Crosstab

			ContinentGroup				
			1	2	3	4	Total
FB_Address	0	Count	41	77	33	25	176
		% within ContinentGroup	82,0%	98,7%	89,2%	92,6%	91,7%
	1	Count	9	1	4	2	16
		% within ContinentGroup	18,0%	1,3%	10,8%	7,4%	8,3%
Total		Count	50	78	37	27	192
		% within ContinentGroup	100,0%	100,0%	100,0%	100,0%	100,0%

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	11,521	3	,009
N of Valid Cases	192		

Table D15

Crosstab

			ContinentGroup				Total
			1	2	3	4	
FB_IM	0	Count	32	66	21	21	140
		% within ContinentGroup	64,0%	84,6%	56,8%	77,8%	72,9%
	1	Count	18	12	16	6	52
		% within ContinentGroup	36,0%	15,4%	43,2%	22,2%	27,1%
Total		Count	50	78	37	27	192
		% within ContinentGroup	100,0%	100,0%	100,0%	100,0%	100,0%

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	12,634	3	,005
N of Valid Cases	192		

Table D16

Directional Measures

			Value
Nominal by Interval	Eta	Sum_Info_Reveal Dependent	,261

Table D17

Ranks

	ContinentGroup	N	Mean Rank	Sum of Ranks
FB_Info_Wellprot	1	50	78,01	3900,50
	2	78	55,84	4355,50
	Total	128		
FB_Info_Wellprot	2	78	53,74	4192,00
	3	37	66,97	2478,00
	Total	115		

Test Statistics[a]

	FB_Info_Wellprot (group 1 & 2)	FB_Info_Wellprot (group 2 & 3)
Mann-Whitney U	1274,500	1111,000
Asymp. Sig. (2-tailed)	,001	,038

a. Grouping Variable: ContinentGroup

Table D18

Crosstab

			ContinentGroup				
			1	2	3	4	Total
FB_Info_Wellprot	1	Count	1	11	2	4	18
		% within ContinentGroup	2,0%	14,1%	5,4%	14,8%	9,4%
	2	Count	8	30	8	7	53
		% within ContinentGroup	16,0%	38,5%	21,6%	25,9%	27,6%
	3	Count	22	19	16	9	66
		% within ContinentGroup	44,0%	24,4%	43,2%	33,3%	34,4%
	4	Count	18	16	11	6	51
		% within ContinentGroup	36,0%	20,5%	29,7%	22,2%	26,6%
	5	Count	1	2	0	1	4
		% within ContinentGroup	2,0%	2,6%	,0%	3,7%	2,1%
Total		Count	50	78	37	27	192
		% within ContinentGroup	100,0%	100,0%	100,0%	100,0%	100,0%

Table D19

Crosstab

			ContinentGroup				Total
			1	2	3	4	
FB_Consc_privsett	1	Count	0	1	0	1	2
		% within ContinentGroup	,0%	1,3%	,0%	3,7%	1,0%
	2	Count	1	2	1	4	8
		% within ContinentGroup	2,0%	2,6%	2,7%	14,8%	4,2%
	3	Count	9	6	6	7	28
		% within ContinentGroup	18,0%	7,7%	16,2%	25,9%	14,6%
	4	Count	28	37	9	9	83
		% within ContinentGroup	56,0%	47,4%	24,3%	33,3%	43,2%
	5	Count	12	32	21	6	71
		% within ContinentGroup	24,0%	41,0%	56,8%	22,2%	37,0%
Total		Count	50	78	37	27	192
		% within ContinentGroup	100,0%	100,0%	100,0%	100,0%	100,0%

Table D20

Crosstab

			ContinentGroup				Total
			1	2	3	4	
FB_Chg_Privsett	0	Count	8	8	4	6	26
		% within ContinentGroup	16,0%	10,3%	10,8%	22,2%	13,5%
	1	Count	42	70	33	21	166
		% within ContinentGroup	84,0%	89,7%	89,2%	77,8%	86,5%
Total		Count	50	78	37	27	192
		% within ContinentGroup	100,0%	100,0%	100,0%	100,0%	100,0%

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	2,951	3	,399
N of Valid Cases	192		

Table D21

Crosstab

			ContinentGroup				Total
			1	2	3	4	
FB_Friend_Unknwn	1	Count	16	43	21	9	89
		% within ContinentGroup	32,0%	55,1%	56,8%	33,3%	46,4%
	2	Count	20	24	11	7	62
		% within ContinentGroup	40,0%	30,8%	29,7%	25,9%	32,3%
	3	Count	9	8	2	6	25
		% within ContinentGroup	18,0%	10,3%	5,4%	22,2%	13,0%
	4	Count	4	3	3	3	13
		% within ContinentGroup	8,0%	3,8%	8,1%	11,1%	6,8%
	5	Count	1	0	0	2	3
		% within ContinentGroup	2,0%	,0%	,0%	7,4%	1,6%
Total		Count	50	78	37	27	192
		% within ContinentGroup	100,0%	100,0%	100,0%	100,0%	100,0%

Table D22

Ranks

	ContinentGroup	N	Mean Rank	Sum of Ranks
FB_Friend_Unknwn	1	50	74,84	3742,00
	2	78	57,87	4514,00
	Total	128		
FB_Friend_Unknwn	1	50	48,98	2449,00
	3	37	37,27	1379,00
	Total	87		
FB_Friend_Unknwn	2	78	48,68	3797,00
	4	27	65,48	1768,00
	Total	105		
FB_Friend_Unknwn	3	37	28,20	1043,50
	4	27	38,39	1036,50
	Total	64		

Test Statistics[a]

	FB_Friend_Unknwn (group 1 & 2)	FB_Friend_Unknwn (group 1 & 3)	FB_Friend_Unknwn (group 2 & 4)	FB_Friend_Unknwn (group 3 & 4)
Mann-Whitney U	1433,000	676,000	716,000	340,500
Asymp. Sig. (2-tailed)	,006	,022	,007	,021

a. Grouping Variable: ContinentGroup

Appendix E : Correlations and Constructs

Table E1

Correlations

			Achieve_risks	Reward_risks	Important_protect	Concerned_privacy	Information_protected	SNS_how_long	Frequently_active	Number_friends_SNS	Freq_stsupdate	Nbr_apps	FB_Concern_Info	FB_Info_Wellprot	FB_Aware_privsett	FB_Consc_privsett	FB_Friend_Unknwn	FB_Aware_Info	FB_Apps_Harmful	FB_Aw_Terms	FB_Terms_Part	More_Consc_use	Nbr_SNS
Spearman's rho	Achieve_risks	Correlation Coefficient	1 000	,429**	,059	,182**	,062	,201**	,093	,107	,023	,102	,086	,049	,147*	,148*	-,084	,242**	-,040	,163*	,063	-,025	,102
		Sig. (2-tailed)	.	,000	,408	,010	,381	,004	,190	,130	,750	,149	,227	,489	,038	,036	,236	,001	,574	,020	,378	,729	,149
		N	201	201	201	201	201	201	201	201	201	201	201	201	201	201	201	201	201	201	201	201	201
	Reward_risks	Correlation Coefficient	,429**	1 000	,069	-,013	,008	,139*	,282**	,206**	,100	-,013	,081	,032	,073	,107	-,032	,094	-,050	-,030	,008	-,066	,049
		Sig. (2-tailed)	,000	.	,333	,860	,908	,049	,000	,003	,158	,851	,253	,656	,303	,130	,654	,187	,484	,672	,910	,350	,490
		N	201	201	201	201	201	201	201	201	201	201	201	201	201	201	201	201	201	201	201	201	201
	Important_protect	Correlation Coefficient	,059	,069	1 000	,418**	,129	-,026	,025	-,023	-,164*	-,116	,248**	,091	,070	,065	-,152*	,059	-,180*	-,026	,189**	,104	,005
		Sig. (2-tailed)	,408	,333	.	,000	,068	,714	,723	,750	,020	,101	,000	,199	,325	,357	,031	,402	,011	,716	,007	,142	,948
		N	201	201	201	201	201	201	201	201	201	201	201	201	201	201	201	201	201	201	201	201	201
	Concerned_privacy	Correlation Coefficient	,182**	-,013	,418**	1 000	-,095	-,116	-,001	-,034	-,053	-,021	,396**	-,041	,079	,005	-,090	,048	-,110	,080	,259**	,242**	,096
		Sig. (2-tailed)	,010	,860	,000	.	,181	,100	,988	,629	,456	,772	,000	,566	,268	,948	,205	,497	,122	,260	,000	,001	,174
		N	201	201	201	201	201	201	201	201	201	201	201	201	201	201	201	201	201	201	201	201	201
	Information_protected	Correlation Coefficient	,062	,008	,129	-,095	1 000	,017	-,057	-,025	,006	,064	-,223**	,416**	,125	,097	-,041	,046	,115	,148*	,064	,040	-,030
		Sig. (2-tailed)	,381	,908	,068	,181	.	,805	,424	,721	,937	,363	,001	,000	,076	,171	,562	,520	,103	,036	,368	,570	,673
		N	201	201	201	201	201	201	201	201	201	201	201	201	201	201	201	201	201	201	201	201	201
	SNS_how_long	Correlation Coefficient	,201**	,139*	-,026	-,116	,017	1 000	,205**	,473**	,135	,159*	-,110	,114	,169*	,091	-,002	,063	-,040	,079	,104	-,021	,323**
		Sig. (2-tailed)	,004	,049	,714	,100	,805	.	,003	,000	,055	,023	,118	,105	,016	,197	,982	,371	,568	,263	,142	,768	,000
		N	201	201	201	201	201	202	202	202	202	202	202	202	202	202	202	202	202	202	202	202	202
	Frequently_active	Correlation Coefficient	,093	,282**	,025	-,001	-,057	,205**	1 000	,368**	,316**	,196**	-,031	,115	,040	-,038	,095	,043	,013	-,128	-,094	,082	,216**
		Sig. (2-tailed)	,190	,000	,723	,988	,424	,003	.	,000	,000	,005	,658	,103	,572	,591	,180	,543	,854	,070	,185	,246	,002
		N	201	201	201	201	201	202	202	202	202	202	202	202	202	202	202	202	202	202	202	202	202
	Number_friends_SNS	Correlation Coefficient	,107	,206**	-,023	-,034	-,025	,473**	,368**	1 000	,316**	,189**	-,063	,186**	,046	,043	,099	,005	-,038	-,026	-,005	,010	,327**
		Sig. (2-tailed)	,130	,003	,750	,629	,721	,000	,000	.	,000	,007	,377	,008	,513	,542	,161	,949	,587	,709	,944	,892	,000
		N	201	201	201	201	201	202	202	202	202	202	202	202	202	202	202	202	202	202	202	202	202
	Freq_stsupdate	Correlation Coefficient	,023	,100	-,164*	-,053	,006	,135	,316**	,316**	1 000	,289**	-,083	,130	,029	-,011	,178*	,066	-,024	,073	-,025	-,023	,143*
		Sig. (2-tailed)	,750	,158	,020	,456	,937	,055	,000	,000	.	,000	,241	,064	,680	,878	,011	,350	,731	,303	,726	,742	,042
		N	201	201	201	201	201	202	202	202	202	202	202	202	202	202	202	202	202	202	202	202	202
	Nbr_apps	Correlation Coefficient	,102	-,013	-,116	-,021	,064	,159*	,196**	,189**	,289**	1 000	,046	,125	,159*	,114	,160*	,186**	,220**	,093	,025	-,021	,136
		Sig. (2-tailed)	,149	,851	,101	,772	,363	,023	,005	,007	,000	.	,519	,075	,023	,107	,023	,008	,002	,189	,726	,762	,053
		N	201	201	201	201	201	202	202	202	202	202	202	202	202	202	202	202	202	202	202	202	202

		Achiev e_risks	Reward _risks	Important _protect	Concerne d_privacy	Information _protected	SNS_ho w_long	Frequentl y_active	Number_fri ends_SNS	Freq_st supdate	Nbr_a pps	FB_Conc ern_Info	FB_Info_ Wellprot	FB_Aware _privsett	FB_Consc _privsett	FB_Friend _Unknwn	FB_Awa re_Info	FB_Apps _Harmful	FB_Aw _Terms	FB_Ter ms_Part	More_Co nsc_use	Nbr_S NS
FB_Concern_I nfo	Correlation Coefficient	,086	,081	,248**	,396**	-,223**	-,110	-,031	-,063	-,083	,046	1 000	-,263**	,092	,120	-,096	,067	-,195**	,072	,221**	-,047	-,001
	Sig. (2-tailed)	,227	,253	,000	,000	,001	,118	,658	,377	,241	,519	.	,000	,192	,090	,172	,340	,006	,308	,002	,505	,991
	N	201	201	201	201	201	202	202	202	202	202	202	202	202	202	202	202	202	202	202	202	202
FB_Info_Wellp rot	Correlation Coefficient	,049	,032	,091	-,041	,416**	,114	,115	,186**	,130	,125	-,263**	1 000	,155*	,104	,048	,106	,234**	,155*	,009	-,006	,064
	Sig. (2-tailed)	,489	,656	,199	,566	,000	,105	,103	,008	,064	,075	,000	.	,028	,142	,495	,134	,001	,028	,904	,927	,362
	N	201	201	201	201	201	202	202	202	202	202	202	202	202	202	202	202	202	202	202	202	202
FB_Aware_pri vsett	Correlation Coefficient	,147*	,073	,070	,079	,125	,169*	,040	,046	,029	,159*	,092	,155*	1 000	,531**	-,203**	,432**	-,029	,313**	,097	-,037	,116
	Sig. (2-tailed)	,038	,303	,325	,268	,076	,016	,572	,513	,680	,023	,192	,028	.	,000	,004	,000	,686	,000	,170	,600	,101
	N	201	201	201	201	201	202	202	202	202	202	202	202	202	202	202	202	202	202	202	202	202
FB_Consc_pri vsett	Correlation Coefficient	,148*	,107	,065	,005	,097	,091	-,038	,043	-,011	,114	,120	,104	,531**	1 000	-,200**	,497**	-,237**	,198**	,174*	-,197**	,058
	Sig. (2-tailed)	,036	,130	,357	,948	,171	,197	,591	,542	,878	,107	,090	,142	,000	.	,004	,000	,001	,005	,013	,005	,410
	N	201	201	201	201	201	202	202	202	202	202	202	202	202	202	202	202	202	202	202	202	202
FB_Friend_Un knwn	Correlation Coefficient	-,084	-,032	-,152*	-,090	-,041	-,002	,095	,099	,178*	,160*	-,096	,048	-,203**	-,200**	1 000	-,317**	,308**	-,046	-,033	,143*	,204**
	Sig. (2-tailed)	,236	,654	,031	,205	,562	,982	,180	,161	,011	,023	,172	,495	,004	,004	.	,000	,000	,516	,637	,042	,004
	N	201	201	201	201	201	202	202	202	202	202	202	202	202	202	202	202	202	202	202	202	202
FB_Aware_Inf o	Correlation Coefficient	,242**	,094	,059	,048	,046	,063	,043	,005	,066	,186**	,067	,106	,432**	,497**	-,317**	1 000	-,171*	,269**	,196**	-,033	-,029
	Sig. (2-tailed)	,001	,187	,402	,497	,520	,371	,543	,949	,350	,008	,340	,134	,000	,000	,000	.	,015	,000	,005	,641	,685
	N	201	201	201	201	201	202	202	202	202	202	202	202	202	202	202	202	202	202	202	202	202
FB_Apps_Har mful	Correlation Coefficient	-,040	-,050	-,180*	-,110	,115	-,040	,013	-,038	-,024	,220**	-,195**	,234**	-,029	-,237**	,308**	-,171*	1 000	-,003	-,143*	,135	,040
	Sig. (2-tailed)	,574	,484	,011	,122	,103	,568	,854	,587	,731	,002	,006	,001	,686	,001	,000	,015	.	,969	,043	,056	,572
	N	201	201	201	201	201	202	202	202	202	202	202	202	202	202	202	202	202	202	202	202	202
FB_Aw_Terms	Correlation Coefficient	,163*	-,030	-,026	,080	,148*	,079	-,128	-,026	,073	,093	,072	,155*	,313**	,198**	-,046	,269**	-,003	1 000	,398**	-,126	-,020
	Sig. (2-tailed)	,020	,672	,716	,260	,036	,263	,070	,709	,303	,189	,308	,028	,000	,005	,516	,000	,969	.	,000	,075	,773
	N	201	201	201	201	201	202	202	202	202	202	202	202	202	202	202	202	202	202	202	202	202
FB_Terms_Pa rt	Correlation Coefficient	,063	,008	,189**	,259**	,064	,104	-,094	-,005	-,025	,025	,221**	,009	,097	,174*	-,033	,196**	-,143*	,398**	1 000	,054	,138
	Sig. (2-tailed)	,378	,910	,007	,000	,368	,142	,185	,944	,726	,726	,002	,904	,170	,013	,637	,005	,043	,000	.	,446	,051
	N	201	201	201	201	201	202	202	202	202	202	202	202	202	202	202	202	202	202	202	202	202
More_Consc_ use	Correlation Coefficient	-,025	-,066	,104	,242**	,040	-,021	,082	,010	-,023	-,021	-,047	-,006	-,037	-,197**	,143*	-,033	,135	-,126	,054	1 000	-,035
	Sig. (2-tailed)	,729	,350	,142	,001	,570	,768	,246	,892	,742	,762	,505	,927	,600	,005	,042	,641	,056	,075	,446	.	,622
	N	201	201	201	201	201	202	202	202	202	202	202	202	202	202	202	202	202	202	202	202	202
Nbr_SNS	Correlation Coefficient	,102	,049	,005	,096	-,030	,323**	,216**	,327**	,143*	,136	-,001	,064	,116	,058	,204**	-,029	,040	-,020	,138	-,035	1 000
	Sig. (2-tailed)	,149	,490	,948	,174	,673	,000	,002	,000	,042	,053	,991	,362	,101	,410	,004	,685	,572	,773	,051	,622	.
	N	201	201	201	201	201	202	202	202	202	202	202	202	202	202	202	202	202	202	202	202	202

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

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

Table E2: Construct Awareness

Case Processing Summary

		N	%
Cases	Valid	202	100,0
	Excluded[a]	0	,0
	Total	202	100,0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
,719	5

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
FB_Aware_privsett	14,55	7,423	,528	,654
FB_Consc_privsett	14,34	7,627	,483	,671
FB_Aware_Info	14,43	6,922	,543	,644
FB_Aw_Terms	15,20	6,969	,474	,674
FB_Terms_Part	15,29	7,559	,377	,713

Table E3: Construct Activity

Case Processing Summary

		N	%
Cases	Valid	202	100,0
	Excluded[a]	0	,0
	Total	202	100,0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
,645	5

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
Freq_stsupdate	10,7772	13,547	,297	,635
Frequently_active	9,4703	13,992	,446	,598
SNS_how_long	9,8911	9,799	,457	,568
Number_friends_SNS	10,1584	8,154	,570	,497
Nbr_SNS	11,1089	14,406	,377	,618

Appendix F: Linear Regression

Table F1

Variables Entered/Removed[b]

Model	Variables Entered	Variables Removed	Method
1	Age, Gender[a]	.	Enter

a. All requested variables entered.

b. Dependent Variable: Sum_Info_Reveal

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	,340[a]	,116	,107	2,697

a. Predictors: (Constant), Age, Gender

ANOVA[b]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	188,763	2	94,381	12,977	,000[a]
	Residual	1440,053	198	7,273		
	Total	1628,816	200			

a. Predictors: (Constant), Age, Gender

b. Dependent Variable: Sum_Info_Reveal

Table F2

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	10,693	,689		15,520	,000
	Gender	-1,421	,381	-,250	-3,731	,000
	Age	-,079	,024	-,220	-3,294	,001

a. Dependent Variable: Sum_Info_Reveal

Table F3

Test for heteroskedasticity pertaining to the regression in Table F1 and F2

White's test for heteroskedasticity
OLS, using observations 1-201
Dependent variable: uhat^2

	coefficient	std. error	t-ratio	p-value
const	−6.67073	6.53891	−1.020	0.3089
Age	0.826144	0.423411	1.951	0.0525*
Gender	4.33133	4.55767	0.9503	0.3431
sq_Age	−0.00942402	0.00655940	−1.437	0.1524
X2_X3	−0.226493	0.163370	−1.386	0.1672

Unadjusted R-squared = 0.039144

Test statistic: TR^2 = 7.867897,
with p-value = P(Chi-square(4) > 7.867897) = 0.096539

Table F4

Variables Entered/Removed[b]

Model	Variables Entered	Variables Removed	Method
1	constr_act[a]	.	Enter

a. All requested variables entered.

b. Dependent Variable: Sum_Info_Reveal

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	,458[a]	,210	,206	2,538

a. Predictors: (Constant), constr_act

ANOVA[b]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	341,835	1	341,835	53,068	,000[a]
	Residual	1288,284	200	6,441		
	Total	1630,119	201			

a. Predictors: (Constant), constr_act

b. Dependent Variable: Sum_Info_Reveal

Table F5

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	3,819	,583		6,552	,000
	constr_act	,315	,043	,458	7,285	,000

a. Dependent Variable: Sum_Info_Reveal

Table F6

Test for heteroskedasticity pertaining to the regression in Table F4 and F5

White's test for heteroskedasticity
OLS, using observations 1-201
Dependent variable: uhat^2

	coefficient	std. error	t-ratio	p-value
const	2.06427	4.06854	0.5074	0.6125
constr_act	0.844378	0.687739	1.228	0.2210
sq_constr_act	−0.0357230	0.0277789	−1.286	0.2000

Unadjusted R-squared = 0.008388

Test statistic: TR^2 = 1.686026,
with p-value = P(Chi-square(2) > 1.686026) = 0.430412

Table F7

Variables Entered/Removed[b]

Model	Variables Entered	Variables Removed	Method
1	Gender, constr_act, Age[a]	.	Enter

a. All requested variables entered.

b. Dependent Variable: Sum_Info_Reveal

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	,545[a]	,297	,286	2,412

a. Predictors: (Constant), Gender, constr_act, Age

ANOVA[b]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	483,037	3	161,012	27,684	,000[a]
	Residual	1145,779	197	5,816		
	Total	1628,816	200			

a. Predictors: (Constant), Gender, constr_act, Age

b. Dependent Variable: Sum_Info_Reveal

Table F8

Coefficients[a]

		Unstandardized Coefficients		Standardized Coefficients		
Model		B	Std. Error	Beta	t	Sig.
1	(Constant)	5,962	,907		6,575	,000
	constr_act	,300	,042	,436	7,113	,000
	Age	-,045	,022	-,125	-2,034	,043
	Gender	-1,498	,341	-,263	-4,397	,000

a. Dependent Variable: Sum_Info_Reveal

Table F9

Test for heteroskedasticity pertaining to the regression in Table F7 and F8

White's test for heteroskedasticity
OLS, using observations 1-201
Dependent variable: uhat^2

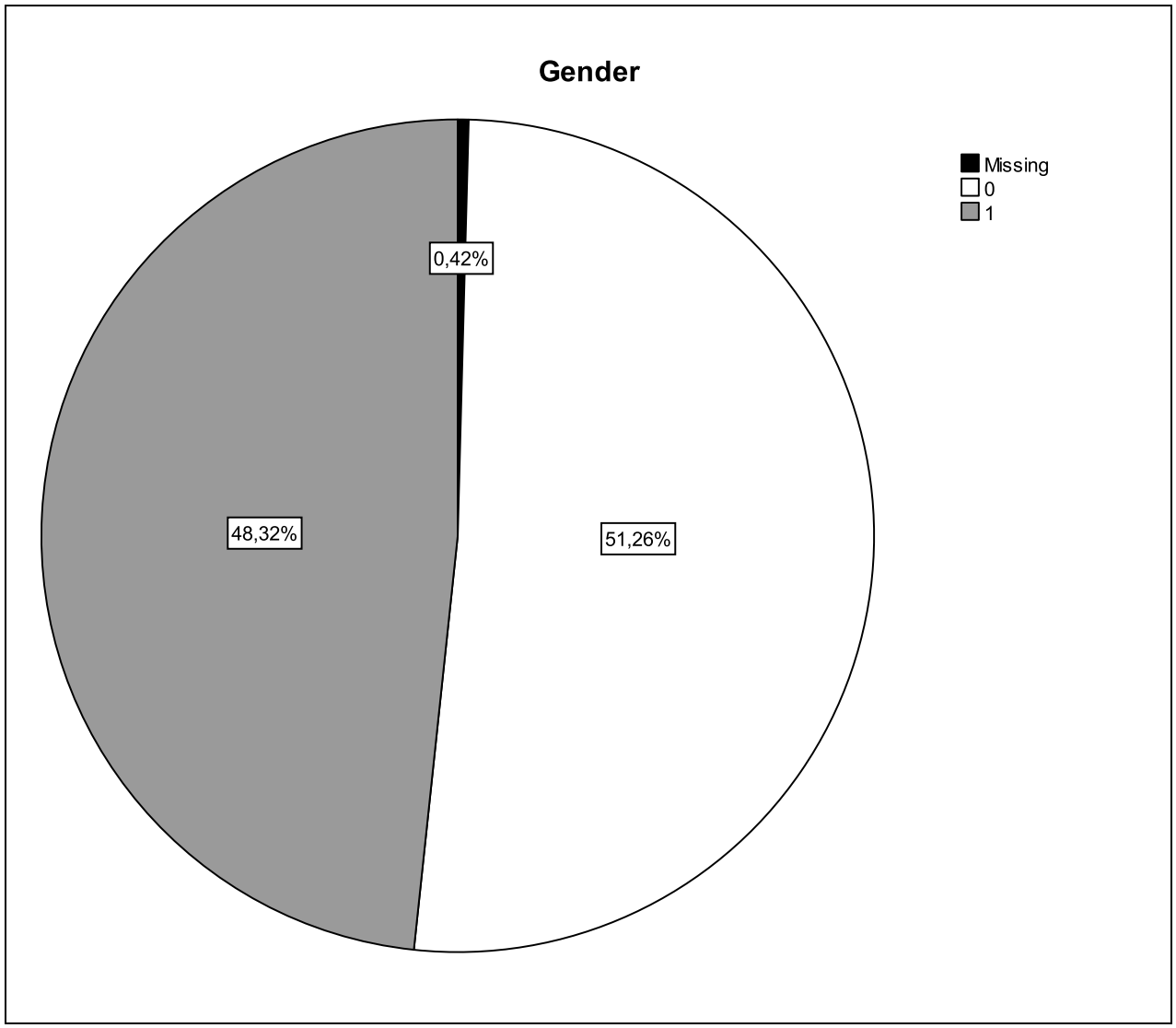
	coefficient	std. error	t-ratio	p-value
const	−0.102869	9.30162	−0.01106	0.9912
constr_act	0.664753	0.911373	0.7294	0.4666
Age	0.0697733	0.381466	0.1829	0.8551
Gender	0.173984	5.72352	0.03040	0.9758
sq_constr_act	−0.0378720	0.0265115	−1.429	0.1548
X2_X3	0.00483081	0.0160141	0.3017	0.7632
X2_X4	0.139541	0.266032	0.5245	0.6005
sq_Age	0.00145474	0.00548822	0.2651	0.7912
X3_X4	−0.106160	0.141040	−0.7527	0.4526

Unadjusted R-squared = 0.047646

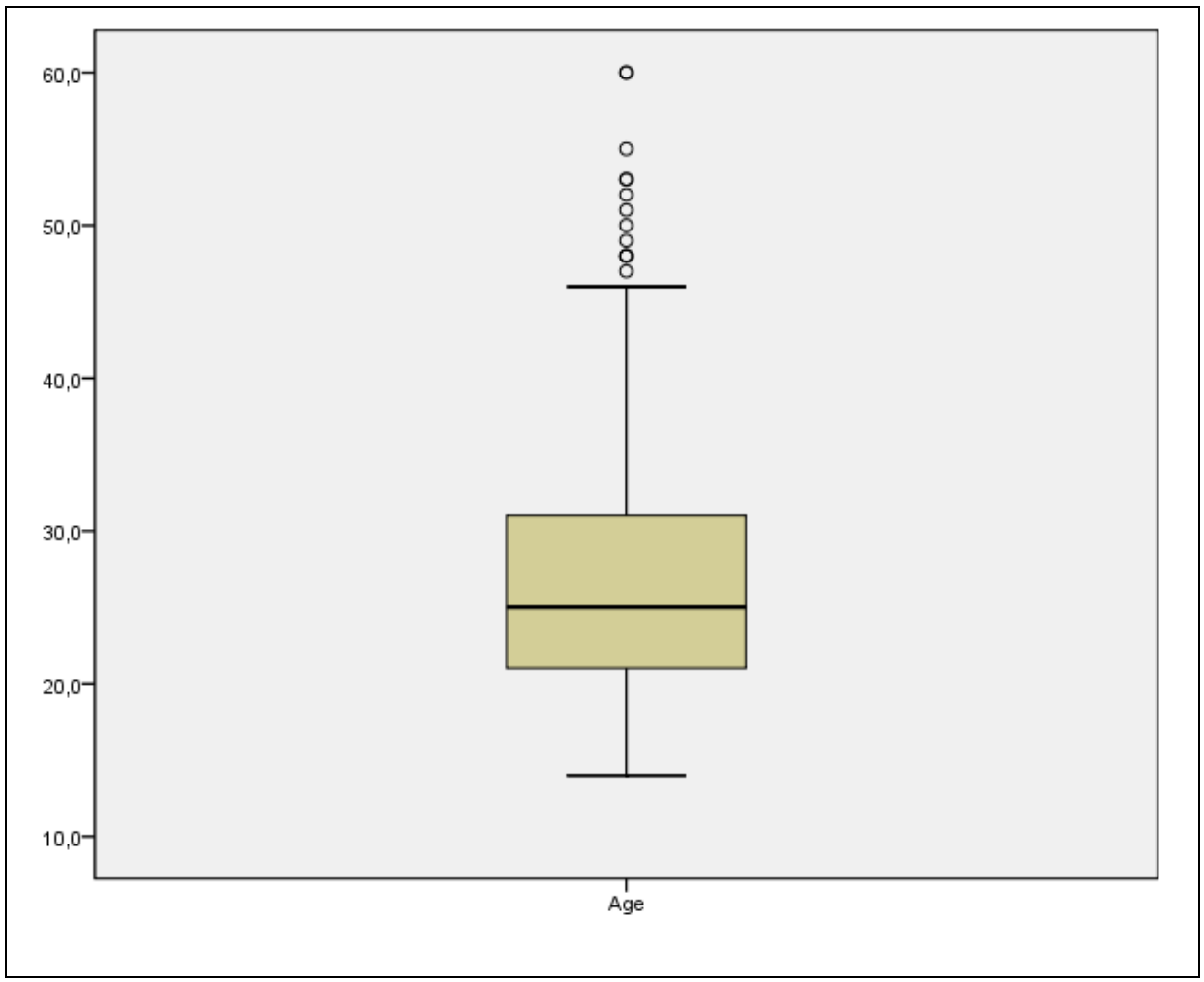
Test statistic: TR^2 = 9.576763,
with p-value = P(Chi-square(8) > 9.576763) = 0.295996

Appendix G : Graphs

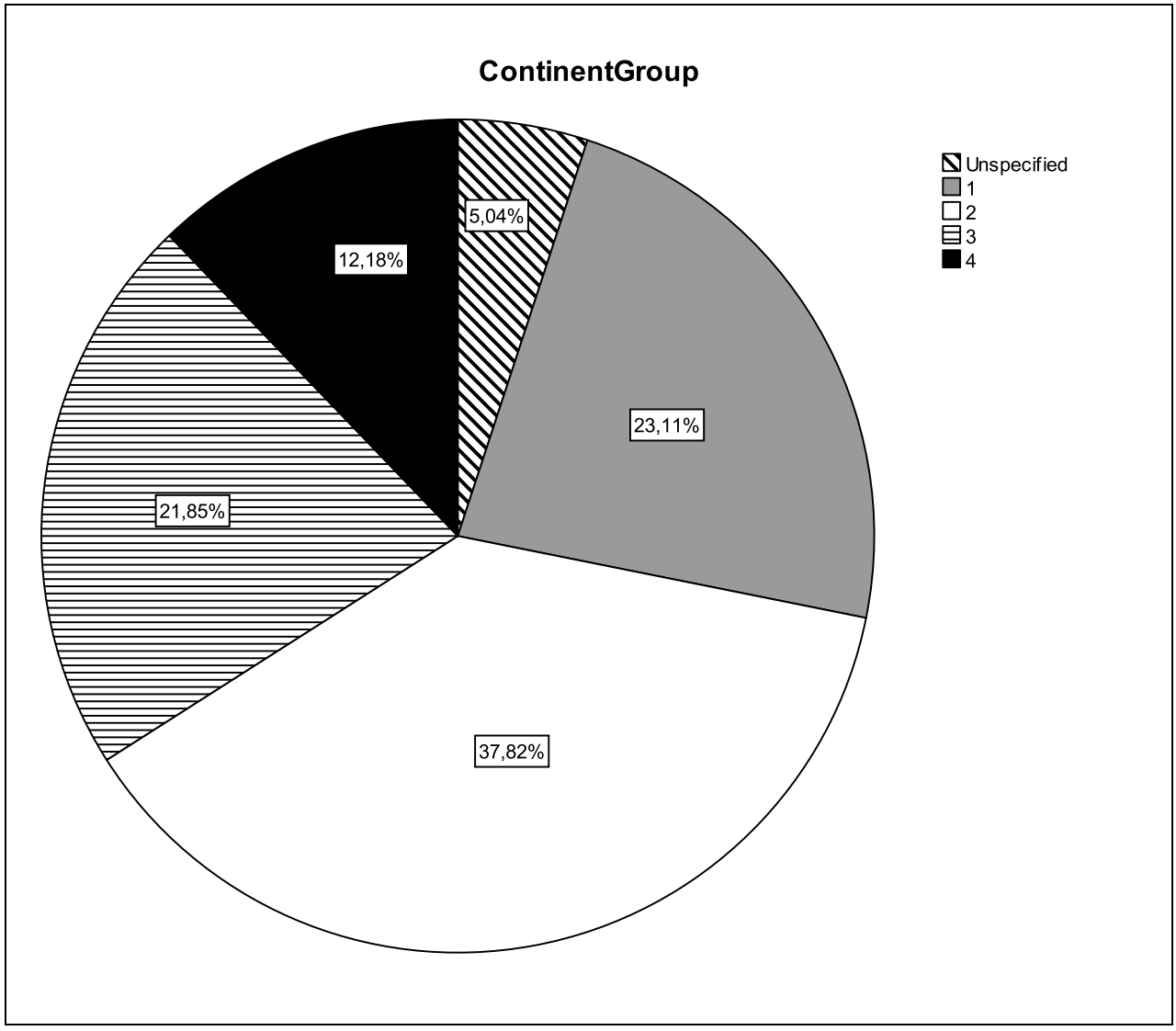
Graph G1



Graph G2

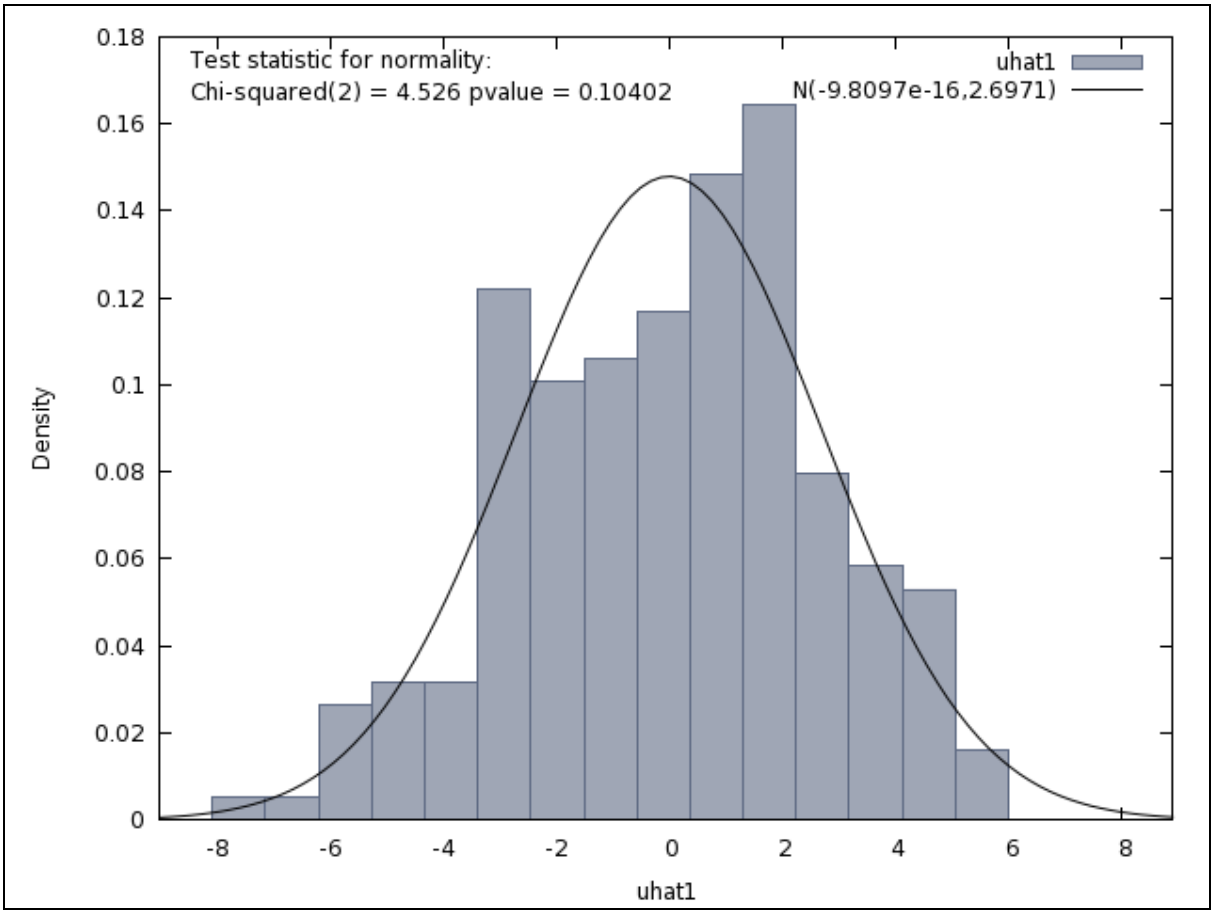


Graph G3

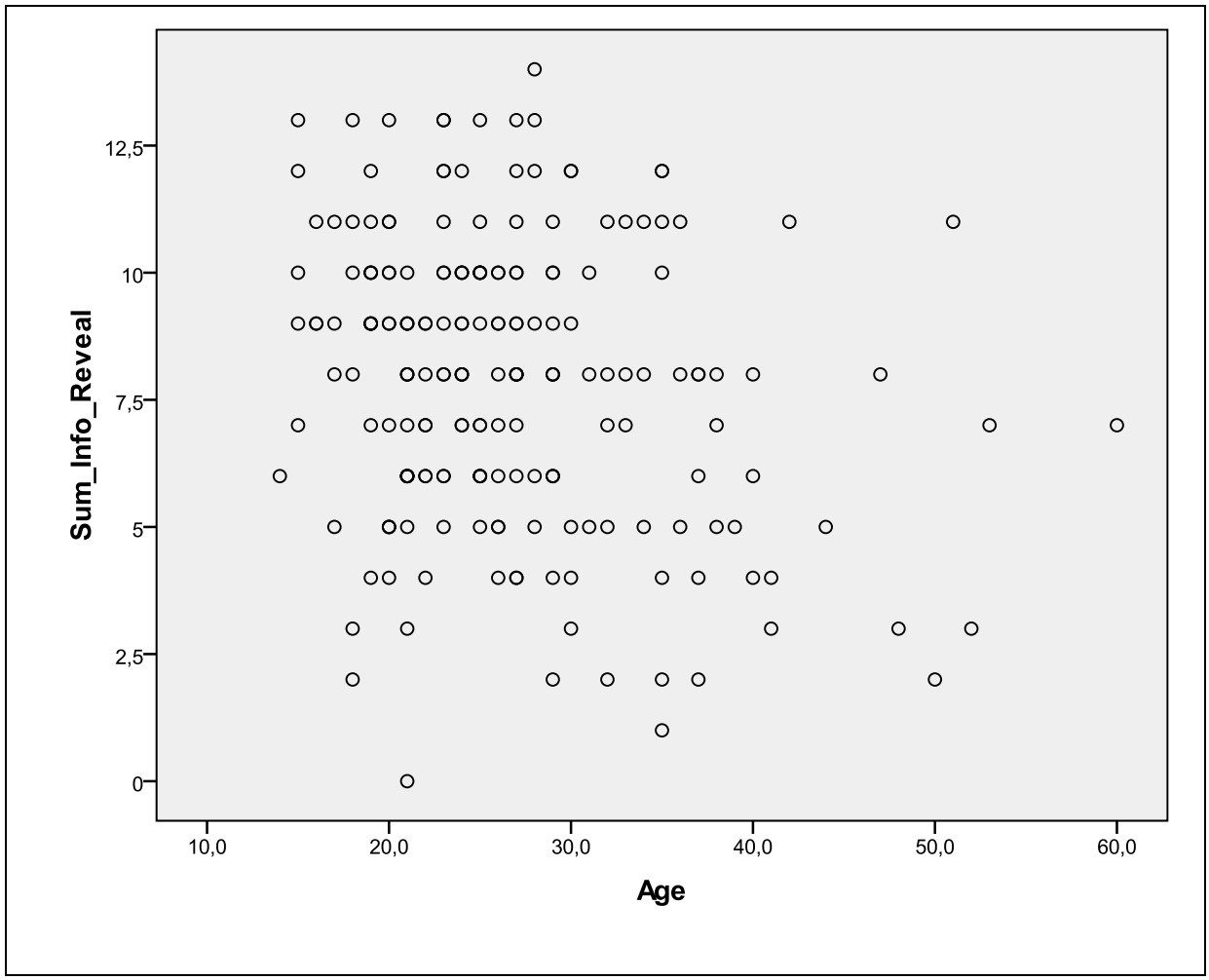


Graph G4

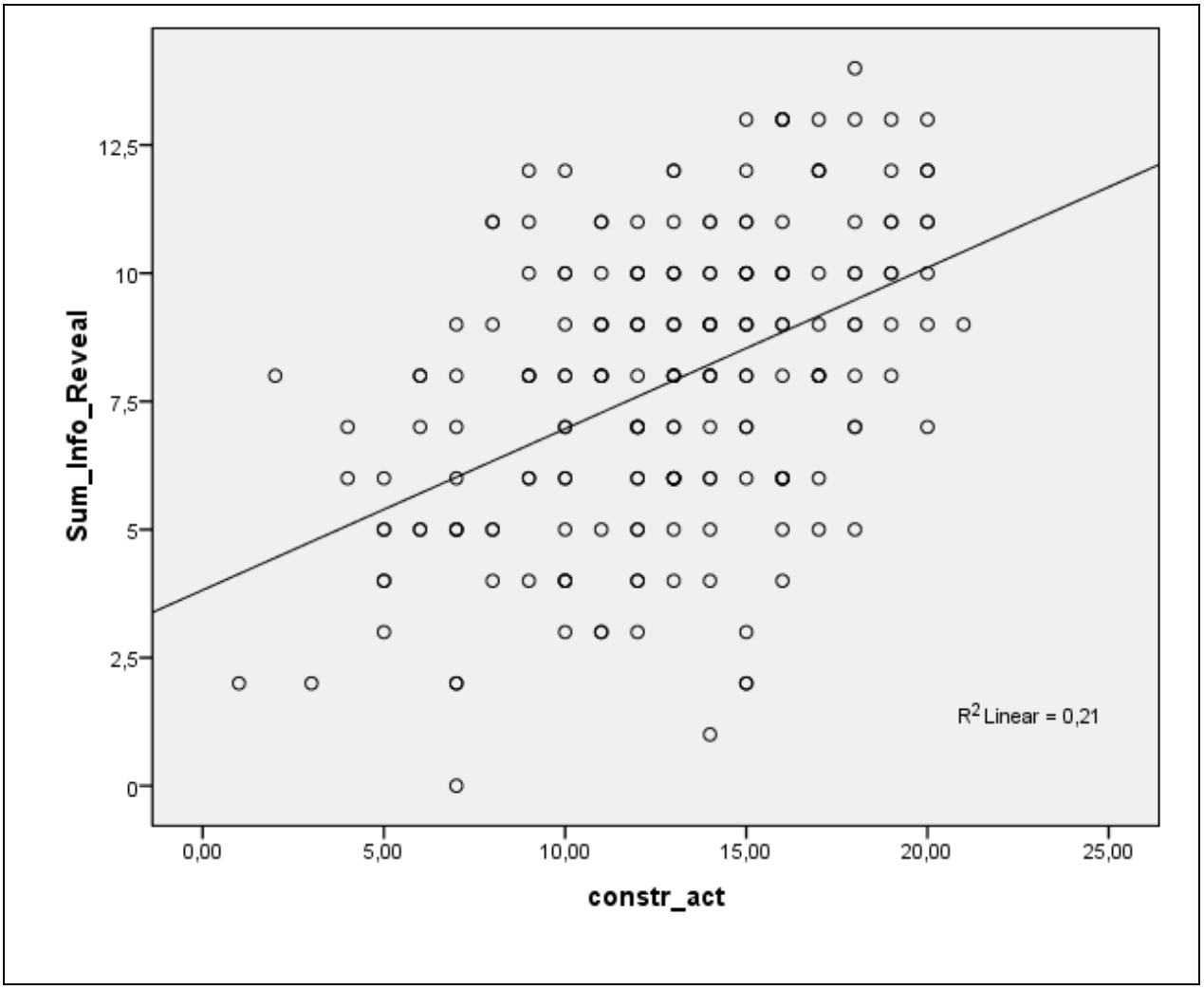
Test for normality of residuals pertaining to the regression in Table F1 and F2



Graph G5

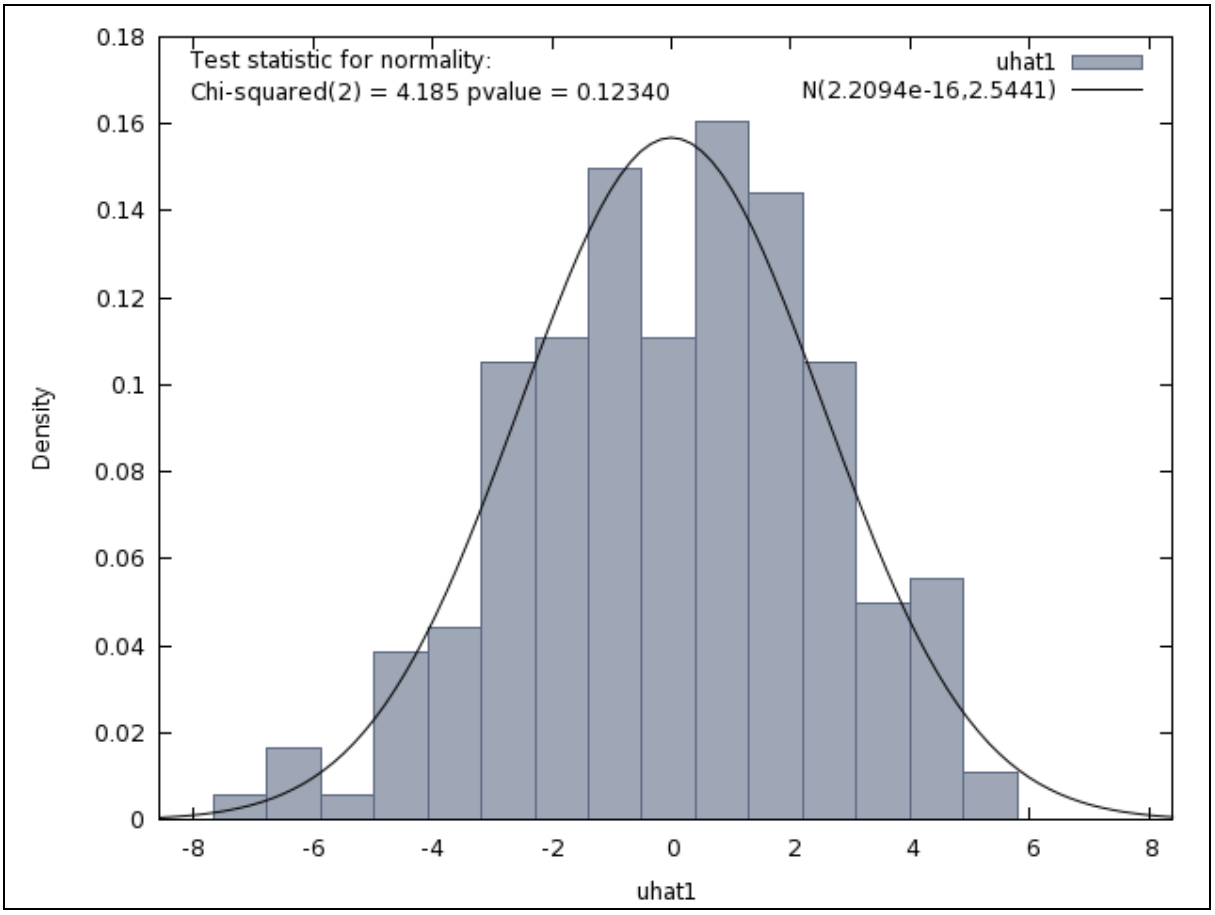


Graph G6


Sum_Info_Reveal
12,5
10
7,5
5
2,5
0
0,00
5,00
10,00
15,00
20,00
25,00
constr_act
R2 Linear = 0,21

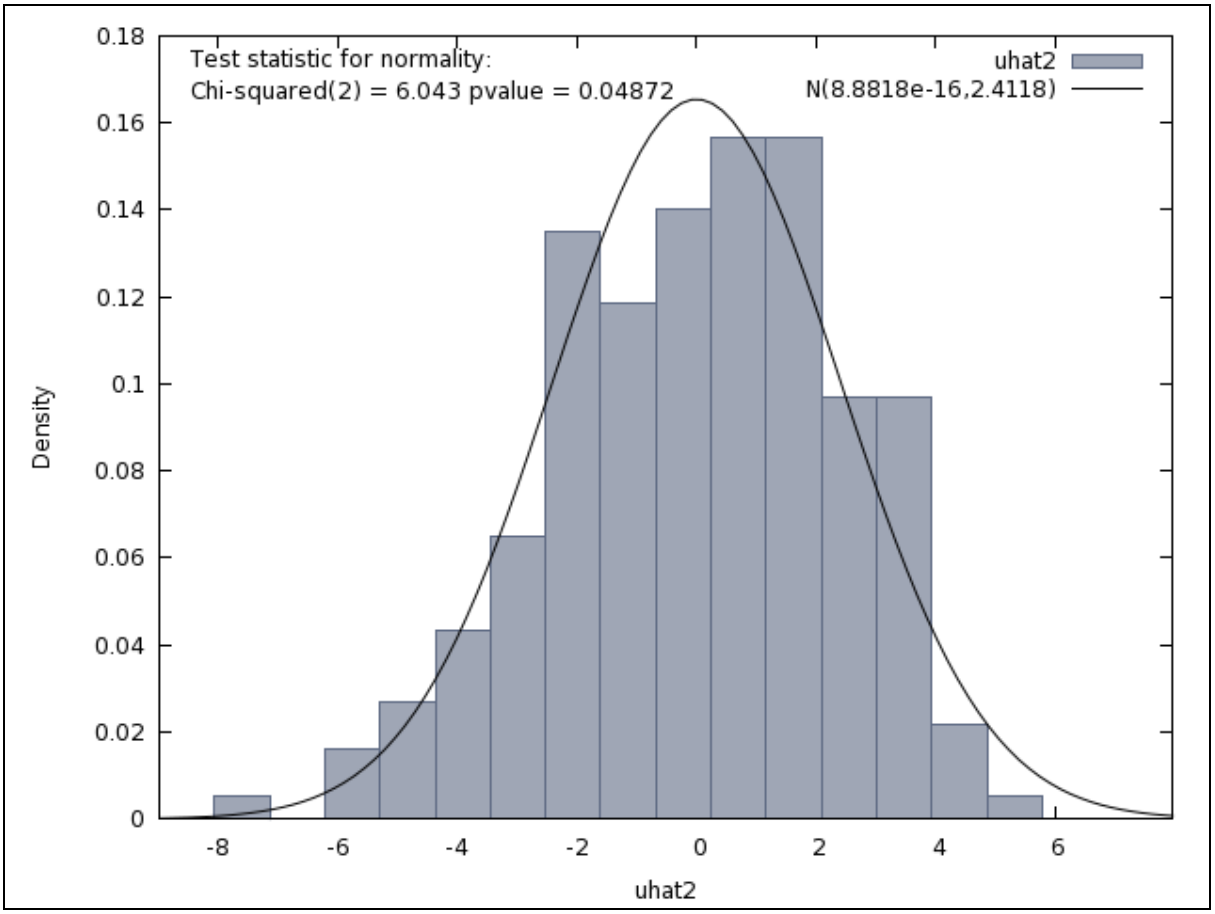
Graph G7

Test for normality of residuals pertaining to the regression in Table F4 and F5

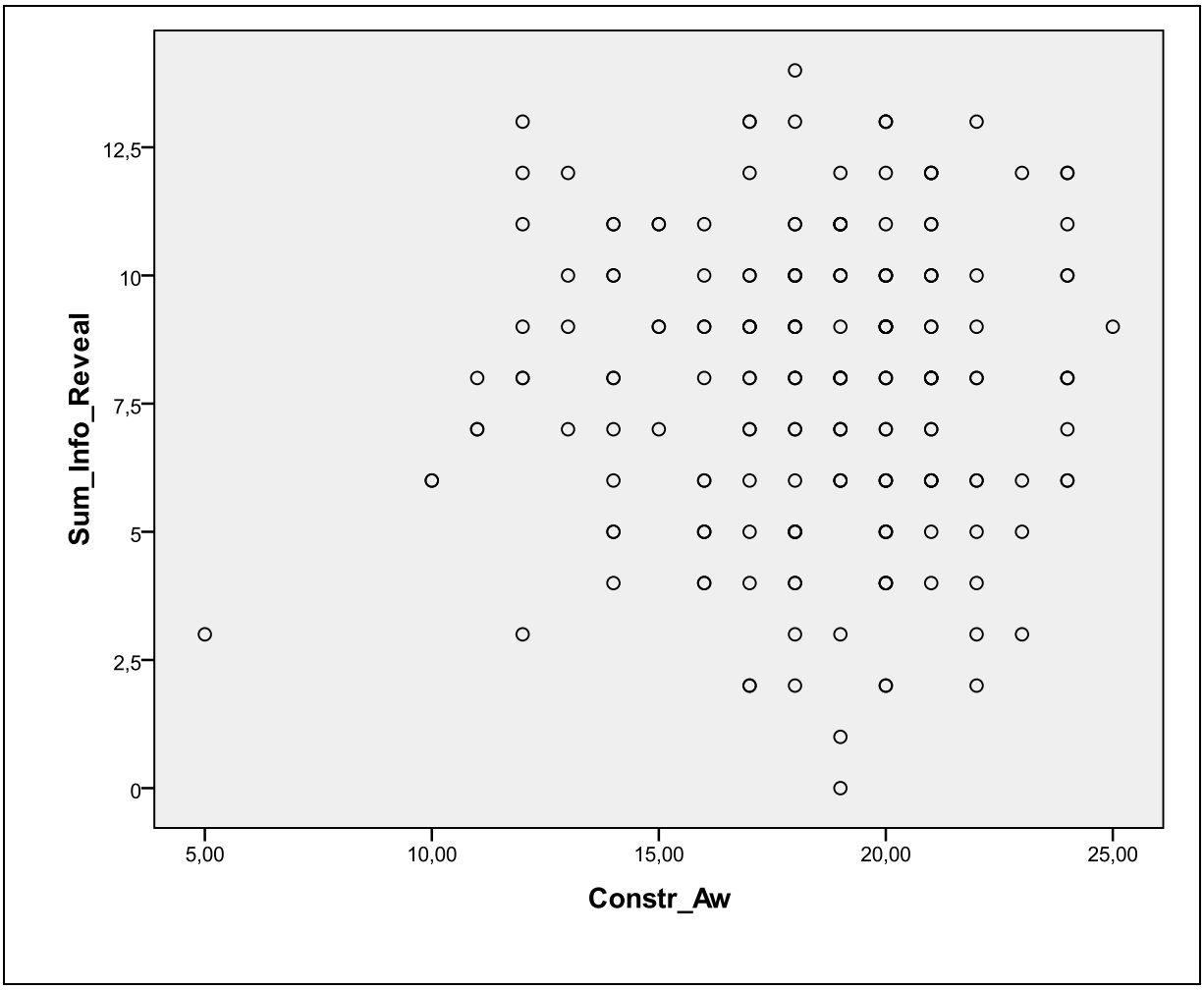


Graph G8

Test for normality of residuals pertaining to the regression in Table F7 and F8



Graph G9


Sum_Info_Reveal
12,5
10
7,5
5
2,5
0
5,00
10,00
15,00
20,00
25,00
Constr_Aw

Appendix H: Facebook's Terms and Conditions

This agreement was written in English (US). Please note that Section 16 contains certain changes to the general terms for users outside the United States.

Date of Last Revision: April 22, 2010

Statement of Rights and Responsibilities

This Statement of Rights and Responsibilities ("Statement") derives from the Facebook Principles, and governs our relationship with users and others who interact with Facebook. By using or accessing Facebook, you agree to this Statement.

1. **Privacy**
   Your privacy is very important to us. We designed our Privacy Policy to make important disclosures about how you can use Facebook to share with others and how we collect and can use your content and information. We encourage you to read the Privacy Policy, and to use it to help make informed decisions.
2. **Sharing Your Content and Information**
   You own all of the content and information you post on Facebook, and you can control how it is shared through your privacy and application settings. In addition:
   1. For content that is covered by intellectual property rights, like photos and videos ("IP content"), you specifically give us the following permission, subject to your privacy and application settings: you grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook ("IP License"). This IP License ends when you delete your IP content or your account unless your content has been shared with others, and they have not deleted it.
   2. When you delete IP content, it is deleted in a manner similar to emptying the recycle bin on a computer. However, you understand that removed content may persist in backup copies for a reasonable period of time (but will not be available to others).
   3. When you use an application, your content and information is shared with the application. We require applications to respect your privacy, and your agreement with that application will control how the application can use, store, and transfer that content and information. (To learn more about Platform, read our Privacy Policy and About Platform page.)
   4. When you publish content or information using the "everyone" setting, it means that you are allowing everyone, including people off of Facebook, to access and use that information, and to associate it with you (i.e., your name and profile picture).
   5. We always appreciate your feedback or other suggestions about Facebook, but you understand that we may use them without any obligation to compensate you for them (just as you have no obligation to offer them).
3. **Safety**
   We do our best to keep Facebook safe, but we cannot guarantee it. We need your help to do that, which includes the following commitments:
   1. You will not send or otherwise post unauthorized commercial communications (such as spam) on Facebook.

2. You will not collect users' content or information, or otherwise access Facebook, using automated means (such as harvesting bots, robots, spiders, or scrapers) without our permission.
3. You will not engage in unlawful multi-level marketing, such as a pyramid scheme, on Facebook.
4. You will not upload viruses or other malicious code.
5. You will not solicit login information or access an account belonging to someone else.
6. You will not bully, intimidate, or harass any user.
7. You will not post content that: is hateful, threatening, or pornographic; incites violence; or contains nudity or graphic or gratuitous violence.
8. You will not develop or operate a third-party application containing alcohol-related or other mature content (including advertisements) without appropriate age-based restrictions.
9. You will not offer any contest, giveaway, or sweepstakes ("promotion") on Facebook without our prior written consent. If we consent, you take full responsibility for the promotion, and will follow our Promotions Guidelines and all applicable laws.
10. You will not use Facebook to do anything unlawful, misleading, malicious, or discriminatory.
11. You will not do anything that could disable, overburden, or impair the proper working of Facebook, such as a denial of service attack.
12. You will not facilitate or encourage any violations of this Statement.

4. **Registration and Account Security**

Facebook users provide their real names and information, and we need your help to keep it that way. Here are some commitments you make to us relating to registering and maintaining the security of your account:

1. You will not provide any false personal information on Facebook, or create an account for anyone other than yourself without permission.
2. You will not create more than one personal profile.
3. If we disable your account, you will not create another one without our permission.
4. You will not use your personal profile for your own commercial gain (such as selling your status update to an advertiser).
5. You will not use Facebook if you are under 13.
6. You will not use Facebook if you are a convicted sex offender.
7. You will keep your contact information accurate and up-to-date.
8. You will not share your password, (or in the case of developers, your secret key), let anyone else access your account, or do anything else that might jeopardize the security of your account.
9. You will not transfer your account (including any page or application you administer) to anyone without first getting our written permission.
10. If you select a username for your account we reserve the right to remove or reclaim it if we believe appropriate (such as when a trademark owner complains about a username that does not closely relate to a user's actual name).

5. **Protecting Other People's Rights**

We respect other people's rights, and expect you to do the same.

1. You will not post content or take any action on Facebook that infringes or violates someone else's rights or otherwise violates the law.
2. We can remove any content or information you post on Facebook if we believe that it violates this Statement.
3. We will provide you with tools to help you protect your intellectual property rights. To learn more, visit our How to Report Claims of Intellectual Property Infringement page.

4. If we remove your content for infringing someone else's copyright, and you believe we removed it by mistake, we will provide you with an opportunity to appeal.
5. If you repeatedly infringe other people's intellectual property rights, we will disable your account when appropriate.
6. You will not use our copyrights or trademarks (including Facebook, the Facebook and F Logos, FB, Face, Poke, Wall and 32665), or any confusingly similar marks, without our written permission.
7. If you collect information from users, you will: obtain their consent, make it clear you (and not Facebook) are the one collecting their information, and post a privacy policy explaining what information you collect and how you will use it.
8. You will not post anyone's identification documents or sensitive financial information on Facebook.
9. You will not tag users or send email invitations to non-users without their consent.

6. **Mobile**
    1. We currently provide our mobile services for free, but please be aware that your carrier's normal rates and fees, such as text messaging fees, will still apply.
    2. In the event you change or deactivate your mobile telephone number, you will update your account information on Facebook within 48 hours to ensure that your messages are not sent to the person who acquires your old number.
    3. You provide all rights necessary to enable users to sync (including through an application) their contact lists with any basic information and contact information that is visible to them on Facebook, as well as your name and profile picture.
7. **Payments**
   If you make a payment on Facebook or use Facebook Credits, you agree to our Payments Terms.
8. **Special Provisions Applicable to Share Links**
   If you include our Share Link button on your website, the following additional terms apply to you:
    1. We give you permission to use Facebook's Share Link button so that users can post links or content from your website on Facebook.
    2. You give us permission to use and allow others to use such links and content on Facebook.
    3. You will not place a Share Link button on any page containing content that would violate this Statement if posted on Facebook.
9. **Special Provisions Applicable to Developers/Operators of Applications and Websites**
   If you are a developer or operator of a Platform application or website, the following additional terms apply to you:
    1. You are responsible for your application and its content and all uses you make of Platform. This includes ensuring your application or use of Platform meets our Developer Principles and Policies and our Advertising Guidelines.
    2. Your access to and use of data you receive from Facebook, will be limited as follows:
        1. You will only request data you need to operate your application.
        2. You will have a privacy policy that tells users what user data you are going to use and how you will use, display, share, or transfer that data.
        3. You will not use, display, share, or transfer a user’s data in a manner inconsistent with your privacy policy.
        4. You will delete all data you receive from us concerning a user if the user asks you to do so, and will provide a mechanism for users to make such a request.
        5. You will not include data you receive from us concerning a user in any advertising creative.

6. You will not directly or indirectly transfer any data you receive from us to (or use such data in connection with) any ad network, ad exchange, data broker, or other advertising related toolset, even if a user consents to that transfer or use.
7. We can limit your access to data.
8. You will comply with all other restrictions contained in our Developer Principles and Policies.

3. You will not give us information that you independently collect from a user or a user's content without that user's consent.
4. You will make it easy for users to remove or disconnect from your application.
5. You will make it easy for users to contact you. We can also share your email address with users and others claiming that you have infringed or otherwise violated their rights.
6. You will provide customer support for your application.
7. You will not show third party ads or web search boxes on Facebook.
8. We give you all rights necessary to use the code, APIs, data, and tools you receive from us.
9. You will not sell, transfer, or sublicense our code, APIs, or tools to anyone.
10. You will not misrepresent your relationship with Facebook to others.
11. You may use the logos we make available to developers or issue a press release or other public statement so long as you follow our Developer Principles and Policies.
12. We can issue a press release describing our relationship with you.
13. You will comply with all applicable laws. In particular you will (if applicable):
    1. have a policy for removing infringing content and terminating repeat infringers that complies with the Digital Millennium Copyright Act.
    2. comply with the Video Privacy Protection Act ("VPPA"), and obtain any opt-in consent necessary from users so that user data subject to the VPPA may be shared on Facebook. You represent that any disclosure to us will not be incidental to the ordinary course of your business.
14. We do not guarantee that Platform will always be free.
15. You give us all rights necessary to enable your application to work with Facebook, including the right to incorporate content and information you provide to us into streams, profiles, and user action stories.
16. You give us the right to link to or frame your application, and place content, including ads, around your application.
17. We can analyze your application, content, and data for any purpose, including commercial (such as for targeting the delivery of advertisements and indexing content for search).
18. To ensure your application is safe for users, we can audit it.
19. We can create applications that offer similar features and services to, or otherwise compete with, your application.

10. **About Advertisements on Facebook**

Our goal is to deliver ads that are not only valuable to advertisers, but also valuable to you. In order to do that, you agree to the following:

1. You can use your privacy settings to limit how your name and profile picture may be associated with commercial or sponsored content served by us. You give us permission to use your name and profile picture in connection with that content, subject to the limits you place.
2. We do not give your content or information to advertisers without your consent.
3. You understand that we may not always identify paid services and communications as such.

11. **Special Provisions Applicable to Advertisers**

You can target your specific audience by buying ads on Facebook or our publisher network. The

following additional terms apply to you if you place an order through our online advertising portal ("Order"):

1. When you place an Order, you will tell us the type of advertising you want to buy, the amount you want to spend, and your bid. If we accept your Order, we will deliver your ads as inventory becomes available.
2. You will pay for your Orders in accordance with our Payments Terms. The amount you owe will be calculated based on our tracking mechanisms.
3. Your ads will comply with our Advertising Guidelines.
4. We will determine the size, placement, and positioning of your ads.
5. We do not guarantee the activity that your ads will receive, such as the number of clicks you will get.
6. We cannot control how people interact with your ads, and are not responsible for click fraud or other improper actions that affect the cost of running ads. We do, however, have systems to detect and filter certain suspicious activity, learn more here.
7. You can cancel your Order at any time through our online portal, but it may take up to 24 hours before the ad stops running. You are responsible for paying for those ads.
8. Our license to run your ad will end when we have completed your Order. You understand, however, that if users have interacted with your ad, your ad may remain until the users delete it.
9. We can use your ads and related content and information for marketing or promotional purposes.
10. You will not issue any press release or make public statements about your relationship with Facebook without written permission.
11. We may reject or remove any ad for any reason.

    If you are placing ads on someone else's behalf, we need to make sure you have permission to place those ads, including the following:
12. You warrant that you have the legal authority to bind the advertiser to this Statement.
13. You agree that if the advertiser you represent violates this Statement, we may hold you responsible for that violation.

12. **Special Provisions Applicable to Pages**

    If you create or administer a Page on Facebook, you agree to our Pages Terms.
13. **Amendments**
    1. We can change this Statement if we provide you notice (by posting the change on the Facebook Site Governance Page) and an opportunity to comment To get notice of any future changes to this Statement, visit our Facebook Site Governance Page and become a fan.
    2. For changes to sections 7, 8, 9, and 11 (sections relating to payments, application developers, website operators, and advertisers), we will give you a minimum of three days notice. For all other changes we will give you a minimum of seven days notice. All such comments must be made on the Facebook Site Governance Page.
    3. If more than 7,000 users comment on the proposed change, we will also give you the opportunity to participate in a vote in which you will be provided alternatives. The vote shall be binding on us if more than 30% of all active registered users as of the date of the notice vote.
    4. We can make changes for legal or administrative reasons, or to correct an inaccurate statement, upon notice without opportunity to comment.
14. **Termination**

    If you violate the letter or spirit of this Statement, or otherwise create risk or possible legal exposure for us, we can stop providing all or part of Facebook to you. We will notify you by email or at the next time you attempt to access your account. You may also delete your account or

disable your application at any time. In all such cases, this Statement shall terminate, but the following provisions will still apply: 2.2, 2.4, 3-5, 8.2, 9.1-9.3, 9.9, 9.10, 9.13, 9.15, 9.18, 10.3, 11.2, 11.5, 11.6, 11.9, 11.12, 11.13, and 14-18.

15. **Disputes**
    1. You will resolve any claim, cause of action or dispute ("claim") you have with us arising out of or relating to this Statement or Facebook exclusively in a state or federal court located in Santa Clara County. The laws of the State of California will govern this Statement, as well as any claim that might arise between you and us, without regard to conflict of law provisions. You agree to submit to the personal jurisdiction of the courts located in Santa Clara County, California for the purpose of litigating all such claims.
    2. If anyone brings a claim against us related to your actions, content or information on Facebook, you will indemnify and hold us harmless from and against all damages, losses, and expenses of any kind (including reasonable legal fees and costs) related to such claim.
    3. WE TRY TO KEEP FACEBOOK UP, BUG-FREE, AND SAFE, BUT YOU USE IT AT YOUR OWN RISK. WE ARE PROVIDING FACEBOOK "AS IS" WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. WE DO NOT GUARANTEE THAT FACEBOOK WILL BE SAFE OR SECURE. FACEBOOK IS NOT RESPONSIBLE FOR THE ACTIONS, CONTENT, INFORMATION, OR DATA OF THIRD PARTIES, AND YOU RELEASE US, OUR DIRECTORS, OFFICERS, EMPLOYEES, AND AGENTS FROM ANY CLAIMS AND DAMAGES, KNOWN AND UNKNOWN, ARISING OUT OF OR IN ANY WAY CONNECTED WITH ANY CLAIM YOU HAVE AGAINST ANY SUCH THIRD PARTIES. IF YOU ARE A CALIFORNIA RESIDENT, YOU WAIVE CALIFORNIA CIVIL CODE §1542, WHICH SAYS: "A GENERAL RELEASE DOES NOT EXTEND TO CLAIMS WHICH THE CREDITOR DOES NOT KNOW OR SUSPECT TO EXIST IN HIS FAVOR AT THE TIME OF EXECUTING THE RELEASE, WHICH IF KNOWN BY HIM MUST HAVE MATERIALLY AFFECTED HIS SETTLEMENT WITH THE DEBTOR." WE WILL NOT BE LIABLE TO YOU FOR ANY LOST PROFITS OR OTHER CONSEQUENTIAL, SPECIAL, INDIRECT, OR INCIDENTAL DAMAGES ARISING OUT OF OR IN CONNECTION WITH THIS STATEMENT OR FACEBOOK, EVEN IF WE HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. OUR AGGREGATE LIABILITY ARISING OUT OF THIS STATEMENT OR FACEBOOK WILL NOT EXCEED THE GREATER OF ONE HUNDRED DOLLARS ($100) OR THE AMOUNT YOU HAVE PAID US IN THE PAST TWELVE MONTHS. APPLICABLE LAW MAY NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY OR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU. IN SUCH CASES, FACEBOOK'S LIABILITY WILL BE LIMITED TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW.

16. **Special Provisions Applicable to Users Outside the United States**

    We strive to create a global community with consistent standards for everyone, but we also strive to respect local laws. The following provisions apply to users outside the United States:
    1. You consent to having your personal data transferred to and processed in the United States.
    2. If you are located in a country embargoed by the United States, or are on the U.S. Treasury Department's list of Specially Designated Nationals you will not engage in commercial activities on Facebook (such as advertising or payments) or operate a Platform application or website.

3. Certain specific terms that apply only for German users are available here.

17. **Definitions**
    1. By "Facebook" we mean the features and services we make available, including through (a) our website at www.facebook.com and any other Facebook branded or co-branded websites (including sub-domains, international versions, widgets, and mobile versions); (b) our Platform; and (c) other media, software (such as a toolbar), devices, or networks now existing or later developed.
    2. By "us," "we" and "our" we mean Facebook, Inc., or if you are outside of the United States, Facebook Ireland Limited.
    3. By "Platform" we mean a set of APIs and services that enable others, including application developers and website operators, to retrieve data from Facebook or provide data to us.
    4. By "information" we mean facts and other information about you, including actions you take.
    5. By "content" we mean anything you post on Facebook that would not be included in the definition of "information."
    6. By "data" we mean content and information that third parties can retrieve from Facebook or provide to Facebook through Platform.
    7. By "post" we mean post on Facebook or otherwise make available to us (such as by using an application).
    8. By "use" we mean use, copy, publicly perform or display, distribute, modify, translate, and create derivative works of.
    9. By "active registered user" we mean a user who has logged into Facebook at least once in the previous 30 days.
    10. By "application" we mean any application or website that uses or accesses Platform, as well as anything else that receives data from us.

18. **Other**
    1. This Statement makes up the entire agreement between the parties regarding Facebook, and supersedes any prior agreements.
    2. If any portion of this Statement is found to be unenforceable, the remaining portion will remain in full force and effect.
    3. If we fail to enforce any of this Statement, it will not be considered a waiver.
    4. Any amendment to or waiver of this Statement must be made in writing and signed by us.
    5. You will not transfer any of your rights or obligations under this Statement to anyone else without our consent.
    6. All of our rights and obligations under this Statement are freely assignable by us in connection with a merger, acquisition, or sale of assets, or by operation of law or otherwise.
    7. Nothing in this Statement shall prevent us from complying with the law.
    8. This Statement does not confer any third party beneficiary rights.

Appendix I: Facebook's Privacy Policy

This policy contains eight sections, and you can jump to each by selecting the links below:

1. Introduction
2. Information We Receive
3. Information You Share With Third Parties
4. Sharing Information on Facebook
5. How We Use Your Information
6. How We Share Information
7. How You Can View, Change, or Remove Information
8. How We Protect Information
9. Other Terms

1. Introduction

Questions. If you have any questions or concerns about our privacy policy, contact our privacy team through this help page. You may also contact us by mail at 1601 S. California Avenue, Palo Alto, CA 94304.

TRUSTe Program. Facebook is a certified licensee of the TRUSTe Privacy Seal Program. This means that our privacy policy and practices have been reviewed by TRUSTe, an independent organization focused on reviewing privacy and security policies and practices, for compliance with its strict program requirements. This privacy policy covers the website www.facebook.com. The TRUSTe program covers only information that is collected through this Web site, and does not cover other information, such as information that may be collected through software downloaded from Facebook.

If you have any complaints about our policy or practices please let us know through this help page. If you are not satisfied with our response, you can contact TRUSTe.

Safe Harbor. Facebook also adheres to the Safe Harbor framework developed by the U.S. Department of Commerce and the European Union. As part of our participation in the Safe Harbor, we agree to resolve

all disputes you have with us in connection with our policies and practices through TRUSTe. To view our certification, visit the U.S. Department of Commerce's Safe Harbor Web site.

Scope. This privacy policy covers all of Facebook. It does not, however, apply to entities that Facebook does not own or control, such as applications and websites using Platform. By using or accessing Facebook, you agree to our privacy practices outlined here.

No information from children under age 13. If you are under age 13, please do not attempt to register for Facebook or provide any personal information about yourself to us. If we learn that we have collected personal information from a child under age 13, we will delete that information as quickly as possible. If you believe that we might have any information from a child under age 13, please contact us through this help page.

Parental participation. We strongly recommend that minors 13 years of age or older ask their parents for permission before sending any information about themselves to anyone over the Internet and we encourage parents to teach their children about safe internet use practices. Materials to help parents talk to their children about safe internet use can be found on this help page.

2. Information We Receive

Information you provide to us:

Information About Yourself. When you sign up for Facebook you provide us with your name, email, gender, and birth date. During the registration process we give you the opportunity to connect with your friends, schools, and employers. You will also be able to add a picture of yourself. In some cases we may ask for additional information for security reasons or to provide specific services to you. Once you register you can provide other information about yourself by connecting with, for example, your current city, hometown, family, relationships, networks, activities, interests, and places. You can also provide personal information about yourself, such as your political and religious views.

Content. One of the primary reasons people use Facebook is to share content with others. Examples include when you update your status, upload or take a photo, upload or record a video, share a link, create an event or a group, make a comment, write something on someone's Wall, write a note, or send someone a message. If you do not want us to store metadata associated with content you share on Facebook (such as photos), please remove the metadata before uploading the content.

Transactional Information. We may retain the details of transactions or payments you make on Facebook. If you do not want us to store your payment source account number, you can remove it using your payments page.

Friend Information. We offer contact importer tools to help you upload your friends' addresses so that you can find your friends on Facebook, and invite your contacts who do not have Facebook accounts to join. If you do not want us to store this information, visit this help page. If you give us your password to retrieve those contacts, we will not store your password after you have uploaded your contacts' information.

Information we collect when you interact with Facebook:

Site activity information. We keep track of some of the actions you take on Facebook, such as adding connections (including joining a group or adding a friend), creating a photo album, sending a gift, poking another user, indicating you "like" a post, attending an event, or connecting with an application. In some

cases you are also taking an action when you provide information or content to us. For example, if you share a video, in addition to storing the actual content you uploaded, we might log the fact that you shared it.

Access Device and Browser Information. When you access Facebook from a computer, mobile phone, or other device, we may collect information from that device about your browser type, location, and IP address, as well as the pages you visit.

Cookie Information. We use "cookies" (small pieces of data we store for an extended period of time on your computer, mobile phone, or other device) to make Facebook easier to use, to make our advertising better, and to protect both you and Facebook. For example, we use them to store your login ID (but never your password) to make it easier for you to login whenever you come back to Facebook. We also use them to confirm that you are logged into Facebook, and to know when you are interacting with Facebook Platform applications and websites, our widgets and Share buttons, and our advertisements. You can remove or block cookies using the settings in your browser, but in some cases that may impact your ability to use Facebook.

Information we receive from third parties:

Facebook Platform. We do not own or operate the applications or websites that you use through Facebook Platform (such as games and utilities). Whenever you connect with a Platform application or website, we will receive information from them, including information about actions you take. In some cases, in order to personalize the process of connecting, we may receive a limited amount of information even before you connect with the application or website.

Information from other websites. We may institute programs with advertising partners and other websites in which they share information with us:

- We may ask advertisers to tell us how our users responded to the ads we showed them (and for comparison purposes, how other users who didn't see the ads acted on their site). This data sharing, commonly known as "conversion tracking," helps us measure our advertising effectiveness and improve the quality of the advertisements you see.
- We may receive information about whether or not you've seen or interacted with certain ads on other sites in order to measure the effectiveness of those ads.

If in any of these cases we receive data that we do not already have, we will "anonymize" it within 180 days, meaning we will stop associating the information with any particular user. If we institute these programs, we will only use the information in the ways we explain in the "How We Use Your Information" section below.

Information from other users. We may collect information about you from other Facebook users, such as when a friend tags you in a photo, video, or place, provides friend details, or indicates a relationship with you.

3. Sharing information on Facebook.

This section explains how your privacy settings work, and how your information is shared on Facebook. You should always consider your privacy settings before sharing information on Facebook.

Name and Profile Picture. Facebook is designed to make it easy for you to find and connect with others. For this reason, your name and profile picture do not have privacy settings. If you are

uncomfortable with sharing your profile picture, you should delete it (or not add one). You can also control who can find you when searching on Facebook or on public search engines using the application section of your privacy settings.

Contact Information. Your contact information settings control who can contact you on Facebook, and who can see your contact information such as your email and phone number(s). Remember that none of this information is required except for your email address, and you do not have to share your email address with anyone.

Personal Information. Your personal information settings control who can see your personal information, such as your religious and political views, if you choose to add them. We recommend that you share this information using the friends of friends setting.

Posts by Me. You can select a privacy setting for every post you make using the publisher on our site. Whether you are uploading a photo or posting a status update, you can control exactly who can see it at the time you create it. Whenever you share something look for the lock icon. Clicking on the lock will bring up a menu that lets you choose who will be able to see your post. If you decide not to select your setting at the time you post the content, your content will be shared consistent with your Posts by Me privacy setting.

Connections. Facebook enables you to connect with virtually anyone or anything you want, from your friends and family to the city you live in to the restaurants you like to visit to the bands and movies you love. Because it takes two to connect, your privacy settings only control who can see the connection on your profile page. If you are uncomfortable with the connection being publicly available, you should consider removing (or not making) the connection.

Gender and Birth Date. In addition to name and email address, we require you to provide your gender and birth date during the registration process. We ask for your date of birth to verify that you are 13 or older, and so that we can better limit your access to content and advertisements that are not age appropriate. Because your date of birth and gender are required, you cannot delete them. You can, however, edit your profile to hide all (or part) of such fields from other users.

Other. Here are some other things to remember:

- Some of the content you share and the actions you take will show up on your friends' home pages and other pages they visit.
- If another user tags you in a photo or video or at a place, you can remove the tag. You can also limit who can see that you have been tagged on your profile from your privacy settings.
- Even after you remove information from your profile or delete your account, copies of that information may remain viewable elsewhere to the extent it has been shared with others, it was otherwise distributed pursuant to your privacy settings, or it was copied or stored by other users.
- You understand that information might be reshared or copied by other users.
- Certain types of communications that you send to other users cannot be removed, such as messages.
- When you post information on another user's profile or comment on another user's post, that information will be subject to the other user's privacy settings.
- If you use an external source to publish information to Facebook (such as a mobile application or a Connect site), you should check the privacy setting for that post, as it is set by that external source.

"Everyone" Information. Information set to "everyone" is publicly available information, just like your name, profile picture, and connections. Such information may, for example, be accessed by everyone on the Internet (including people not logged into Facebook), be indexed by third party search engines, and be imported, exported, distributed, and redistributed by us and others without privacy limitations. Such information may also be associated with you, including your name and profile picture, even outside of Facebook, such as on public search engines and when you visit other sites on the internet. The default privacy setting for certain types of information you post on Facebook is set to "everyone." You can review and change the default settings in your privacy settings. If you delete "everyone" content that you posted on Facebook, we will remove it from your Facebook profile, but have no control over its use outside of Facebook.

Minors. We reserve the right to add special protections for minors (such as to provide them with an age-appropriate experience) and place restrictions on the ability of adults to share and connect with minors, recognizing this may provide minors a more limited experience on Facebook

4. Information You Share With Third Parties.

Facebook Platform. As mentioned above, we do not own or operate the applications or websites that use Facebook Platform. That means that when you use those applications and websites you are making your Facebook information available to someone other than Facebook. Prior to allowing them to access any information about you, we require them to agree to terms that limit their use of your information (which you can read about in Section 9 of our Statement of Rights and Responsibilities) and we use technical measures to ensure that they only obtain authorized information. To learn more about Platform, visit our About Platform page.

Connecting with an Application or Website. When you connect with an application or website it will have access to General Information about you. The term General Information includes your and your friends' names, profile pictures, gender, user IDs, connections, and any content shared using the Everyone privacy setting. We may also make information about the location of your computer or access device and your age available to applications and websites in order to help them implement appropriate security measures and control the distribution of age-appropriate content. If the application or website wants to access any other data, it will have to ask for your permission.

We give you tools to control how your information is shared with applications and websites that use Platform. For example, you can block specific applications from accessing your information by visiting your application settings or the application's "About" page. You can also use your privacy settings to limit which of your information is available to "everyone".

You should always review the policies of third party applications and websites to make sure you are comfortable with the ways in which they use information you share with them. We do not guarantee that they will follow our rules. If you find an application or website that violates our rules, you should report the violation to us on this help page and we will take action as necessary.

When your friends use Platform. If your friend connects with an application or website, it will be able to access your name, profile picture, gender, user ID, and information you have shared with "everyone." It will also be able to access your connections, except it will not be able to access your friend list. If you have already connected with (or have a separate account with) that website or application, it may also be able to connect you with your friend on that application or website. If the application or website wants to access any of your other content or information (including your friend list), it will have to obtain specific permission from your friend. If your friend grants specific permission to the application or website, it will generally only be able to access content and information about you that your friend can access. In

addition, it will only be allowed to use that content and information in connection with that friend. For example, if a friend gives an application access to a photo you only shared with your friends, that application could allow your friend to view or print the photo, but it cannot show that photo to anyone else.

We provide you with a number of tools to control how your information is shared when your friend connects with an application or website. For example, you can use your application privacy settings to limit some of the information your friends can make available to applications and websites. You can also block particular applications or websites from accessing your information. You can use your privacy settings to limit which friends can access your information, or limit which of your information is available to "everyone." You can also disconnect from a friend if you are uncomfortable with how they are using your information.

Pre-Approved Third-Party Websites and Applications. In order to provide you with useful social experiences off of Facebook, we occasionally need to provide General Information about you to pre-approved third party websites and applications that use Platform at the time you visit them (if you are still logged in to Facebook). Similarly, when one of your friends visits a pre-approved website or application, it will receive General Information about you so you and your friend can be connected on that website as well (if you also have an account with that website). In these cases we require these websites and applications to go through an approval process, and to enter into separate agreements designed to protect your privacy. For example, these agreements include provisions relating to the access and deletion of your General Information, along with your ability to opt-out of the experience being offered. You can also remove any pre-approved website or application you have visited here, or block all pre-approved websites and applications from getting your General Information when you visit them here. In addition, if you log out of Facebook before visiting a pre-approved application or website, it will not be able to access your information. You can see a complete list of pre-approved websites on our About Platform page.

Exporting Information. You (and those you make your information available to) may use tools like RSS feeds, mobile phone address book applications, or copy and paste functions, to capture, export (and in some cases, import) information from Facebook, including your information and information about you. For example, if you share your phone number with your friends, they may use third party applications to sync that information with the address book on their mobile phone.

Advertisements. Sometimes the advertisers who present ads on Facebook use technological methods to measure the effectiveness of their ads and to personalize advertising content. You may opt-out of the placement of cookies by many of these advertisers here. You may also use your browser cookie settings to limit or prevent the placement of cookies by advertising networks.

Links. When you click on links on Facebook you may leave our site. We are not responsible for the privacy practices of other sites, and we encourage you to read their privacy statements.

5. How We Use Your Information

We use the information we collect to try to provide a safe, efficient, and customized experience. Here are some of the details on how we do that:

To manage the service. We use the information we collect to provide our services and features to you, to measure and improve those services and features, and to provide you with customer support. We use the information to prevent potentially illegal activities, and to enforce our Statement of Rights and Responsibilities. We also use a variety of technological systems to detect and address anomalous activity

and screen content to prevent abuse such as spam. These efforts may on occasion result in a temporary or permanent suspension or termination of some functions for some users.

To contact you. We may contact you with service-related announcements from time to time. You may opt out of all communications except essential updates on your account notifications page. We may include content you see on Facebook in the emails we send to you.

To serve personalized advertising to you. We don't share your information with advertisers without your consent. (An example of consent would be if you asked us to provide your shipping address to an advertiser to receive a free sample.) We allow advertisers to choose the characteristics of users who will see their advertisements and we may use any of the non-personally identifiable attributes we have collected (including information you may have decided not to show to other users, such as your birth year or other sensitive personal information or preferences) to select the appropriate audience for those advertisements. For example, we might use your interest in soccer to show you ads for soccer equipment, but we do not tell the soccer equipment company who you are. You can see the criteria advertisers may select by visiting our advertising page. Even though we do not share your information with advertisers without your consent, when you click on or otherwise interact with an advertisement there is a possibility that the advertiser may place a cookie in your browser and note that it meets the criteria they selected.

To serve social ads. We occasionally pair advertisements we serve with relevant information we have about you and your friends to make advertisements more interesting and more tailored to you and your friends. For example, if you connect with your favorite band's page, we may display your name and profile photo next to an advertisement for that page that is displayed to your friends. We only share the personally identifiable information visible in the social ad with the friend who can see the ad. You can opt out of having your information used in social ads on this help page.

To supplement your profile. We may use information about you that we collect from other Facebook users to supplement your profile (such as when you are tagged in a photo or mentioned in a status update). In such cases we generally give you the ability to remove the content (such as allowing you to remove a photo tag of you) or limit its visibility on your profile.

To make suggestions. We use your profile information, the addresses you import through our contact importers, and other relevant information, to help you connect with your friends, including making suggestions to you and other users that you connect with on Facebook. For example, if another user imports the same email address as you do, we may suggest that you connect with each other. If you want to limit your visibility in suggestions we make to other people, you can adjust your search visibility privacy setting, as you will only be visible in our suggestions to the extent you choose to be visible in public search listings. You may also block specific individual users from being suggested to you and you from being suggested to them.

To help your friends find you. We allow other users to use contact information they have about you, such as your email address, to find you, including through contact importers and search. You can prevent other users from using your email address to find you using the basic information section of your privacy settings.

Downloadable Software. Certain downloadable software applications and applets that we offer, such as our browser toolbars and photo uploaders, transmit data to us. We may not make a formal disclosure if we believe our collection of and use of the information is the obvious purpose of the application, such as the fact that we receive photos when you use our photo uploader. If we believe it is not obvious that we are collecting or using such information, we will make a disclosure to you the first time you provide the information to us so that you can decide whether you want to use that feature.

Memorializing Accounts. If we are notified that a user is deceased, we may memorialize the user's account. In such cases we restrict profile access to confirmed friends, and allow friends and family to write on the user's Wall in remembrance. We may close an account if we receive a formal request from the user's next of kin or other proper legal request to do so.

6. How We Share Information

Facebook is about sharing information with others — friends and people in your communities — while providing you with privacy settings that you can use to restrict other users from accessing some of your information. We share your information with third parties when we believe the sharing is permitted by you, reasonably necessary to offer our services, or when legally required to do so. For example:

When you make a payment. When you enter into transactions with others or make payments on Facebook, we will share transaction information with only those third parties necessary to complete the transaction. We will require those third parties to agree to respect the privacy of your information.

When you invite a friend to join. When you ask us to invite a friend to join Facebook, we will send your friend a message on your behalf using your name. The invitation may also contain information about other users your friend might know. We may also send up to two reminders to them in your name. You can see who has accepted your invitations, send reminders, and delete your friends' email addresses on your invite history page. If your friend does not want us to keep their information, we will also remove it at their request by using this help page.

When you choose to share your information with marketers. You may choose to share information with marketers or electronic commerce providers that are not associated with Facebook through on-site offers. This is entirely at your discretion and we will not provide your information to these marketers without your consent.

To help your friends find you. By default, we make certain information you have posted to your profile available in search results on Facebook to help your friends find you. However, you can control who can see some of this information, as well as who can find you in searches, through your privacy settings. We also partner with email and instant messaging providers to help their users identify which of their contacts are Facebook users, so that we can promote Facebook to those users.

To give search engines access to publicly available information. We generally limit search engines' access to our site. We may allow them to access information set to the "everyone" setting (along with your name and profile picture) and your profile information that is visible to everyone. You can change the visibility of some of your profile information using your privacy settings. You can also prevent search engines from indexing your profile using your search settings.

To help improve or promote our service. Sometimes we share aggregated information with third parties to help improve or promote our service. But we only do so in such a way that no individual user can be identified or linked to any specific action or information.

To provide you with services. We may provide information to service providers that help us bring you the services we offer. For example, we may use third parties to help host our website, send out email updates about Facebook, remove repetitive information from our user lists, process payments, or provide search results or links (including sponsored links). These service providers may have access to your personal information for use for a limited time, but when this occurs we implement reasonable contractual and technical protections to limit their use of that information to helping us provide the service.

To advertise our services. We may ask advertisers outside of Facebook to display ads promoting our services. We may ask them to deliver those ads based on the presence of a cookie, but in doing so will not share any other information with the advertiser.

To offer joint services. We may provide services jointly with other companies, such as the classifieds service in the Facebook Marketplace. If you use these services, we may share your information to facilitate that service. However, we will identify the partner and present the joint service provider's privacy policy to you before you use that service.

To respond to legal requests and prevent harm. We may disclose information pursuant to subpoenas, court orders, or other requests (including criminal and civil matters) if we have a good faith belief that the response is required by law. This may include respecting requests from jurisdictions outside of the United States where we have a good faith belief that the response is required by law under the local laws in that jurisdiction, apply to users from that jurisdiction, and are consistent with generally accepted international standards. We may also share information when we have a good faith belief it is necessary to prevent fraud or other illegal activity, to prevent imminent bodily harm, or to protect ourselves and you from people violating our Statement of Rights and Responsibilities. This may include sharing information with other companies, lawyers, courts or other government entities.

Transfer in the Event of Sale or Change of Control. If the ownership of all or substantially all of our business changes, we may transfer your information to the new owner so that the service can continue to operate. In such a case, your information would remain subject to the promises made in any pre-existing Privacy Policy.

7. How You Can Change or Remove Information

Editing your profile. You may change or remove your profile information at any time by going to your profile page and clicking "Edit My Profile." Information will be updated immediately.

Delete uploaded contacts. If you use our contact importer to upload addresses, you can later delete the list on this help page. You can delete the email addresses of friends you have invited to join Facebook on your invite history page.

Deactivating or deleting your account. If you want to stop using your account you may deactivate it or delete it. When you deactivate an account, no user will be able to see it, but it will not be deleted. We save your profile information (connections, photos, etc.) in case you later decide to reactivate your account. Many users deactivate their accounts for temporary reasons and in doing so are asking us to maintain their information until they return to Facebook. You will still have the ability to reactivate your account and restore your profile in its entirety. When you delete an account, it is permanently deleted from Facebook. You should only delete your account if you are certain you never want to reactivate it. You may deactivate your account on your account settings page or delete your account on this help page.

Limitations on removal. Even after you remove information from your profile or delete your account, copies of that information may remain viewable elsewhere to the extent it has been shared with others, it was otherwise distributed pursuant to your privacy settings, or it was copied or stored by other users. However, your name will no longer be associated with that information on Facebook. (For example, if you post something to another user's profile and then you delete your account, that post may remain, but be attributed to an "Anonymous Facebook User.") Additionally, we may retain certain information to prevent identity theft and other misconduct even if deletion has been requested. If you have given third party applications or websites access to your information, they may retain your information to the extent

permitted under their terms of service or privacy policies. But they will no longer be able to access the information through our Platform after you disconnect from them.

Backup copies. Removed and deleted information may persist in backup copies for up to 90 days, but will not be available to others.

Non-user contact information. If a user provides your email address to us, and you are not a Facebook user but you want us to delete your address, you can do so on this help page. However, that request will only apply to addresses we have at the time of the request and not to any addresses that users provide to us later.

8. How We Protect Information

We do our best to keep your information secure, but we need your help. For more detailed information about staying safe on Facebook, visit the Facebook Security Page.

Steps we take to keep your information secure. We keep your account information on a secured server behind a firewall. When you enter sensitive information (such as credit card numbers and passwords), we encrypt that information using secure socket layer technology (SSL). We also use automated and social measures to enhance security, such as analyzing account behavior for fraudulent or otherwise anomalous behavior, may limit use of site features in response to possible signs of abuse, may remove inappropriate content or links to illegal content, and may suspend or disable accounts for violations of our Statement of Rights and Responsibilities.

Risks inherent in sharing information. Although we allow you to set privacy options that limit access to your information, please be aware that no security measures are perfect or impenetrable. We cannot control the actions of other users with whom you share your information. We cannot guarantee that only authorized persons will view your information. We cannot ensure that information you share on Facebook will not become publicly available. We are not responsible for third party circumvention of any privacy settings or security measures on Facebook. You can reduce these risks by using common sense security practices such as choosing a strong password, using different passwords for different services, and using up to date antivirus software.

Report Violations. You should report any security violations to us on this help page.

9. Other Terms

Changes. We may change this Privacy Policy pursuant to the procedures outlined in the Facebook Statement of Rights and Responsibilities. Unless stated otherwise, our current privacy policy applies to all information that we have about you and your account. If we make changes to this Privacy Policy we will notify you by publication here and on the Facebook Site Governance Page. You can make sure that you receive notice directly by becoming a fan of the Facebook Site Governance Page.

Consent to Collection and Processing in the United States. By using Facebook, you consent to having your personal data transferred to and processed in the United States.

Defined Terms. "Us," "we," "our," "Platform" and "Facebook" mean the same as they do in the Statement of Rights and Responsibilities. “Information” and “content” are used more generally and interchangeably here than in the Statement of Rights and Responsibilities unless otherwise limited by the context.

Appendix J: Facebook’s Privacy Explanation

Privacy on Facebook

Privacy is built around a few key ideas: You should have control over what you share. It should be easy to find and connect with friends. Your privacy settings should be simple and easy to understand.

On Facebook, there are three basic levels of privacy: **Friends**, **Friends of Friends**, **Everyone**. You also have a set of public information, which helps your friends find and connect with you: your Name, Profile Picture, Gender, and any Connections you've made. This includes the friends, networks and Pages you've chosen to connect to. You also always have control over who can see your Connections on your profile.

Facebook's Privacy Policy

You can read our full Privacy Policy here.

How others see you

If you are ever curious about how your friends see your profile, or what information Everyone can see, use this tool to see how people see you.

Recommended settings

We offer recommendations for your privacy settings based on the three levels of privacy: Friends, Friends of Friends, and Everyone.

We recommend **Everyone** be able to see information that will make it easier for friends to find, identify and learn about you. This includes basic information like your About Me description and your Website, as well as the default setting for posts that you create, like photo albums and status updates.

Remember, any information that's visible to Everyone may be seen by everyone on the internet. It will be visible to anyone viewing your profile, and Facebook Platform applications and websites that you use will be able to access it. Additionally, it may be visible in search engines or through RSS feeds.

Some information is more personal, so we recommend **Friends of Friends** be able to see that type of info. This includes the settings for your Birthday, Religious and Political views, and Photos and Videos of Me, which is all the photos and videos you've been tagged in.

We recommend that your contact information, like mobile phone number and email address, only be visible to **Friends**.

Understanding your settings

The Privacy Settings page is organized into the following sections:

Personal Information and Posts covers personal details like your birthday and political views, along with your content and content others have posted to your Wall. You control who is able to see each type of information.

Contact Information covers contact details like your mailing address and phone number. We recommend you make this visible to friends only.

Friends, Tags and Connections covers information and content that's shared between you and others on Facebook. This includes relationships (shared between you and the person you're in the relationship with), interests, and photos you're tagged in. These settings let you control who sees this information on your actual profile. However, it may still be visible in other places unless you remove it from your profile itself. For example, people will be able to see that you're connected to a Page if they're on the Page itself, and your relationships to other people may appear on the profiles of those people.

Application and Websites covers what information is available to the applications you and your friends use.

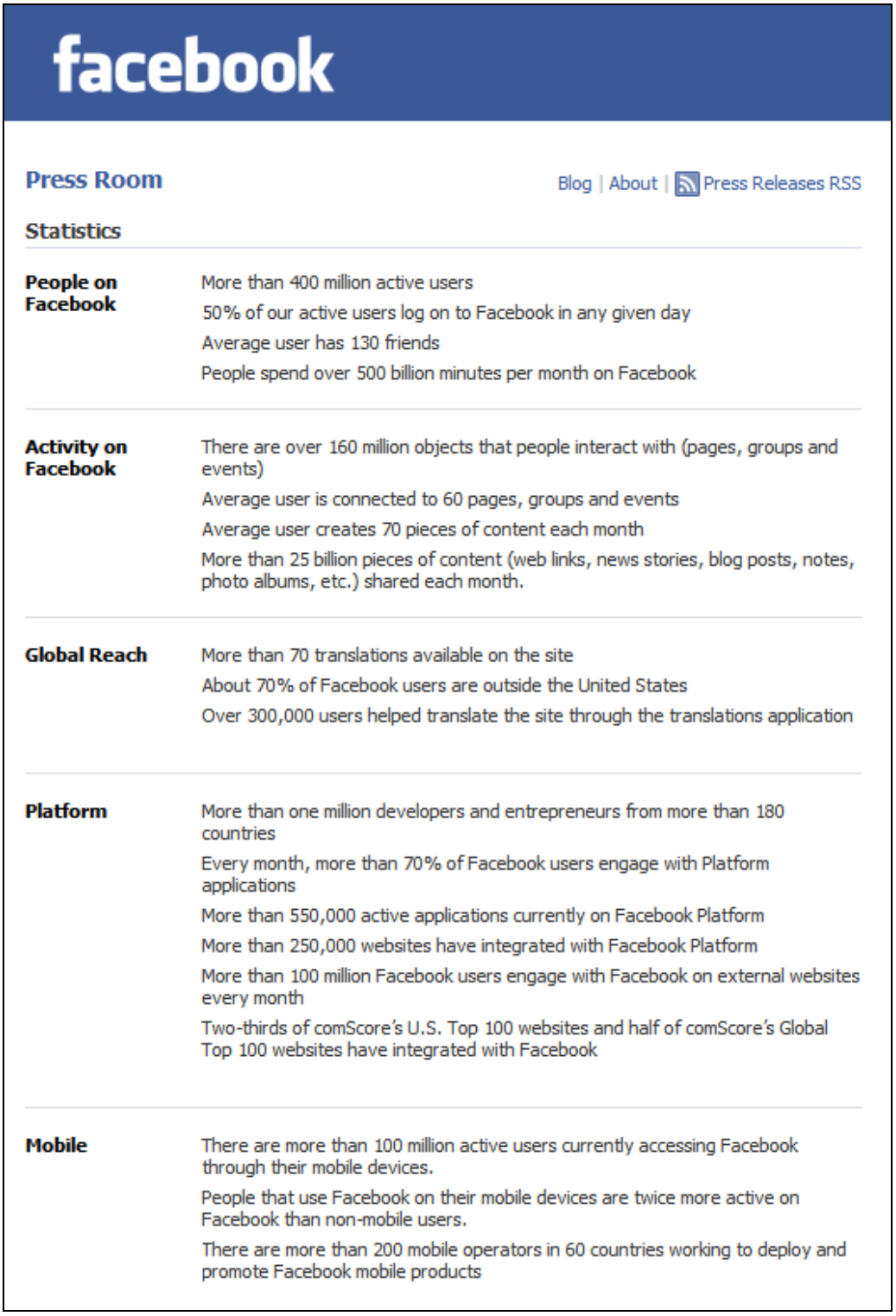
Search lets you control whether a public search listing is created for you. You can also control who can see your information in Facebook search.

Block List allows you to identify specific people who you want to prevent from interacting with you on Facebook.

Protecting your privacy

We are committed to protecting minors who use Facebook. Until their eighteenth birthday, minors will have their information limited to Friends of Friends and Networks.

Appendix K: Facebook's Press Room Statistics



facebook

Press Room

Blog | About | Press Releases RSS

Statistics

People on Facebook	More than 400 million active users 50% of our active users log on to Facebook in any given day Average user has 130 friends People spend over 500 billion minutes per month on Facebook
Activity on Facebook	There are over 160 million objects that people interact with (pages, groups and events) Average user is connected to 60 pages, groups and events Average user creates 70 pieces of content each month More than 25 billion pieces of content (web links, news stories, blog posts, notes, photo albums, etc.) shared each month.
Global Reach	More than 70 translations available on the site About 70% of Facebook users are outside the United States Over 300,000 users helped translate the site through the translations application
Platform	More than one million developers and entrepreneurs from more than 180 countries Every month, more than 70% of Facebook users engage with Platform applications More than 550,000 active applications currently on Facebook Platform More than 250,000 websites have integrated with Facebook Platform More than 100 million Facebook users engage with Facebook on external websites every month Two-thirds of comScore's U.S. Top 100 websites and half of comScore's Global Top 100 websites have integrated with Facebook
Mobile	There are more than 100 million active users currently accessing Facebook through their mobile devices. People that use Facebook on their mobile devices are twice more active on Facebook than non-mobile users. There are more than 200 mobile operators in 60 countries working to deploy and promote Facebook mobile products

Appendix L: Questionnaire

Questionnaire on Privacy Concerns and Risk Taking on Social Networking Sites

You are welcomed to take part in this questionnaire. This questionnaire consists of 17 questions and should only take less than 5 minutes to complete. The aim of this questionnaire is to identify users' privacy concerns and risk taking on social networking websites. Participation in this questionnaire is entirely voluntary and anonymous. No attempt will be made to associate you with the responses you provide. You can withdraw at any time simply by leaving this page. The results obtained from this questionnaire will be used in a Master's thesis at Lund University.

* Required

1. Age *

2. Gender *

- ○ Male
- ○ Female

3. Nationality *

4. General attitude *

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
To achieve something in life, one has to take risks	○	○	○	○	○
If there is a great chance of a reward, I will take high risks	○	○	○	○	○
It is important for me to protect my identity information	○	○	○	○	○
In general, I am concerned about my privacy when using the internet	○	○	○	○	○
I believe my identity information is well-protected online	○	○	○	○	○

5. Do you have your own profile on a social networking site (Facebook, MySpace, LinkedIn etc.) ? *

- ○ Yes
- ○ No

6. Roughly for how long have you been using social networking sites ? *

- ◯ < 1 year
- ◯ 1-2 years
- ◯ 2-3 years
- ◯ 3-4 years
- ◯ 4-5 years
- ◯ 5+ years

7. How frequently are you being active on social networking sites ? *

- ◯ Several times per day
- ◯ Several times per week
- ◯ Several times per month
- ◯ Several times per year
- ◯ Even less frequently

8. Roughly how many friends do you have in all of your social networking sites combined ? *

- ◯ 0 - 49
- ◯ 50 - 99
- ◯ 100 - 199
- ◯ 200 - 299
- ◯ 300 - 399
- ◯ 400 - 499
- ◯ 500+

9. I have my own profile on:

- ☐ LinkedIn
- ☐ MySpace
- ☐ Bilddagboken
- ☐ Friendster
- ☐ Hi5
- ☐ Lunarstorm

10. Do you have a Facebook account ? *

- ◯ Yes
- ◯ No

11. Which of the following information do you include in your Facebook profile ? *

	Yes	No	Yes, but it is fake or inaccurate
Full name	○	○	○
Birthday	○	○	○
Profile picture	○	○	○
E-mail address	○	○	○
Home town or city	○	○	○
Street address	○	○	○
Instant messenger account	○	○	○
Phone number	○	○	○
Religious/Political views	○	○	○
Relationship status	○	○	○
Sexual orientation	○	○	○
Interests/Activities	○	○	○
Education/Work information	○	○	○
Photographs of yourself	○	○	○

12. Roughly how often do you update your status message on Facebook ? *

- ○ Several times per day
- ○ Several times per week
- ○ Several times per month
- ○ Several times per year
- ○ Even less frequently

13. Roughly how many third-party applications (games, quizzes etc.) have you added to your Facebook account ? *

- ○ 0
- ○ 1 - 4
- ○ 5 - 9
- ○ 10 - 14
- ○ 15 - 19
- ○ 20+

14. Attitudes towards Facebook *

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
I am concerned about the information submitted to Facebook	○	○	○	○	○
I feel that the privacy of my personal information is well protected by Facebook	○	○	○	○	○
I am aware of Facebook's privacy settings	○	○	○	○	○
I have made a conscious decision regarding my Facebook account's privacy settings	○	○	○	○	○
I will accept a friend request from an unknown person on Facebook	○	○	○	○	○
I am aware of who can see my profile and the information in it on Facebook	○	○	○	○	○
Adding third-party applications in Facebook is not likely to be harmful	○	○	○	○	○
I am aware of Facebook's terms and conditions regarding my information	○	○	○	○	○
Facebook's terms and conditions affect my decision regarding whether or not to participate in it	○	○	○	○	○

15. I have changed my Facebook account's privacy settings (from the default settings). *

○ Yes

○ No

16. After completing this questionnaire, I have become more conscious of my use of social networking sites. *

○ Strongly disagree

○ Disagree

○ Neutral

○ Agree

○ Strongly agree

17. You are given a choice between the following two scenarios: 1. You receive an amount of money M with 100% certainty. 2. A coin is flipped to decide whether you receive $100 or nothing (50% certainty each). What amount of money M is required for you to choose the first scenario ? *

Note that there is no 'one right answer' for this question

« Back Submit

Powered by Google Docs

Report Abuse - Terms of Service - Additional Terms

Bibliography

Acquisti, A. and Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the facebook. *Privacy Enhancing Technologies*, pp. 36–58.

Anderson, D. R., Sweeney, D. J., Williams, T. A., Freeman, J. and Shoesmith, E. (2009). *Statistics for Business and Economics.* London: South-Western Cengage Learning.

Argyrous, G. (2005). *Statistics for Research* (2nd ed.). London: Sage.

Aune, S.P. (2007). *Facebook Blocked In Syria*. [Online] (Updated 24 November 2007) Available at: http://mashable.com/2007/11/24/facebook-blocked-in-syria/ [Accessed 14 May 2010].

BBC News. (2009). *Tehran blocks access to Facebook*. [Online] (Updated 24 May 2009) Available at : http://news.bbc.co.uk/2/hi/8065578.stm [Accessed 13 May 2010].

Bellman, S., Johnson, E.J., Kobrin, S.J. and Lohse, G.L. (2004). International differences in information privacy concerns: A global survey of consumers. *The Information Society*, 20 (5), pp. 313-324.

Benzie, R. (2007) . Facebook banned for Ontario staffers. *Toronto: TheStar.com*, [Internet] 3 May. Available at: http://www.thestar.com/News/article/210014 [Accessed 6 May 2010].

Blau, P. (1964). *Exchange and power in social life*. New York: Wiley

Boyd, D. (2004). Friendster and Publicly Articulated Social Networks. *Conference on Human Factors and Computing Systems (CHI 2004).* Vienna: ACM, April 24-29.

Boyd, D. (2006). Social Network Sites: My Definition. [Online] Available at: http://www.zephoria.org/thoughts/archives/2006/11/10/social_network-2.html [Accessed 16 March 2010].

Boyd, D. (2007). Why youth (heart) social network sites: The role of networked publics in teenage social life. *MacArthur Foundation Series on Digital Learning - Youth, Identity, and Digital Media Volume* (ed. David Buckingham). Cambridge, MA: MIT Press, pp. 119-142.

Boyd, D. M. and Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication, 13*(1), article 11. [Online] Available at: http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html [Accessed 25 April 2010]

Brady, H.E., Grand, S.A., Powell, M.A. and Schink, W. (2001). Access and confidentiality issues with administrative data, Studies of Welfare Populations: Data Collection and Research Issues. *National Academy of Sciences*, Washington, D.C, pp. 220-274.

Briggs, S.R. and Cheek, J.M. (1986). The role of factor analysis in the development and evaluation of personality scales. *Journal of Personality, 54*, pp. 106-48.

Bryman, A. (2008). *Social Research Methods* (3rd ed.). Oxford: Oxford University Press.

Bryman, A. and Bell, E. (2003). *Business Research Methods.* Oxford: Oxford University Press.

Bryman, A. and Bell, E. (2007). *Business Research Methods* (2nd ed.). Oxford: Oxford University Press.

Campbell, A. (1997). Relationship Marketing in Consumer Markets: A Comparison of Managerial and Consumer Attitudes About Information Privacy. *Journal of Direct Marketing, 11* (8), pp. 44-57.

CareerBuilder. (2009). *Forty-five Percent of Employers Use Social Networking Sites to Research Job Candidates, CareerBuilder Survey Finds*. [Online] (Updated 19 August 2009) Available at: http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?id=pr519&sd=8/19/2009&ed=12/31/2009&siteid=cbpr&sc_cmp1=cb_pr519_&cbRecursionCnt=2&cbsid=e44f93410c7840248a3b33a1dfc379e2-325757619-VF-4 [Accessed 28 April 2010].

Chetry, K. (2010). *Facebook posting allegedly led to house robbery*. [Online] (Updated 26 March 2010) Available at: http://amfix.blogs.cnn.com/2010/03/26/facebook-posting-allegedly-led-to-house-robbery/ [Accessed 13 May 2010].

Cho, H., Rivera, M. and Lim, S. S. (2009). A multinational study on online privacy: Global concerns and local responses. *New Media & Society, 11*(3), pp. 409-431.

Christofides, E., Muise, A. and Desmarais, S. (2009). Information Disclosure and Control on Facebook: Are They Two Sides of the Same Coin or Two Different Processes ?. *CyberPsychology & Behavior, 12*(3), pp. 341-345.

Chung, D. and Nam, C.S. (2007). An analysis of the variables predicting instant messenger use. *New Media and Society, 9* (2), pp. 212–234.

Clemons, E.K., Barnett, S. and Appadurai, A. (2007). The Future of Advertising and the Value of Social Network Websites*:* Some Preliminary Examinations. *Proceedings of the ninth international conference on Electronic commerce*, pp. 267 - 276

comScore. (2008). *Social networking explodes worldwide as sites increase their focus on cultural relevance*. [Online] Available at: http://www.comscore.com/Press_Events/Press_Releases/2008/08/Social_Networking_World_Wide [Accessed 26 March 2010].

ConsumerReports.org. (2010a). *7 things to stop doing now on Facebook.* [Online] Available at : http://www.consumerreports.org/cro/magazine-archive/2010/june/electronics-computers/social-insecurity/7-things-to-stop-doing-on-facebook/index.htm [Accessed 13 May 2010].

ConsumerReports.org. (2010b). *When sharing goes too far*. [Online] Available at : http://www.consumerreports.org/cro/magazine-archive/2010/june/electronics-computers/social-insecurity/when-sharing-goes-too-far/index.htm [Accessed 13 May 2010].

Creswell, J. W. (2007). *Qualitative inquiry and research design: Choosing among five traditions.* (2nd ed.). Thousand Oaks, CA*:* Sage.

Dickinson, A. (2010). YouTube, Facebook biggest work distractions – survey. *The Daily Telegraph,* [Internet] 12 March. Available at: http://www.dailytelegraph.com.au/business/youtube-facebook-biggest-work-distractions-survey/story-e6frez7r-1225839895757 [Accessed 13 May 2010].

Digital Buzz Blog (2010). Facebook: Facts & Figures For 2010. [Online] (Updated 22 March 2010) Available at: http://www.digitalbuzzblog.com/facebook-statistics-facts-figures-for-2010/ [Accessed 17 May 2010].

Dolgin, K.G., Meyer, L. and Schwartz, J. (1991). Effects of Gender, Target's Gender, Topic, and Self-Esteem on disclosure to Best and Midling Friends. *Sex Roles, 25* (9), pp. 311-329.

Dwyer, C., Hiltz, S.R. and Passerini, K. (2007). Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. *Proceedings of the Thirteenth Americas Conference on Information Systems*, (Keystone, Colorado).

EarthTimes. (2009). *Yearender: Vietnam is no longer friends with Facebook.* [Online] (Updated 21 December 2009) Available at : http://www.earthtimes.org/articles/show/300350,yearender-vietnam-is-no-longer-friends-with-facebook.html [Accessed 13 May 2010].

Ehrlinger, J., Gilovich, T. and Ross, L. (2005). Peering Into the Bias Blind Spot: People's Assessments of Bias in Themselves and Others. *Personality and Social Psychology Bulletin, 31*(5), pp. 680-692.

Ellison, N., Steinfeld, C. and Lampe, C. (2007). The benefits of Facebook 'friends': Exploring the relationship between college students' use of online social networks and social capital. *Journal of Computer-Mediated Communication*, 12(3).

Facebook (2010a). *Statistics*. [Online] Available at: http://www.facebook.com/press/info.php?statistics [Accessed 17 May 2010].

Facebook (2010b). *A guide to privacy on Facebook*. [Online] Available at: http://www.facebook.com/privacy/explanation.php [Accessed 17 May 2010].

Facebook (2010c). *Facebook's privacy policy.* [Online] (Updated 22 April 2010) Available at: http://www.facebook.com/policy.php [Accessed 17 May 2010].

Facebook (2010d). *Statement of Rights and Responsibilities*. [Online] (Updated 22 April 2010) Available at http://www.facebook.com/terms.php?ref=pf [Accessed 17 May 2010].

Farmer, A. D., Bruckner Holt, C. E., Cook, M. J. and Hearing, S. D. (2009). Social networking sites: a novel portal for communication. *Postgrad. Med. J, 85*(1007), pp. 455 - 459.

Fischer, F. (1998). Beyond Empiricism: Policy Inquiry in Postpositivist Perspective**.** *Policy Studies Journal*, *26* (1), pp. 129-146

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

Garbarino, E. and Strahilevitz, M. (2004). Gender differences in the perceived risk of buying online and efforts of receiving a site recommendation. *Journal of Business Research, 57*, pp. 768-775.

Gefen D. and Straub, D. W. (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, 1* (8), pp. 1-30.

Get Safe Online (2007). *Press release #8: Social networkers and wireless networks users provide "rich pickings" for criminals.* [Online] GetSafeOnline.org. Available at http://www.getsafeonline.org/nqcontent.cfm?a_id=1469 [Accessed 3 May 2010]

Google. (2009). *Privacy Policy.* [Online] (Updated 11 March 2009) Available at: http://www.google.com/privacypolicy.html [Accessed 20 May 2010].
Govani, T. and Pashley, H. (2005). Student Awareness of the Privacy Implications while Using Facebook. [Online] Available at: http://lorrie.cranor.org/courses/fa05/tubzhlp.pdf [Accessed 14 May 2010].

Gravetter, F. J. and Wallnau, L. B. (2009). *Statistics for the Behavioral Sciences* (8th ed). Belmont, CA: Wadsworth Publishing

Griffith, S., and Liyanage, L. (2008). An Introduction to the Potential of Social Networking Sites in Education. *Emerging Technologies Conference 2008*, Paper 9. [Online] Available at: http://ro.uow.edu.au/cgi/viewcontent.cgi?article=1008&context=etc08 [Accessed 12 May 2010]

Gross, R. and Acquisti, A. (2005). Information revelation and privacy in online social networks (The Facebook case). *ACM Workshop on Privacy in the Electronic Society*, pp. 71–80.

Hammersley, M. and Gomm, R. (1997)**.** Bias in Social Research, *Sociological Research Online 2* (1). [Online] Available at: http://www.socresonline.org.uk/2/1/2.html [Accessed 22 March 2010].

Harris, L. and Rae, A. (2009). Social Networks: the future of marketing for small businesses. *Journal of Business Strategy, 30* (5), pp. 24-31.

Harrison, R. and Thomas, M. (2009). Identity in Online Communities: Social Networking Sites and Language Learning. *International Journal of Emerging Technologies, 7* (2), pp. 109-124.

Homans, G.C. (1958). Social Behavior as Exchange. *American Journal of Sociology, 63*(6), pp. 597–606.

Hoofnagle, C.J., King, J., Li, S. and Turow, J. (2010). How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies? April 14, 2010. Available at SSRN: http://ssrn.com/abstract=1589864 [Accessed 17 May 2010].

Howitt, D. and Cramer, D. (2005). *Introduction to SPSS in Psychology.* Essex, England: Pearson Education.

Hoy, M.G. and Milne, G. (2010). Gender Differences in Privacy-Related Measures for Young Adult Facebook Users. *Journal of Interactive Advertising, 10* (2), pp. 28-45.

IBM (2010). *A Global Innovation Outlook report: Security, Privacy and Web 2.0.* [Online] IBM. Available at: http://www.ibm.com/ibm/files/V808675J59502E65/ibm_gio_web2point0_brochure_hi.pdf [Accessed 4 May 2010]

Israel, M. and Hay, I. (2006). *Research ethics for social scientists: between ethical conduct and regulatory compliance*. London: Sage.

Jacobsson, C. (2009). *Arbetsgivare kollar jobbsökande på nätet*. [Online] (Updated 29 January 2009) Available at: http://www.dn.se/ekonomi/arbetsgivare-kollar-jobbsokande-pa-natet-1.485571 [Accessed 28 April 2010].

Jamieson, S. (2004). Likert scales: how to (ab)use them. *Medical Education, 38* (12), pp. 1217-1219

Joinson, A. N. (2008). Looking at', 'Looking up' or 'Keeping up with' people? Motives and uses of Facebook. *CHI 2008 Proceedings*, pp. 1027–1036.

Jones, H. and Soltren, J.H. (2005). Facebook: Threats to Privacy. [Online] Available at: http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall05-papers/facebook.pdf [Accessed 15 April 2010].

Karmarkar, U.S. (1978). Subjectively weighted utility: A descriptive extension of the expected utility model. *Organizational Behavior and Human Performance, 21* (1), pp. 61-72.

Kazeniac, A. (2009). *Social Networks: Facebook Takes Over Top Spot, Twitter Climbs.* [Online] (Updated 9 February 2009) Available at: http://blog.compete.com/2009/02/09/facebook-myspace-twitter-social-network/ [Accessed 17 May 2010].

Kelly, S. (2008). *Identity 'at risk' on Facebook.* [Online] (Updated 1 May 2008) Available at: http://news.bbc.co.uk/2/hi/programmes/click_online/7375772.stm [Accessed 7 April 2010].

Kvale, S. and Brinkmann, S. (2009). *Interviews: Learning the Craft of qualitative research interviewing* (2nd ed.). Thousand Oaks, CA: Sage.

Lampe, C., Ellison, N. and Steinfeld, C. (2006). A Face(book) in the crowd: Social searching vs. social browsing. *Proceedings of the 2006 20th Anniversary Conference on Computer Supported Cooperative Work*, pp. 167-170. New York: ACM Press.

Lampe, C., Ellison, N. and Steinfeld, C. (2007). A familiar Face(book): Profile elements as signals in an online social network. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 435-444. New York: ACM Press.

Lang, M., Devitt, J., Kelly, S., Kinneen, A., O'Malley, J. and Prunty, D. (2009). Social Networking and Personal Data Security: A Study of Attitudes and Public Awareness in Ireland. *In Proceedings of International Conference on Management of e-Commerce and e-Government (ICMeCG), Nanchang, China, September 16-19. IEEE Computer Society*, pp. 486-489.

Legal and General (2009). *Digital Criminal report.* [Online] Legal and General. Available at:

http://www.legalandgeneralmediacentre.com/imagelibrary/downloadMedia.ashx?MediaDetailsID=366 [Accessed 14 May 2010]

Lewis, K., Kaufman, J. and Christakis, N. (2008). The taste for privacy: An analysis of college student privacy settings in an online social network. *Journal of Computer-Mediated Communication, 14* (1), pp. 79–100

Litwin, M.S.. (1995). *The survey kit: TSK 7. How to measure survey reliability and validity*. Thousand Oaks, CA: Sage.

Lynch, P. D. and Beck J.C. (2001). Profiles of Internet buyers in 20 countries: Evidence for region-specific strategies. *Journal of International Business Studies*, *32* (4), pp.725 - 748.

MacDonald, E. (2009). *China's Facebook Status: Blocked.* [Online] (Updated 8 July 2009) Available at: http://blogs.abcnews.com/theworldnewser/2009/07/chinas-facebook-status-blocked.html [Accessed 6 May 2010].

Manago, A. M., Graham, M. B., Greenfield, P. M. and Salimkhan, G. (2008). Self-presentation and gender on MySpace. *Journal of Applied Developmental Psychology*, *29*, pp. 446-458.

Matyszczyk, C (2009). *Facebook post gets NFL Eagles' worker fired*. [Online] (Updated 9 March 2009) Available at: http://news.cnet.com/8301-17852_3-10192227-71.html [Accessed 13 May 2010].

Mayer, R. C., Davis, J. H. and Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review*, *20*(3), pp. 709-34.

Maynard, M. and Taylor, C. (1996).A comparative analysis of Japanese and U.S. attitudes toward direct marketing. *Journal of Direct Marketing, 10* (1), pp. 34–44.

Metzger, M., J. (2004). Privacy, Trust and Disclosure: Exploring Barriers to Electronic Commerce. *Journal of Computer-Mediated Communication*, *9* (4).

Milne, G R. and Culnan, M.J. (2004). Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices. *Journal of Interactive Marketing, 18* (3), pp. 15-29.

Milne, G. R., Beckman, J. and Taubman, M. L. (1996). Consumer Attitudes Towards Privacy and Direct Marketing in Argentina. *Journal of Direct Marketing, 10* (1), pp. 22-33.

Mohtasebi, A. and Borazjani, P.M. (2010). Privacy Concerns in Social Networks and Online Communities. *VALA2010 Proceedings*.

Moore, V. (2009). The fake world of Facebook and Bebo: How suicide and cyber bullying lurk behind the facade of 'harmless fun'. *MailOnline*, [Internet] 4 August. Available at: http://www.dailymail.co.uk/femail/article-1204062/The-fake-world-Facebook-Bebo-How-suicide-cyber-bullying-lurk-facade-harmless-fun.html#ixzz0nonbyOyV [Accessed 13 May 2010].

Murados, N. (2008). *Social Networking vs. Privacy: Research into Privacy Implications in a Social Networking Site Context*. M.Sc. thesis, Brunel University.

Norris, N. (1997). Error, bias and validity in qualitative research. *Educational Action Research, 5* (1), pp. 172-176.

Nunnally, J., (1978). *Psychometric theory*. New York: McGraw Hill.

Ofcom (2008a). *Social networking: a quantitative and qualitative research report into attitudes, behaviours and use.* [Online] Office of Communications. Available at: http://www.ofcom.org.uk/advice/media_literacy/medlitpub/medlitpubrss/socialnetworking/report.pdf [Accessed 3 May 2010].

Ofcom (2008b). *Annex 3: Social Networking Qualitative research report.* [Online] Office of Communications. Available at: http://www.ofcom.org.uk/advice/media_literacy/medlitpub/medlitpubrss/socialnetworking/annex3.pdf [Accessed 3 May 2010].

Opsahl, K. (2010). *Facebook's Eroding privacy policy: A Timeline.* [Online] (Updated 28 April 2010) Available at: http://www.eff.org/deeplinks/2010/04/facebook-timeline [Accessed 14 May 2010].

Paine, C., Reips, U-D., Stieger, S., Joinson, A. and Buchanan, T. (2007). Internet users' perceptions of 'privacy concerns' and 'privacy actions'. *International Journal of Human-Computer Studies, 65* (6), pp. 526-536.

Pallant, J. (2007). *SPSS Survival Manual* (3rd ed.). Berkshire, England: McGraw-Hill Education

Pan, Y. and Zinkhan, G.M. (2006). Exploring the impact of online privacy disclosures on consumer trust. *Journal of Retailing, 82*(4), pp 331-338.

Patel, B. (2007). *Social networking sites cause distraction for college students.* [Online] (Updated 19 April 2010) Available at: http://www.crcconnection.com/2.9559/social-networking-sites-cause-distraction-for-college-students-1.1369506 [Accessed 13 May 2010].

Pfeil, U., Arjan, R. and Zaphiris, P. (2009). Age differences in online social networking – A study of user profiles and the social capital divide among teenagers and older users in MySpace. *Computers in Human Behavior, 25*(3), pp. 643-654.

Phillips, S. (2007). *A brief history of Facebook.* [Online] Available at: http://www.guardian.co.uk/technology/2007/jul/25/media.newmedia [Accessed 14 May 2010].

Ratnasingham, P. (1999). Risks in low trust among trading partners in electronic commerce. *Computers and Security, 18* (7), pp. 587-592.

Robinson, J.P., P.R. Shaver and L.S. Wrightsman. (1991). Criteria for Scale Selection and Evolution. In J. P. Robinson, P. R. Shaver, and L. S. Wrightsman (Eds.). *Measures of personality and social psychological attitudes.* San Diego, CA: Academic Press.

Rodgers, S. and Harris, M.A. (2003). Gender and e-Commerce: An Exploratory Study, *Journal of Advertising Research, 43*(3), pp. 322–329.

Royal Pingdom (2009). Study: Males vs. females in social networks. [Online] (Updated 27 November 2009) Available at: http://royal.pingdom.com/2009/11/27/study-males-vs-females-in-social-networks/ [Accessed 14 May 2010].

Royal Pingdom (2010). Study: Ages of social network users. [Online] (Updated 16 February 2010) Available at: http://royal.pingdom.com/2010/02/16/study-ages-of-social-network-users/ [Accessed 14 May 2010].

Salaway, G. and Caruso, J. B. (2008). *The ECAR study of undergraduate students and information technology, 2008.* [Online] ECAR. Available at: http://net.educause.edu/ir/library/pdf/ERS0808/RS/ERS0808w.pdf [Accessed 11 May 2010].

Schonfeld, E. (2009). *Facebook Is Now the Fourth Largest Site In The World.* [Online] (Updated 4 August 2009) Available at: http://techcrunch.com/2009/08/04/facebook-is-now-the-fourth-largest-site-in-the-world/ [Accessed 17 May 2010].

Seale, C. (1999). *The quality of qualitative research*. London: Sage.

Seock, Y. and Chen-Yu, J.H. (2007). Website evaluation criteria among U.S. college student consumers with different shopping orientations and Internet channel usage. *International Journal of Consumer Studies, 31* (3), pp. 204-12.

Sheehan, K.B. (1999). An Investigation of Gender Differences in On-Line Privacy Concerns and Resultant Behavior. *Journal of Interactive Marketing, 13* (4), pp. 24-38.

Smith, J (2009). *Latest Data on Facebook's US Growth by Age and Gender – November 2, 2009.* [Online] Available at: http://www.insidefacebook.com/2009/11/02/latest-data-on-facebook%E2%80%99s-us-growth-by-age-and-gender-%E2%80%93-november-2-2009/ [Accessed 12 May 2010].

Steel, J. L. (1991). Interpersonal correlates of trust and self-disclosure. *Psychological Reports, 68*, pp. 1319-1320.

Strater, K. and Richter, H. (2007). Examining Privacy and Disclosure in a Social Networking Community. *Symposium On Usable Privacy and Security (SOUPS).* Pittsburgh

Streiner, D.L. and Norman, G.R. (1989). *Health Measurement Scales A Practical Guide to Their Development and Use.* New York: Oxford University Press, Inc.

Stutzman, F. (2006). An evaluation of identity-sharing behavior in social network communities. *iDMAa Journal, 3* (1), pp. 1-7.

Taylor, C. (2010). *Increase Website Traffic Through Facebook marketing.* [Online] (Updated 22 January 2010) Available at: http://www.socialmediatoday.com/SMC/168612 [Accessed 13 May 2010].

The Harris Poll (2010). *Adults in Largest European Countries, U.S. and China Concerned Over Online Security*. [Online] Harris Interactive. Available at: http://www.harrisinteractive.com/NewsRoom/HarrisPolls/tabid/447/ctl/ReadCustom%20Default/mid/1508/ArticleId/234/Default.aspx [Accessed 17 May 2010].

Thelwall, M. (2008). Social networks, gender and friending: An analysis of MySpace member profiles. *Journal of the American Society for Information Science and Technology*, 59 (8), pp. 1321–1330

Thibaut, J.W. and Kelley, H.H. (1959). *The social psychology of groups*. New York: Wiley.

TT (2009). *Åtalas efter erkännande på Facebook.* [Online] (Updated 17 December 2009) Available at: http://www.dn.se/nyheter/sverige/atalas-efter-erkannande-pa-facebook-1.1015312 [Accessed 7 April 2010].

TT (2010a). *Jagar bedragare via Facebook.* [Online] (Updated 11 February 2010) Available at: http://www.dn.se/nyheter/sverige/jagar-bedragare-via-facebook-1.1043070 [Accessed 7 April 2010].

TT (2010b). *Bitsk tjuv fast på Facebook.* [Online] (Updated 11 February 2010) Available at: http://www.dn.se/nyheter/sverige/bitsk-tjuv-fast-pa-facebook-1.1036262 [Accessed 7 April 2010].

Tufekci, Z. (2008). Can You See Me Now? Audience and Disclosure Management in Online Social Network Sites. *Bulletin of Science and Technology Studies*, *28*(1), pp. 20-36.

Tuunainen, V.K., Pitkänen, O. and Hovi, M. (2009). Users' Awareness of Privacy on Online Social Networking Sites - Case Facebook Company. *BLED 2009 Proceedings*: Paper 42.

Utz, S. and Krämer, N. (2009). The privacy paradox on social network sites revisited: The role of individual characteristics and group norms. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 3*(2), article 1. [Online] Available at: http://cyberpsychology.eu/view.php?cisloclanku=2009111001&article=1 [Accessed 25 April 2010]

Wallén, G. (1996). *Vetenskapsteori och forskningsmetodik*, 2:a upplagan. Lund: Studentlitteratur.

White, H. (1980). A Heteroskedasticity-Consistent Covariance Matrix Estimator and a Direct Test for Heteroskedasticity. *Econometrica,* 48 (4), pp. 817–838.

Wixom, B.H and Watson, H.J. (2001). An empirical investigation of the factors affecting data warehousing success. *MIS Quarterly, 25* (1), pp. 16-41.

Yalta, A.T. and Yalta, A.Y. (2007). Gretl 1.6.0 and its Numerical Accuracy. *Journal of Applied Econometrics*, 22 (4), pp. 849 – 54.

Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents**.** *Journal of Consumer Affairs, 43*(3), pp. 389-418.