Risk Perceptions on Social Networking Sites: An Investigation of Age and Other Factors

Aideen M. Keaney

A dissertation submitted to
The Faculty of Engineering Mathematics and Science
of
Trinity College
The University of Dublin
For the award of
Doctor of Philosophy
2012

DECLARATION

I declare that this thesis has not been submitted as an exercise for a degree at this or any other university and it is entirely my own work.

I agree to deposit this thesis in the University's open access institutional repository or allow the library to do so on my behalf, subject to Irish Copyright Legislation and Trinity College Library conditions of use and acknowledgement.

_____ _____

Signature of Candidate Date

SUMMARY

Since the mid 2000's, social networking sites (SNSs) such as Facebook and Bebo have seen phenomenal growth. These sites provide many benefits for users, but there are risks in using them. To date most of the studies that have examined the risks associated with SNSs have examined their prevalence and impact on adolescents and to lesser extent emerging adults as these age groups have been seen as the primary users of SNSs. However, recent evidence shows that the growth in the numbers using SNSs is not only continuing, but is happening in the older age groups. As far as it is known, this is the first study of its kind to examine risk prevalence on SNSs across a number of age groups, including adults. It is also the first study to examine users' perception of these risks. The following is a summary of the methods used and the major findings of this dissertation.

The research approach combines quantitative and qualitative research methods, using a mixed method sequential explanatory design. The quantitative first phase of the design is a survey of 551 adolescents (ages 12-17), 1,044 emerging adults (ages 18-25) and 156 working adults. The survey measures users' risks perceptions with respect to SNSs. The second, qualitative phase expands on the results found in the survey and looks for explanations as to why certain risk perceptions exist. The second phase consists of 15 semi-structured interviews with the emerging adult cohort and four focus groups interviews with the adolescent group.

The findings from this research in some cases confirm those found in other studies and in a number of instances contradict those found in previous work. This study also makes a number of new findings about risk perception and SNSs. While all users show an awareness and a recognition of the risks on SNSs, most users exhibit a lack of concern about the risks on SNSs and do not think that these negative events are likely to happen to them. While it might be expected that users would be most concerned and have highest risk perceptions for the serious threatening risks such as cyberbullying and meeting strangers, this is not the case and users express higher levels of concern about and perceive greater threats from risks to their reputation. For most of the negative events on SNSs, when compared to the other age groups, adolescents perceive themselves to be at a higher risk, show higher levels of awareness, are more concerned and perceive the consequences of risks to be higher. The qualitative interviews and focus group discussions highlight some misconceptions with regard to these risks and in particular users' lack of awareness

of the scale and scope of the audience on SNSs and how easily their personal information can be accessed and harvested.

This research examines why some users perceive themselves to be at high personal risk on SNSs and others do not. Three factors are significant predictors of the likelihood of high personal risk perceptions: prior experience of the risk, concern about the risk and age group. The most significant predictor of high personal risk perception is prior experience. Although suggested as significant predictors of risk perception by previous research, both knowledge of risk and controllability of risk show small effects on the likelihood of high personal risk perceptions. Again, contrary to the findings of previous risk perception studies, gender does not emerge as a significant predictor for any of the risk categories.

This study highlights a number of behaviours on SNSs that could make users more vulnerable to risk. Users tend to underestimate the amount of time they spend on SNSs and may be unaware of the distracting aspects of SNSs. In contrast to some previous studies, this study has found that the majority of respondents have restricted their privacy settings, indicating that SNS users may be becoming more aware and concerned about the privacy risks on SNSs. However, similar to the findings of other studies, this concern does not extend to restricting the amount of information respondents disclose. Users continue to reveal substantial amounts of personal information. Adolescents are less likely than the other age cohorts studied to reveal personal contact information, but overall older adolescents and emerging adults reveal significantly more information than the other age cohorts studied. The qualitative interviews indicate that SNS users tend to be guided by the SNS company, accepting the default privacy settings and filling in the information categories provided on the SNS.

To date, most studies have addressed the prevalence of these risks for children and adolescents. This study differs as it examines the prevalence of risks over a number of age cohorts and highlights that many of these risks have been experienced by emerging adults and adults. This study addresses a number of gaps in the extant literature and the research findings provide both a theoretical and a practical contribution to this field. The results of the research include a preliminary framework that captures the factors that influence risk perception on SNSs. The findings of this research can inform not only further studies of SNS risks, but also studies of other Internet and technology related risks.

ACKNOWLEDGMENTS

I would like to take this opportunity to thank a number of people who have helped me during the course of writing this dissertation.

To my husband Charlie, who is my rock.

To my mother and late father, who have supported me throughout my life. My father was always proud of my achievements. This thesis is dedicated to his memory.

I wish to thank my supervisor, Professor Frank Bannister, for his exceptional guidance, support and assistance throughout the research process.

My colleagues in the School of Computer Science and Statistics and in particular those in the Department of Statistics have provided support and encouragement throughout this process. In particular I would like to thank Professor Cathal Walsh for his help with the quantitative analysis, and especially Professor Myra O'Regan who provided not only expert advice but is a true and supportive friend.

To Olivia Lombard, thank you for listening and for all your encouragement and genuine help and friendship.

Finally, my thanks to everyone who took part in this research and who gave so willingly of their time.

TABLE OF CONTENTS

CHAPTER 3: LITERATURE REVIEW SOCIAL NETWORKING SITES

CHAPTER 4: METHODOLOGY

CHAPTER 6: DISCUSSION

CHAPTER 7: CONCLUSIONS

BIBLIOGRAPHY

APPENDICES

LIST OF FIGURES

LIST OF TABLES

LIST OF CHARTS

1 Introduction and Overview

1.1 Background to Research

In his book, The Facebook Effect, David Kirkpatrick (2010) describes how one person on Facebook mobilised others in a mass demonstration. In late 2007, President Hugo Chavez of Venezuela was negotiating with the Revolutionary Armed Forces of Colombia, also known as FARC, for the release of some hostages. At the time FARC held over 700 hostages. One such hostage was a four year old boy called Manuel. His mother had been kidnapped in 2002 and Manuel had been born in captivity. In January 2008, FARC said they were going to release Manuel, but it later emerged that FARC did not actually have him; Manuel had become ill two years earlier and FARC had left him with a peasant family. This caused a lot of outrage amongst the Columbian people, one person Oscar Morales wanted to show his annoyance and he turned to Facebook. He created a Facebook group against FARC. He called the group one million voices against FARC "*Un Millon de Voces Contra Las Farc*" and the page contained four requests: no more kidnappings, no more lies, no more killings, no more FARC. Morales created the group at midnight on January 4th 2008 and made the group public so that any Facebook member could join. He invited all 100 of his Facebook friends. By 9am the next morning, the group had 1,500 members. Two days later there were 8,000 members. Membership grew exponentially with 100,000 members by the end of the first week. A consensus was emerging that the Facebook group should go public and members convinced Morales to organise a demonstration. The group decided to stage a national march against FARC in a number of cities in Columbia on February 4th, one month after the group was formed. Members of the Facebook group in Miami, Buenos Aires, Madrid, Paris and elsewhere suggested that the march should be global. What happened was astonishing and showed the power of Facebook to mobilise people. On February 4th an estimated 10 million people marched against FARC in hundreds of cities in Columbia and a further 2 million marched in cities around the world. A single post on a Facebook group led to one of the largest demonstrations ever seen, all organised within a month. In the past, people who had organised protests against FARC remained anonymous, this protest was different as more that 500,000 people showed their real names and faces on the Facebook group. Facebook allowed these protesters to feel secure about showing their disgust. In light of this protest, FARC released some hostages. It still holds around 200 hostages but membership of

FARC has dropped from 40,000 to 7,000 and it has retreated further underground (Pérez, 2008, Kirkpatrick, 2010, Lichtenstein, 2010).

There are numerous examples cited in the press, particularly in relation to the Arab Spring of 2010/2011, of how Facebook and other social networking sites (hereafter referred to as SNSs) have facilitated communication and enabled the mobilisation of individuals to enact political change. The press referred to them as "*twitter revolutions*". Some journalists have argued that SNSs were a critical factor in these uprisings and this has led to a renewed debate regarding the role of the Internet in political mobilisation. The jury is still out in this regard with some arguing that SNSs can be an enabler of political change (Grossman, 2006, Shirky, 2011) whilst others suggest that SNSs have little political impact (Morozov, 2009, Gladwell, 2010, Morozov, 2011).

Regardless of whether or not SNSs and social media can be touted as an agent for political change, SNSs have made a large impact on modern society in a relatively short period of time. Web 2.0 technologies, such as social networking sites, wikis and blogs, allow users to easily create their own content, share this content and encourage collaboration with other users. This has changed the way people use the Internet. The first SNSs, Classmates.com (focussed on ties with former school mates) and SixDegrees.com (which focussed on indirect ties) were launched as early as the mid 1990's. However the SNSs that are in common use today were only launched to the general public in the mid 2000's. The growth of these SNSs has been staggering with Facebook (as of July 2011) reporting 750 million active users worldwide. Facebook has over 2 million users in Ireland (Socialbakers, 2011), an estimated 43% of the population. The business orientated SNS LinkedIn (as of August 2011) reports a membership of 120+ million professionals worldwide with nearly 500,000 Irish business users. The popularity of particular SNSs has changed over time, with some dropping by the wayside (e.g. MySpace and Bebo). At the time of writing Facebook is currently the most popular SNSs worldwide and is the second most accessed website after Google. Although these sites were initially thought of as a place for the young, this trend is changing and many SNSs are now dominated by the 35-44 age group (Pingdom, 2010), 62% of Facebook users in Ireland are currently over 24 (Socialbakers, 2011).

The emergence of smart phones has made access to the Internet and SNSs seamless and users can access these sites anyplace and anytime. As some mobile phone providers are

now giving access to SNSs for free, users are increasingly using their mobile phones to connect to SNSs. This raises concerns for children's access to SNSs as children now have increasing opportunities to access the Internet and SNSs unsupervised.

Some SNSs have been developed for a specific purpose, such as for sharing photographs (e.g. flickr and picasa), sharing videos (e.g. YouTube), for professionals (e.g. LinkedIn) and for special interest groups (e.g. dogster and catster). The most well-known SNSs have focussed on interpersonal communication e.g. MySpace, Facebook, Bebo and and Twitter. On these SNSs users can create their own online page or "*profile*", they can display an online network of contacts called "*friends*" and they can communicate with these friends privately on a one-to-one basis (like e-mail) or in a more public way by posting a comment on a "*public wall*" (boyd and Ellison, 2007, OFCOM, 2008).

SNSs have led to a new form of electronic communication amongst a social network of friends and acquaintances. A form of communication, that is for some, surpassing email. Messages can be spread with an almost viral like quality on SNSs, not only can the reach of messages be extensive on SNSs, the message can be spread quickly. What was previously in the hands of large media and print organisations has now been moved into the hands of ordinary individuals. The primary reason, however, that most people use SNSs is to communicate and keep in contact with their existing family and friends (Acquisti and Gross, 2006, boyd, 2007, Ellison *et al.*, 2007, Lenhart and Madden, 2007, Anchor, 2008a, OFCOM, 2008, Young and Quan-Haase, 2009, Livingstone *et al.*, 2010b, O'Neill *et al.*, 2011).

Although many users use SNSs as a distraction and as a form of entertainment, SNSs provide many other social benefits including identity development, enhancing social capital and enhancing social support. On SNSs, users attempt to construct a representation of themselves that is affirmed by their peers. Many adolescents, in particular, gain much pleasure in creating this online identity (Livingstone, 2008, Livingstone and Brake, 2010). Positive feedback from friends on SNSs has been shown to increase social self esteem and well being (Valkenburg *et al.*, 2006). SNSs can also enhance social capital and in particular bridging social capital, i.e. the extent to which users are integrated into a particular community, their willingness to support the community, and the extent to which these experiences broaden their social horizons or worldview (Ellison *et al.*, 2007). Social support is another important benefit of interacting in SNSs, the relative anonymity that

SNSs provide allows users to more easily share and seek advice from peers and others (Valkenburg and Peter, 2009).

But being part of a large community on SNSs where users share many personal details about themselves can have some drawbacks. The threatening risks on SNSs have been well publicised by the media and Internet safety awareness campaigns and are the subject of many research studies particularly with children and adolescents. These can be categorised as risks to the health and safety of the user and include risks such as cyberbullying and harassment, stalking, meeting a stranger that was initially met online, and hurtful postings, etc. There is also evidence of self-harm and suicide attempts motivated by SNSs. Due to the large audiences on SNSs and the fact that messages can be spread quickly, fraudsters have moved on to SNSs and this has led to increases in the amount of phishing and malware attacks on SNSs. These criminals take full advantage of the social aspects of SNSs, with many of these attacks appearing to come from friends, thus making users more likely to trust the messages and click on links that allow them to become infected.

One area that has gathered much interest from both the media and academic community is the privacy implications of SNSs and the large quantities of personal information that users reveal on SNSs. Numerous studies have found that SNS users are revealing substantial amounts of personal information (Gross and Acquisti, 2005, Jones and Soltren, 2005, Acquisti and Gross, 2006, Stutzman, 2006, Anchor, 2008b, Hinduja and Patchin, 2008b, Kolek and Saunders, 2008, Tufekci, 2008, Christofides *et al.*, 2009, Fogel and Nehmad, 2009, WEBWISE, 2009, Young and Quan-Haase, 2009, Nosko *et al.*, 2010). As SNSs are in the business of encouraging users to share as much personal information as possible they do not promote their privacy controls or make them intuitive to use (Bonneau and Preibusch, 2010, Brandtzæg *et al.*, 2010, Schneier, 2010, Furnell and Botha, 2011). Facebook in particular has been at the centre of many privacy debates. Their business objective has been to get users to share as much personal information as possible and Facebook only modify privacy controls when there is intense pressure from users. The goal and purpose of Facebook is to increase the efficiency and transparency of communication and this challenges conventional notions of privacy. The CEO of Facebook, Mark Zuckerberg, contends that privacy is no longer a social norm and the rise of SNSs means that people no longer have an expectation of privacy (Johnson, 2010). The privacy policy for Facebook (accessed June 2011) further emphasises this and clearly

states that they cannot and do not guarantee that content users post on the site will not be viewed by unauthorized persons and they are not responsible for circumvention of any privacy settings or security measures contained on the site. Furthermore, they warn that even after removal, copies of user's content may remain viewable in cached and archived pages. Researchers have found that users tend to be unaware of the potential audiences on SNSs (Lampe *et al.*, 2006, Lampe *et al.*, 2008, Livingstone, 2008, Phippen *et al.*, 2009, Pike *et al.*, 2009, West *et al.*, 2009) and how easy it is, regardless of privacy settings, to extract information from the personal profiles and social graph data available on SNSs (Chau *et al.*, 2007, Mislove *et al.*, 2007b, Krishnamurthy and Wills, 2008, Bonneau *et al.*, 2009, Balduzzi *et al.*, 2010). Users are unaware that even when data is presented in an anonymous form that it can be re-identified (Backstrom *et al.*, 2007, Narayanan, 2009). For example, when users are careful not to expose their identities it is possible through face re-identification technologies, such as the Facebook app, Photo Finder[1] or through harvesting information from a number of social network profiles to identify people (Hogg and Adamic, 2004, Liu and Maes, 2005).

Facebook regularly adds new features to encourage users to reveal even more personal information. One such feature, launched in April 2010, is the Open Graph Protocol which allows people to integrate their personal WWW page into the Facebook social graph. This is targeted to WWW pages representing profiles of real-world things, such as movies, sports teams, celebrities, restaurants etc. When an Open Graph tag is included on a WWW page, it makes the page equivalent to a Facebook Page. This means when a user clicks on an Open Graph tag, i.e. a "*Like*" button on a page, a connection is made between the WWW page and the user. The page will appear in the "*Likes and Interests*" section of the user's profile, and the website has the ability to publish updates to the user. This too has privacy implications and recently a German state, Schleswig-Holstein, has banned such links (Meyer, 2011). The data-protection authority in Schleswig-Holstein contend that Facebook carries out an excessive amount of monitoring of its users without letting them know how much they are being profiled and this profiling is illegal under German state and federal law. They also recommended that private citizens should not set up Facebook accounts and should avoid clicking on these "*Like*" buttons.

Other SNS sites have sprung up to address these privacy concerns. Diaspora is one such alternative SNS. Launched in 2010, it is an open-source SNS that contains the same

[1] http://face.com/about.php

functionality as a commercial SNS such as Facebook, but gives users full control and ownership of everything they share on the network. Since its launch however it has made no real impact in the SNS market.

SNSs can be considered part of what Thrift (2005) refers to as "*knowing capitalism*". He contends that IS/ICT have generated a new and vibrant set of markets for capitalism, where knowledge that has up to now evaded capitalism can be easily captured. For example, knowledge transmitted through gossip and small talk can now be captured and turned into opportunities for profit. The information that SNSs hold are of immense value in this context (Beer, 2008). The valuation of these sites confirms this. In July 2010, Tiger Global Management, a hedge fund spent $20 million for a 1% stake in LinkedIn valuing the company at over 2 billion US dollars (Quinn, 2010). It is estimated that Facebook could be worth as much as $100 billion by spring 2012 (Barnett, 2011). The commercial value of these sites has meant that major software players such as Google have made repeated attempts to gain a foothold in this lucrative market. Their most recent attempt is Google+, launched in mid 2011. As stated by Beer (2008) it is important that users remind themselves that although SNSs are free to use, they are commercial spaces. As stated by Fletcher (2010) "*the feelings you experience on Facebook are heartfelt; the data you are providing feeds a bottom line*".

Clearly the privacy implications of SNSs can open users to many risks. This information is valuable as a business commodity, but also to fraudsters and can open users to risks such as stalking, identity theft, building a digital dossier, advertising, spam, phishing, etc. A major concern, however is that the long term implications of revealing such personal information are as yet unknown. The potential dangers could be serious because as stated by Mayer-Schönberger (2011) the Internet never forgets. There are many other risks that SNS users can encounter including risks to their reputation and risk associated with excessive use. A recent report from the Irish marriage advisory service Accord cited excessive use of the Internet and SNSs as the fastest-growing cause of marital difficulties (O'Halloran, 2011). Users can also create many problems for themselves and others on SNSs. One such example is the recent UK court case where a juror contacted a defendant in a multi-million-pound drugs case. This resulted in the trial collapsing and the juror being in contempt of court and facing an eight month jail sentence (Carter, 2011). Producing a definitive list of risks associated with SNS use is difficult, particularly as this is a rapidly evolving environment. New risks are constantly emerging and the full implications of users' behaviour on SNSs are as yet unknown.

1.2 Statement of the Problem

Given that SNS use is increasing at all age levels, and that research has shown that there are many risks that users can encounter on SNSs, it is important to know whether users of SNS perceive any risk in using SNSs and why some users perceive themselves likely to encounter negative events and others do not. By examining risk perception, it is possible to gain an understanding of not only whether a person perceives they are likely to encounter a negative event, but also the perceived harm and consequence of the negative event. As the age profile of SNS users is widening, it is important to have an understanding of how risk perception changes with age and to examine whether certain negative events are more pertinent for particular age cohorts. Understanding how users perceive risks on SNSs and understanding the factors that influence risk perception is critical to the development of strategies for increasing awareness of the risks associated with SNS use and gaining knowledge of users' behaviour on SNSs.

As far as it is known, this is the first study to examine age related risk perception on SNSs. The research adopts a mixed method research design. The rationale for combining both quantitative and qualitative approaches is that the quantitative data and results provide a general picture of the research problem, e.g. what are the factors that contribute to a user perceiving themselves at high risk on SNSs, while the qualitative data will allow the participants' views to be explored in more depth (Tashakkori and Teddlie, 2003, Creswell and Plano Clark, 2007, Creswell, 2009, Teddlie and Tashakkori, 2009)

The intent of this study is to examine adolescents, emerging adults and adults risk perception of a wide range of negative events on SNSs. The purpose of this two-phase explanatory mixed methods study is to obtain statistical, quantitative results from surveys and then follow-up with a number of semi structured interviews (emerging adults) and focus group discussions (adolescents) to explore these results in more depth.

1.3 Research Questions

The principal objective of the research is to investigate whether users perceive themselves at risk of negative events on SNSs. An overview of the research questions is presented here and further discussion of the research questions is presented in Section 3.8.

1 To what extent do users perceive themselves at risk when using SNSs? Does the nature and composition of these risk perceptions vary with age and if so how?

2 What are the factors that contribute to a user perceiving themselves to be at a higher likelihood of experiencing negative events on SNSs?

3 To what extent do users think that others are more likely than them to experience negative events on SNSs?

4 Are SNS users engaging in behaviours that could increase their vulnerability to risk?

1.4 Research Justification

This study can be justified on a number of grounds. The subject area is topical and is gaining interest in the research community; there are gaps in the literature, the findings of the study have practical implications and provide direction for future research.

SNSs have seen phenomenal growth since the mid 2000's and have quickly become an essential communication tool for many Internet users both young and old alike. Their rapid absorption into everyday life has not only made them a topic of interest to the media, but also to researchers from a wide variety of backgrounds, including for example social science, psychology, business, education, computer science and even medicine. Much of the research into SNSs is at an embryonic stage, but certain strands of research are emerging. Some researchers have examined the social and psychological impact of SNSs, in particular comparing online and offline social networks (e.g: Donath and boyd, 2004, Ellison *et al.*, 2007, Lampe *et al.*, 2008, Subrahmanyam *et al.*, 2008), the effects of SNSs on well-being (e.g: Valkenburg *et al.*, 2006, Ellison *et al.*, 2007, Lenhart and Madden, 2007, Ross *et al.*, 2009) and how users manage their identities on SNSs (e.g: boyd, 2004,

Peluchette and Karl, 2008, Zhao *et al.*, 2008, Back *et al.*, 2010). There are also substantial strands of research addressing the privacy implications associated with SNSs and examining risks and risky behaviour on SNSs. This research adds to the latter.

The review of the literature in chapter 3 shows that research into the risks on SNSs has been successful in analysing some types of online risk, but a number of gaps are evident. Many of the risks encountered on SNSs can pose a threat for adults, but are considered of more concern for children as they may not have yet developed adequate coping mechanisms for these threats. This has meant that much of the research in this area has focussed on the risks to children and adolescents, and has not addressed the incidence of online risks with older age cohorts. The risk agenda has been largely been led by researchers who do not necessarily reflect users' concerns. This has meant that the research has tended to focus on the more threatening risks such as cyberbullying, encountering pornography, paedophiles, stranger contact etc. and there is little available research on commercial risks, personal information risks, reputational risks or the impact of excessive use of SNSs. The majority of the research into Internet risks, and risks on SNSs has examined the incidence of these risks, but has made little progress in researching the relation between risk and harm. By examining risk perception it is possible to not only gain an understanding of the perceived likelihood of the risk, but also of the perceived consequences of the risk. A measure of concern about risk gives further insight in this regard.

As discussed in chapter 2, there is a limited body of research examining risk perceptions with relation to IS/ICT risks. These studies have examined a diverse range of IS/ICT risks from a number of different angles and thus there is little commonality in the findings, but the research does show that a number of risk perception theories, including the psychometric paradigm, Cultural Theory and the social amplification of risk framework, have been successfully applied in the IS/ICT domain (e.g: Bener, 2000, MacGregor, 2003, Coles and Hodgkinson, 2008). The risk characteristics examined vary between studies, but some omissions are evident. Many of the studies have not accounted for prior experience of a risk and those that have accounted for prior experience have drawn no conclusions with regard to its relationship to risk perception. The Internet shopping literature, on the other hand, has examined risk perception in more detail and how it affects online purchasing behaviour. However, many of these studies can be criticised because perceived risk has been treated as a unidimensional construct despite the fact that a large body of

literature indicates that risk perception is a complex, multidimensional construct. Many of the studies examining risk perceptions with relation to IS/ICT risks have not addressed the psychological and social aspects of risk perception, an important consideration as information systems are essentially social systems which rely on an important technical component.

This study addresses a number of gaps in the extant literature and is, as far as it is known, the first study to examine age related risk perception of negative events on SNSs. The research provides increased insight into the nature of risk perception of negative events on SNSs and whether these risk perceptions change with age. In addition the study examines a wide range of risks that can be encountered on SNSs and has based the negative events upon what young people themselves consider risky rather than solely upon adult and expert evaluations. The research is further enriched by the inclusion of qualitative interviews and focus group discussions that provide for a deeper understanding of risk perception. A more detailed discussion of the theoretical contribution of this research is presented in Section 6.4.1.

The results of the research are a preliminary framework that captures the factors that influence risk perception on SNSs. This framework provides a deeper knowledge and understanding of the factors that predict high risk perceptions on SNSs. Knowing how users perceive risk on SNSs is of use to a wide range of stakeholders that have a role to play in managing potential risks on SNSs. These stakeholders include: SNS companies, online service providers, regulators, governments, parents, teachers, universities, employers and users themselves. The findings of this research can inform not only further studies of SNS risks, but also studies of IS/ICT risks and Internet shopping research. The practical implications of this research are presented in Section 6.4.2 and future work is discussed in Section 7.3.

1.5 Dissertation Structure

A brief overview of the structure and content of chapters is given below:

Chapter 1: provides a justification for the research and highlights the theoretical and practical contribution of the thesis. The history of SNSs and how research has developed

in this area is included. A statement of the problem and an overview of the research questions are presented.

Chapter 2: presents a review of the current state of research in risk perception. Risk and risk perception are defined. A number of different theories and models used in risk perception research are examined. This is followed by a discussion of the different risk perception theories used to date in Information Systems (IS) research. Adolescent and emerging adult risk perception research is also reviewed.

Chapter 3: examines the research literature relating to social networking sites with a particular emphasis placed on the literature pertaining to the risks with SNSs. Aspects of the Internet that contribute to it being a risky environment are discussed. This is followed by a discussion of the current strands of research into SNSs. The risks that users can encounter on SNSs are examined in detail. The chapter concludes with a list of the research questions.

Chapter 4: begins with an overview of the IS discipline and introduces the main areas of debate within the IS community regarding the identity and scope of IS research. This is followed by an outline and justification of the philosophical stance of this research. The research methodology and research design utilised in this study are discussed in detail.

Chapter 5: presents the main results and findings of the quantitative and qualitative research. This chapter begins by presenting demographic details of the sample. Following this background information on respondents' use and behaviour on SNSs is presented. This is followed by an analysis of risk perception on SNSs and a detailed examination of the factors that contribute to high risk perception. The final section examines optimistic bias.

Chapter 6: presents a discussion of the findings. The findings are considered in the light of existing theory and previous studies in the area. The contribution of the research to theory and practice are outlined.

Chapter 7: concludes the dissertation with a summary of the main findings of the study and a brief discussion of the limitations. Finally, areas for future research are suggested.

1.6 Definitions

This section clarifies the terminology adopted in this thesis. There are difficulties is how risk is defined and how the term is used. People use the term risk in a number of different ways, sometimes risk is used to mean a hazardous activity, sometimes risk is considered to be the probability of an adverse event and risk can sometimes mean the adverse consequences of that event, but as suggested by (Slovic, 2000a) risk is best thought of as a blend of the probability of an event and the consequences of that event. The way probability and consequence are combined is subtle and not easily articulated. In decision theory expected values are computed by multiplying probability by consequence, but from a psychometric perspective this is a relatively crude approach. Humans do not think about risk in terms of simple arithmetic. Thus, when an individual talks about their risk perception it is important to understand whether they are referring to the likelihood of an event happening, the consequences of that event or both. For all further discussions risk perception refers to the latter, i.e. to both the personal likelihood of an event happening and the consequences of that event.

A hazard is defined as anything that (animate or inanimate; natural or human product) could lead to harm (to people or their environment) (Breakwell, 2007). A further confusion can arise as people commonly do not make a distinction between a hazard and a risk, for instance, smoking is sometimes referred to as a risk and sometimes referred to as a hazard. As it is common parlance, a hazard that can be encountered on SNSs is referred to as a risk or a negative event.

When individuals talk about hazards they refer to different features, qualities or characteristics of the hazard, e.g. knowledge of the risk, whether the risk is controllable etc. These will be referred to as risk characteristics.

With regard to age groupings referred to in the thesis, for "*children*", the definition used is that proposed by the UN Convention on the Rights of the Child as persons up to the age of 18. For the results of this analysis, adolescent refers to sample respondents aged 12-17, emerging adults refers to sample respondents aged 18-25 and adults refers to those aged 26 and above.

2. Literature Review Risk Perception

2.1 Introduction

This chapter presents a review of the current state of research in risk perception. A number of different theories and models used in risk perception research are examined. There are numerous theories of risk perception; it is beyond the scope of this thesis to adequately review all these theories so only the theories that are most cited and of most relevance to the context of the research question are examined. Before these theories are presented, the difficulties in defining risk will be highlighted. Each of the differing theories in risk perception is subsequently explored in greater detail. This is followed by a discussion of the different risk perception theories used to date in IS research. Adolescent and emerging adult risk perception research is also reviewed.

2.2 Defining Risk and Risk Perception

2.2.1 Risk

Risk is a concept that is difficult to define precisely. Definitions of risk differ across disciplines and even within disciplines and experts and the public often have different interpretations of risk (Renn, 1998, Weber, 2001).

One element of risk is uncertainty. As Weber (2001) states, in order for a decision or action to appear risky, there has to be some uncertainty about the outcome. It is often assumed that this outcome is negative, for example the risks associated with a nuclear disaster. However, a negative outcome is not always the case, as for example economic theory assumes that gains and losses can be defined as risks. There is also the concept of "*desired*" risk (Machlis and Rosa, 1990). This is where the public seek out thrilling, but risky, experiences such as hang gliding or bungee jumping. Rosa (1998, p28) suggests a definition of risk for uncertain outcomes irrelevant of whether they are negative or positive, *"risk is a situation or event where something of human value (including humans themselves) has been put at stake and where the outcome is uncertain."*

This definition does not suggest a way to measure risk. In scientific studies, risk is often calculated as the probability of an adverse event multiplied by the consequences of that event. Renn, Burns *et al.* (1992) propose that definitions of risk should contain three elements: outcomes that affect what humans value, uncertainty and a formula to combine both elements. The interpretation of each of these three elements is dependent on the disciplinary view of the researcher.

Risk is an important area of research in the social sciences. Much of this is attributable to the extensively cited works of Ulrick Beck (1992) and Anthony Giddens (1991). They assert that individuals and organisations are exposed to many new hazards and risk has become a prominent concept in modern society due to the "*complexification*" of societies' systems (Jackson *et al.*, 2004a). Managing these new hazards has become a central challenge for all societies. Beck contends that in earlier, class-based societies only the poorest were victimised, but in modern society all groups, even business owners and the rich, are threatened. Beck, controversially, argues that the current class system is being overthrown. Draper (1993) thinks this is probably too extreme a view as environmental hazards still present the greatest threat to the poor. Toxic waste dumps are rarely positioned in wealthy areas. Although Beck's "*risk society*" (1992) is widely cited, there has been little empirical work examining this theory. However elements of his theory have been tested empirically, for example there is an academic literature looking at the question of trust with experts, as discussed in section 2.4.3.

Although some of Beck's assertions are extreme, it is clear that there has been an increase in the type of risks posed in modern society. This is evidenced by the six major categories of risk identified by Lupton (1999), see Table 2.1.

Risk Category	Examples
Environmental Risks	pollution, radiation, chemical, floods, fires etc.
Lifestyle Risks	related to the consumption of food and drugs, sexual activities, driving practices, stress etc.
Medical Risks	medical procedures, drug therapy, surgery, etc.
Interpersonal Risks	related to intimate relationships, for example social interactions, sexuality and friendship.
Economic risks	unemployment, debts, investments, bankruptcy, failure of a business etc.
Criminal Risks	being a participant in or potential victim of illegal activities.

Table 2.1 Six Major Categories of Risk in Western Society. Source: (Lupton, 1999)

In addition to this, new technological advances, rather than minimising or controlling risks, can generate new risks and challenges that were not even predicted (Beck, 1992, Ciborra, 2001, Weber, 2001). Another well cited author in the social science area is Mary Douglas (2003), she believes that different individuals and groups may judge the same risks differently as they place differing values on the outcome. This became the basis for Cultural Theory which is discussed in further detail in section 2.3.4. Much of the social science research agues that risk is subjective. As posited by Slovic (1999, p690), "*risk does not exist "out there", independent of our minds and cultures, waiting to be measured. Instead, human beings have invented the concept risk to help them understand and cope with the dangers and uncertainties of life*."

There is a variety of definitions and disciplinary approaches to risk. Rayner (1992) argues that there is no one single all-encompassing definition of risk, instead he sees risk as a number of definitions with many links, but with no single feature that is common to all of them. Tansey and O'Riordan (1999) assert that this approach may lead to a community of deliberation rather than consensus over a single interpretation.

2.2.2 Risk Perception

In modern society individuals have access to an increasing amount of information and choices, but at the same time this has led to increased uncertainty and difficulty in decision making (Beck, 1992, Schwartz, 2005). Risk perception is a judgement that individuals make concerning these uncertain events. The complex nature of risk perception is captured in a definition proposed in the Royal Society's 1992 report on risk. Here risk perception is defined as involving "*people's beliefs, attitudes, judgements and feelings as well as the wider cultural and social dispositions they adopt towards hazards and their benefits*" (Pidgeon *et al.*, 1992, p89). Pidgeon (1998) states that this definition was made deliberately broad to encompass the wide range of multidimensional characteristics of hazards, rather than just an abstract expression of uncertainty and loss.

Perception of risk plays an important role in decision making (Slovic and Weber, 2002) and has been of interest to policy makers and researchers for several decades (Sjöberg, 2000). There are many differing research approaches to risk perception, each of which contributes important arguments to the debate on risk and how risks are perceived. The following sections present an overview of these differing paradigms.

2.3 Approaches to Risk Perception

To structure a discussion on risk perception, it is useful to divide the empirical research into differing theoretical paradigms. Each paradigm defines risk differently and identifies various factors that affect people's perception of risk. From a detailed review of the literature, research on risk perception can be divided into four areas as follows:

1. Objective risk assessments;
2. Cognitive psychology paradigms;
3. Psychometric paradigms; and
4. Sociocultural paradigms.

In objective risk assessments, risk is considered to be objective, measurable and is examined from an individual perspective. The focus is on the way that individuals combine objective risk information, that is, possible consequences of risky choice options such as mortality rates or financial losses, and their probability of occurrence. Research in cognitive psychology examines how individuals approach probabilities of possible outcomes. The psychometric paradigm views risk from an individual's perspective, but assumes that risk is subjective (i.e. personal, intimate). This paradigm has evolved to include people's emotional reactions to risky situations. Studies within the sociocultural paradigm have examined the effect of group and culture on risk perception.

One way to compare the differing approaches to risk perception is to map them onto two dimensions. The dimensions chosen have been proposed by Renn (2005), Taylor-Gooby & Zinn (2006) and Lupton (1999). The first dimension distinguishes between risks measured at an individual level or risks measured from a social and cultural level shared across a group. The second dimension looks at how risk is interpreted and understood. At one level risks are thought to be real and measurable. They can have an independent existence external to the individual or social group that perceives the risk. Risks can also be thought of as constructionist and subjective. Here the understanding of risk can be a personal/internal construction which can be influenced by social and cultural processes. In this case risks will not be perceived by everyone in the same way. Figure 2.1 illustrates where these paradigms lie on subjective – objective and individual – social continuums.

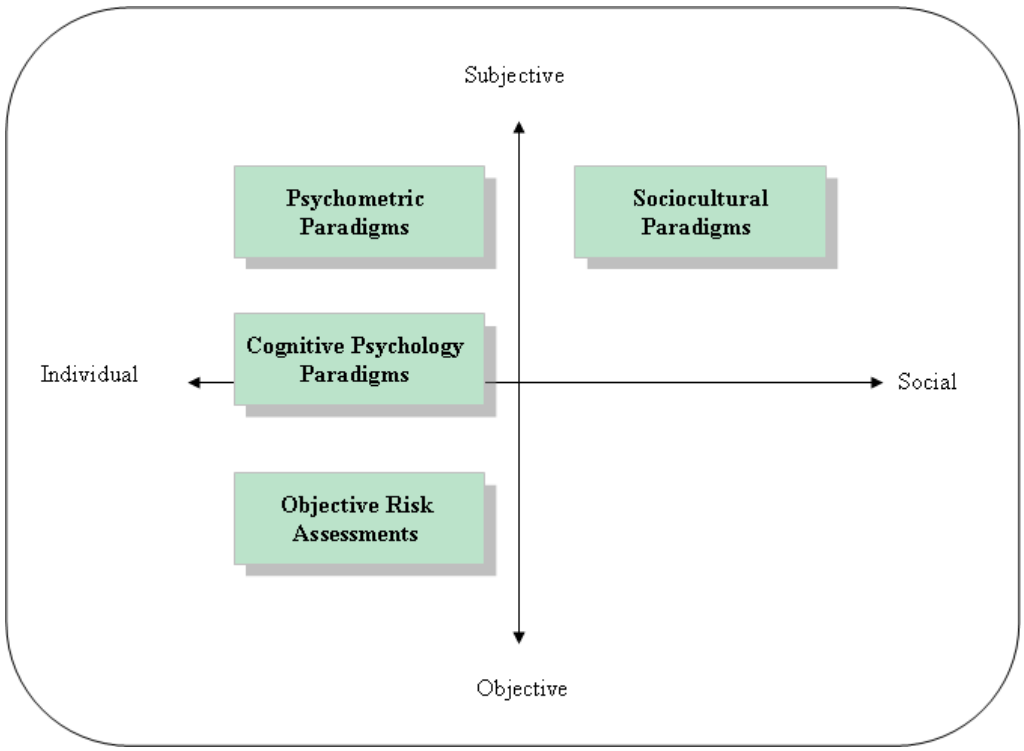


Figure 2.1 Four Paradigms in Risk Perception Research on Subjective – Objective and Individual – Social Continuums.

The following sections examine each of these theoretical risk perception paradigms in further detail. Within each paradigm, the more commonly used and cited risk perception theories are discussed. These theories are then synthesised and critiqued.

2.3.1 Objective Risk Assessments

Although the concept of risk is not new, it is only since the 1950's that academic researchers have attempted to understand, define and quantify risk. The analysis of risk focuses on the areas of risk assessment and risk management. *Risk assessment* is used to identify, characterise and quantify risk. *Risk management* is the process of reducing risks to an acceptable level, see Figure 2.2. Risk assessment is primarily used by qualified analysts to evaluate hazards and is an objective measurement. The public tend to use intuitive risk judgements, called *risk perceptions*. Their judgements are less formal and are often based on news media reports (Slovic, 1987) and are subjective in nature. However the public are able to make objective risk judgements as in gambling for example.

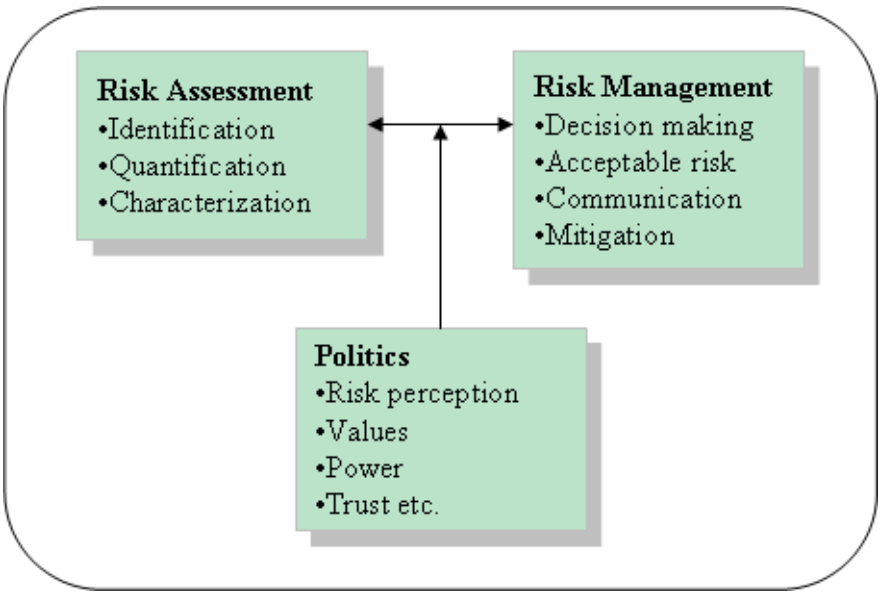


Figure 2.2 Components of Risk Analysis, adapted from (Slovic and Weber, 2002)

This section examines risk assessment in more detail, under the heading of objective risk assessments (technical risk assessments). Numerous risk assessment techniques exist in financial and engineering circles. There are also many examples in the computer security area such as ISO 27001/ISO 1779 (Calder, 2006), COBRA model (Briand *et al.*, 1998), I2S2 model (Korzyk, 2002) and the OCTAVE^{SM} approach (Alberts and Dorofee, 2002). These risk assessments are based on risk theories that use quantitative approaches to produce numerical estimates of the chance or probability of a risk. Many risk assessment models define risk as statistical variance. Sure options carry no risk, since there is no variance around a guaranteed outcome. The wider the distribution of possible outcomes, the greater the risk becomes.

Limitations of objective risk assessments

Objective risk assessments have been criticised, particularly by researchers in the social sciences. Rosa (1998) argues that objective risk assessments have a positivistic orientation where risk is reduced to a "*purely scientific*" measure. Normative judgments are excluded and important social, political and cultural contexts are ignored (Pidgeon *et al.*, 1992, National Research Council, 1996). Slovic (2000b) argues that these objective risk assessments may not be as scientific in practice as it is difficult to make "*objective*" decisions and often the risk modeller has to use subjective judgements and assumptions. According to Renn (1998), these criticisms are well founded, but he argues that objective risk assessments still play an important role in risk analysis. Objective risk assessment has become a sophisticated tool that helps assess the potential harm of threats, particularly in terms of estimating injuries, fatalities and other types of losses (Renn, 1998, Rosa, 1998).

2.3.2 Cognitive Psychology Paradigms

Early research in risk perception assumed that individuals made decisions in a rational way. Individuals were assumed to process available information according to standard statistical principles. Cognitive psychology extends this view to regard a human being as a system that codes and interprets available information in a conscious manner, but where other, less conscious, factors also inform decisions. Cognitive psychologists have questioned the degree to which individuals follow standard statistical principles when making decisions.

It is widely acknowledged that the public have difficulties in interpreting probabilities. A study carried out by Gigerenzer, Hertwig *et al.* (2005) produced interesting findings. The researchers examined how the probability statement "*a 30% chance of rain tomorrow*" was interpreted by individuals in five different cities. A short survey was administered to pedestrians in Amsterdam, Athens, Berlin, Milan and New York. New York was the only location where a majority gave the correct interpretation that in 3 out of 10 cases there will be (at least a trace of) rain tomorrow. The preferred but incorrect interpretation in Europe was that it will rain tomorrow "*30% of the time*", followed by "*in 30% of the area*". There are many other experiments that show individuals' lack of understanding of probabilities (Kahneman *et al.*, 1982). One of the most influential and widely cited papers in the cognitive psychology paradigm, is "*Judgment under Uncertainty: Heuristics and Biases*" by Tversky and Kahneman (1974), which examined the heuristics and biases used by individuals in probabilistic thinking. They found that individuals do not follow the principles of probability theory when making risk judgements; instead individuals use a number of heuristics to evaluate threats. These heuristics can lead to inaccurate judgments ("*cognitive biases*") in some situations. Some of the heuristics that have emerged from this literature are summarised in Table 2.2.

Kahneman and Tversky (1979) also developed "*prospect theory*". This theory examined why an individual's actual behaviour with regard to risky decisions differs from rational choice theory. An important finding of this research showed that individual's attitudes toward risks concerning gains may be quite different from their attitudes toward risks concerning losses. For example, when given a choice between getting €1,000 with certainty or having a 50% chance of getting €2,500, individuals often choose the certain €1,000 in preference to the uncertain chance of getting €2,500 even though the

mathematical expectation of the uncertain option is €1,250. This tendency is called the "*certainty effect*" and contributes to "*risk aversion*". But Kahneman and Tversky found that the same people when confronted with a certain loss of €1,000 versus a 50% chance of no loss or a €2,500 loss often choose the risky alternative. This tendency is called "*risk-seeking*" behaviour.

Heuristic	Description
Availability Heuristic	Threats and dangers that can be more easily brought to mind or imagined are judged to be more likely than events that cannot easily be imagined.
Anchoring Heuristic	Individuals will often start with one piece of known information and then adjust it to create an estimate of an unknown risk - but the adjustment is typically not large enough.
Threshold effects	Individuals prefer to move from uncertainty to certainty over making a similar gain in certainty that does not lead to full certainty. For eg., most people would choose a vaccine that reduces the incidence of disease A from 10% to 0% over one that reduces disease B from 20% to 10%.
Effect of sample size	Most individuals assign the same probabilities in small and large samples, without taking into account that uncertainty about (the variance of) the mean declines rapidly with increasing sample size.
Representativeness	This heuristic underlies an individuals tendency to judge events as being more likely if they conform to a particular image or stereotype they have of a category.

Table 2.2 Summary of Heuristics and Biases used by Individuals to Evaluate Threats.

Overall, research in this area has shown that individuals don't always follow probability or rational decision making theories and can thus make incorrect decisions. As the Royal Statistical Society states in its report "*The trouble with risk*" (2003), as so often with statistics, the truth is not immediately obvious and sometimes runs counter to intuition.

Limitations of cognitive psychology paradigm

Sjöberg (2000) criticises Kahneman and Tversky's research on heuristics and biases as he asserts it is based on probability problems that have been designed to be counterintuitive. A further criticism is that much of this research was carried out using laboratory-based risk perception studies and this could have a limited applicability to how probabilities are understood in applied settings. These are valid arguments, but other researchers such as Gigerenzer, Hertwig *et al.* (2005) have found evidence that the public have difficulties in interpreting probabilities. Work of this nature in the cognitive psychology field is no longer regarded as of primary importance for risk perception as many researchers have shown that the public's risk perception is multidimensional and that subjective probability is only one of many factors (Fischhoff *et al.*, 1982).

2.3.3 Psychometric Paradigm

Early studies of risk perception in the 1970's examined individuals' responses to the threats posed by various technologies and natural hazards. A seminal paper in this area was "*Social Benefit versus Technological Risk"* by Chauncey Starr (1969), which used a "*revealed preference*" approach to analyse historical data on fatalities for a number of risks. Starr's major finding was that the public will accept "*voluntary*" or the illusion of control (e.g. driving a car) risks roughly 1,000 times greater than if they are involuntary (e.g. a nuclear disaster). Following this, a group of researchers proposed a survey based method for studying risk perception (Fischhoff *et al.*, 1978, Slovic *et al.*, 1984). They used psychophysical scaling[2] and multivariate analysis techniques to produce quantitative representations or "*cognitive maps*" of risk attitudes and perceptions. This became known as the *psychometric paradigm* and is still a commonly used theoretical framework (McDaniels *et al.*, 1997, Worsley and Scott, 2000, Lloyd, 2001, Siegrist *et al.*, 2007b).

This approach is appealing for a number of reasons. It shows that individual's conceptions of risk are complex and multi-faceted. The approach elicits current preferences or "*expressed preferences*". It examines aspects of risk and benefit besides monetary implications and fatalities and data can be gathered for a large number of technologies and activities (Slovic, 2000b). These studies asked respondents to rate risks on a number of dimensions. By using factor analysis, two main factors were identified that could explain why people saw some risks as more dangerous than others. These factors were referred to as "*dread and unknown*" (Fischhoff *et al.*, 1979, Slovic *et al.*, 1979, 1980). Figure 2.3 shows the broad descriptive capability of the psychometric paradigm, hazards are located on a cognitive map which shows a range of potential hazards in a two-dimensional space.

A "*dread risk*", as depicted in Factor 1, is perceived as uncontrollable and the danger might be catastrophic, fatal and a high risk to future generations. It is also an involuntary risk. The second factor "*unknown risk*" is composed of qualities such as whether the risk is unobservable and unknown to individuals or science. Riskier activities are associated with the top right quadrant in Figure 2.3.

[2] Psychophysical scaling refers to the process of quantifying psychological events, especially sensations and perceptions. Scaling requires both a set of empirical operations and a theoretical framework to derive the quantitative values or representations. Marks, L. E. & Gescheider, G. A. 2002. Psychophysical Scaling. *In:* Pashler, H. (ed.) *Stevens' Handbook of Experimental Psychology.* 3rd edition ed. New York: John Wiley & Sons, Inc.

Slovic (2000b, pxxiii) states that *"the psychometric paradigm encompasses a theoretical framework that assumes risk is subjectively defined by individuals who may be influenced by a wide array of psychological, social, institutional and cultural factors. The paradigm assumes that, with appropriate design of survey instruments, many of these factors and their interrelationships can be quantified and modelled in order to illuminate the responses of individuals and their societies to the hazards that confront them."*

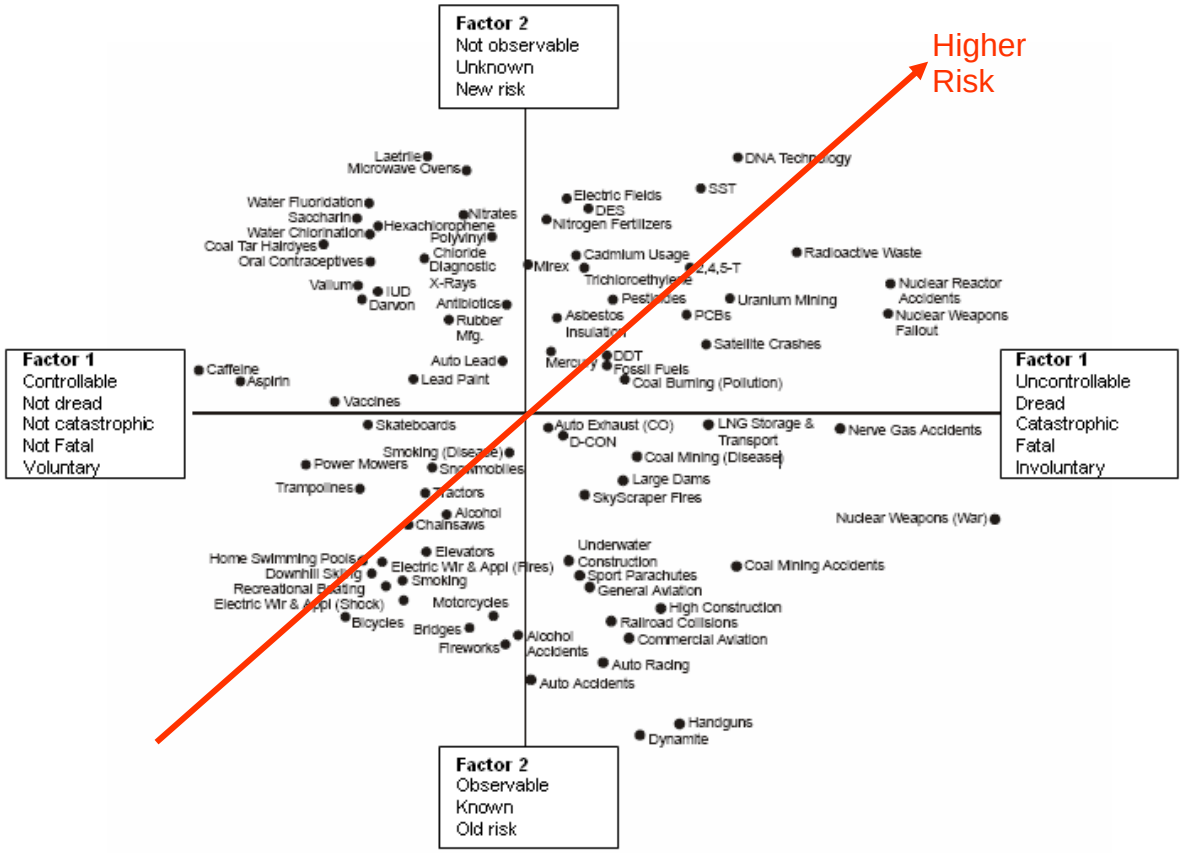


Figure 2.3 Location of 81 hazards on Dread and Unknown Risk factors.
Source: Adapted from, Paul Slovic (2000b), Perception of Risk, p225

A large number of studies has been carried out using this approach. Dread and Unknown have been two commonly found factors in many of the studies, although there are exceptions (Johnson and Tversky, 1984). In general, studies have found that acceptable levels of risk are higher for natural than for technologically induced risks. Familiar and voluntary risk activities, such as driving or smoking are seen as less risky and more acceptable (Slovic, 2000b).

Early studies were limited to local populations of students and citizen groups. In later years, the paradigm was applied internationally, sometimes with local groups and sometimes with representative national samples (Engländer *et al.*, 1986, Teigen *et al.*,

1988, Keown, 1989, Slovic *et al.*, 2000). These studies have shown that in a wide range of countries risk perceptions are affected by the dread and the unknown factor (Renn and Rohrmann, 2000). Countries differ in where respondents place particular hazards within the factor space and this is usually consistent with the countries socioeconomic development (Weber, 2001).

The early psychometric studies compared large sets of heterogeneous hazards, but more recently studies have examined hazards within homogeneous domains, for example threats to the environment or health such as nuclear power (Furby *et al.*, 1988, Bostrom *et al.*, 1994, MacGregor *et al.*, 1994, Dewispelare *et al.*, 1995, Savadori *et al.*, 2004, Zaksek and Arvai, 2004), but risk perception methods have been applied to other areas such as financial risk (March and Shapira, 1987, Olsen, 1997, Olsen, 2001) and adolescent risk perception (Benthin *et al.*, 1993, Cohn *et al.*, 1995, Smith and Rosenthal, 1995, Gullone *et al.*, 2000).

Recently, research using the psychometric approach has begun to address social, political and cultural factors. Social issues such as gender, trust, and emotion have all been addressed using this paradigm and these are discussed in further sections.

Expert and Public Views on Risk

One question posed in the early work of Slovic *et al.* (1979, 1980) addressed how experts and the public differ in how they perceive risks. They found that experts perceived risks as a function of annual fatalities and objective risk estimates, whereas the public perceived risk to be more complex. They found that the public underestimated risks associated with infrequent, catastrophic events and overestimated the risks associated with frequent, familiar and voluntary events, as is suggested by the availability heuristic (Kahneman *et al.*, 1982) (see section 2.3.2). Although the public sometimes lack certain information about hazards, their basic conceptualisation of risk is much richer than that of the experts and reflects legitimate concerns that are typically omitted from expert risk assessments (Slovic, 1987).

During the 1980's technical risk assessments were perceived to be rational, objective and valid, while public perceptions were believed to be largely subjective and therefore less valid. The public were seen as irrational and were thus excluded from risk decisions (Rosa and Freudenburg, 2001). This disparity between public and expert interpretations of risk

caused a problem for policy makers. Policies based on expert judgements could be seen as unpopular, whereas basing policies on the public's perceptions made policies unscientific and too costly (Yearley, 2001). Pidgeon (1998) asserts that one of the most difficult questions faced by public policy makers is to balance expert judgments on the one hand with public risk perceptions on the other. There is still an ongoing debate regarding the importance and role of public participation in decision making.

Sjöberg (2002a) questioned the assertion that the public and experts actually differed in their views. Sjöberg criticised the work of Slovic because it was based on a small expert group of 15 individuals. He argued that this small a number of experts could not adequately cover all the diverse 81 domains studied by Slovic. Sjöberg (2002a) carried out a single domain study comparing risk perceptions of nuclear waste experts (n= 137) to a probability sample of the Swedish population (n = 1,179). In contrast to the findings of Slovic, the study found that the factors explaining experts' risk perception were similar to those of the public. This is further backed up by James Surowiecki in his book "*The Wisdom of Crowds*" (2005) who says it is important not to rely on the wisdom of one or two experts when making difficult decisions. That doesn't mean that expertise is irrelevant. He argues that the aggregation of information in groups is often better than could have been made by any single member of the group.

This research indicates that the public's risk perceptions are valid and should be included in informing risk assessments and risk communications.

Limitations of Psychometric Approach

While the psychometric paradigm has improved understanding of individual's responses to risk, demonstrated the complexity of the factors that influence risk and provided a tool for analysing risk perceptions, the paradigm does have a number of limitations.

One of the most vocal opponents of the psychometric paradigm is Lennart Sjöberg. He presents a number of criticisms of the psychometric paradigm (1996, 1999, 2002b). The first criticism relates to whether the psychometric paradigm addresses individual variations in risk perception. Early papers that tested the paradigm examined the average ratings of a large number of hazards and found strong correlations between mean perceived risk and mean ratings of the risk attributes. These papers reported that high proportions of variance were explained by this model. Sjöberg (1996) through empirical research has shown that

high levels of explained variance only occur when average ratings are analysed across hazards. This does not address individual or intra-individual variation in risk perception. Studies indicate that when individual data rather than averages are used, the explained variance can drop to as low as 20-25% (Sjöberg, 1996, Langford *et al.*, 1999). Siegrist *et al.* (2005) argue that based on the published literature it is impossible to judge how well the psychometric paradigm explains risk perception at the individual level. They conducted a three-way component analysis to determine whether the psychometric paradigm can be used to explain individual differences. They found that their analysis does present a better understanding of an individual's risk perception, but more research is needed to unveil factors that might explain individual differences in risk perception. Sjöberg (2000) argues that this means that other factors may be just as, or more important than, the psychometric factors devised by Fischoff, Slovic *et al.* (1978). Sjöberg asserts that at least one important factor was missed, interference with nature (tampering with nature, immoral and unnatural risk). Sjöberg has carried out empirical studies (Sjöberg and Winroth, 1986, Sjöberg and Torell, 1993) to assess this additional factor and has found that performance of the psychometric model was improved by the introduction of this additional factor which loaded on such items as unnatural risk, immoral risk and human arrogance.

There are other serious criticisms of the psychometric paradigm. The psychometric approach has been criticised because it does not address the fact that risk could be socially constructed (Lupton, 1999). Lupton argues that variables such as age, gender, ethnicity, nationality etc. need to be considered as they may have a significant bearing on the ways in which individuals perceive risk. Further criticisms of this approach are that the paradigm does not explain risk perception, but is rather a description of the perceived risk of hazards rather than the underlying psychological or social processes (Slovic, 2000b). Furthermore the paradigm typically assesses affective feelings and cognitions but not actual behaviour (Pidgeon *et al.*, 1992). The paradigm records snapshots of risk judgments often ignoring the specific social context in which the risk is experienced (Rogers, 1997). Individuals perceptions of risks are by no means constant; but can change in different social settings and in relation to new knowledge experiences.

Slovic (2000b) argues that despite these and other limitations, studies using this approach have produced coherent and interesting results that have encouraged further use of the paradigm.

2.3.4 Cultural Theory

While the cognitive psychological and psychometric approaches have been influential, they have been criticised for concentrating too much on individual perceptions and interpretations of risk. In contrast to these paradigms, cultural theory refers to theories of risk perception that focus on culture rather than individual psychology. The most influential cultural theory, "*the Cultural Theory of risk*" (note: capital C and T) is based on the work of Douglas and Wildavsky (1982). The main point of the theory is to show that risk judgements are not formed independently of social context. Cultural Theory makes two basic claims. First, it argues that views of risk are produced by and support social structures. Fear of certain types of risk serves to uphold the social structure. Secondly, Cultural Theory proposes that there are four basic "*ways of life*", known as "*cultural biases*" each corresponding to a particular social structure and a particular outlook on risk. The four cultural biases are: egalitarian; individualistic; hierarchic and fatalistic.

These four groupings are located along two dimensions that describe, firstly, the degree of social incorporation constituted within the culture, known as "*Grid*" and secondly the nature of these social interactions known as "*Group*". This typology, see Figure 2.4, has become the best known element of the Cultural Theory of risk and is often confused with the theory within which it is embedded (Boholm, 1998).

At the high group and grid level, hierarchy level, all individuals are highly reliant on each other. In terms of risk perception, the key concern is for control and management, implemented by rules and procedures. At the high group low grid, Egalitarian level, there is an emphasis on cooperation and equality. The response to risk is precautionary and risks are avoided where possible. At the low group and grid level, the individualist sees risk as opportunities. Losses are covered by insurance. The fatalist sees risk as inevitable and uncontrollable.

These four rationalities represent four distinct world views. Disputes about risk can be seen as arguments in which the participants are arguing from different premises, different paradigms, different world views or different myths of nature, both physical and human.

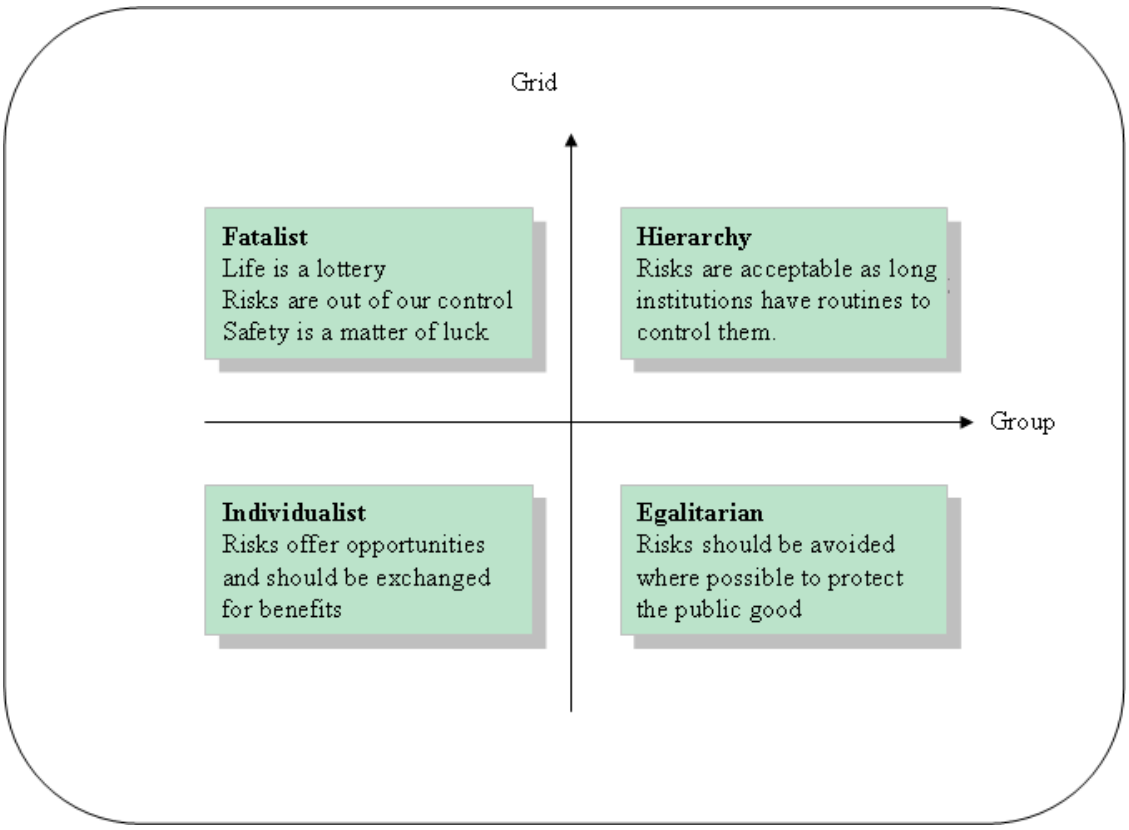


Figure 2.4 Four Groupings in Cultural Theory
Source: Adapted from, Douglas and Wildavsky (2000b)

Cultural Theory shifts the emphasis away from individual perceptions of risk towards group perceptions. In Cultural Theory, individual's perceptions of risk vary according to the way their social relations are organised. Krimsky and Golding (1992, pxv) assert that Cultural Theory is the most comprehensive approach to risk "*covering risk selection, objectivity, science, rationality and public perception."* As the identification of risks is entirely a social process, risk is a cultural phenomenon not a physical one, where context matters (Rosa, 1998). Rayner (1992) has argued that Cultural Theory is true not only at society level but can also be observed in organisations.

There are two different perspectives of Cultural Theory; the stability perspective and the mobility perspective. According to the stability perspective individuals are consistent in their cultural bias. This means that they have the same type of cultural bias in all areas of their life. Questionnaires have been developed to measure an individual's cultural bias independently of a specified time or context (Dake, 1991, Rippl, 2002). The second perspective of the theory, the mobility view, contends that individuals conform to different cultural biases according to specific contexts and/or adopt different biases over time (Renn *et al.*, 1992). It is more difficult to measure this mobility view and for this reason

proponents of this perspective advocate the application of qualitative methods such as participant observation and focus groups (Langford *et al.*, 2000).

Much of the empirical research in Cultural Theory has examined the stability perspective and used the set of questionnaires developed by Karl Dake (1991). These questionnaires have been used in many studies as a way of classifying individuals into one of the four groupings in Cultural Theory. Jackson, Allum *et al.* (2004a) assert that in most studies, individual measures for the four cultural biases tend to correlate weakly with perceptions of risks of various hazards. For example crime-related risks are seen as greater by hierarchists, but individualist and hierarchists are often empirically difficult to distinguish, which they assert calls in to question the value of the theory. Most individuals show some level of agreement with all of the four scales.

These questionnaires developed by Dake (1991) follow a dominant research approach used in the social sciences called methodological individualism[3]. This approach begins by defining individual behaviour and extrapolates to explain social action (Rayner, 1992). Some researchers have argued that this approach is inappropriate for examining a Cultural Theory of risk perception (Tansey and O'Riordan, 1999, Sjöberg, 2000). Rippl (2002) disagrees and argues that individual measurements cannot be used as a direct measure of culture but can be used as a measure of the processes that are connected to culture. From this viewpoint it is possible to learn about social processes from individual level analyses.

Limitations of Cultural Theory

Like the psychometric approach, Cultural Theory has also been widely criticised on a number of grounds (Sjöberg, 1996, Boholm, 1998, Rosa, 1998, Sjöberg, 2000, 2002a, b, Breakwell, 2007, Renn, 2008). Firstly, it is not clear from the theory how people come to adopt a particular cultural perspective and whether people reside in these categories for long periods or whether cultural perspectives are transient. Secondly, the theory is criticised as the two-by-two classification is seen as overly simplistic. Rosa's (1998) criticism of the theory include the failure of the theory to differentiate between the process and the product of socially constructed knowledge. He agrees that knowledge is socially constructed, but this does not preclude the possibility that some of this knowledge is worthless and some useful. A further criticism is that Cultural Theory combines the

[3] Methodological individualism is a philosophical method aimed at explaining and understanding broad society-wide developments as the aggregation of decisions by individuals.

ontology of risk (what is the nature of the world of risk?) and the epistemology of risk (how do we understand and know risks?) into one. The relationship between Cultural Theory and risk perception is also questionable. Although some studies have found significant correlations between cultural biases and risk perception (Dake, 1991, Langford *et al.*, 2000), others have found no significant interactions or low correlations between the variables (Marris *et al.*, 1998, Sjöberg, 2001). Sjöberg (2000) states that these results question the relationship between cultural biases and risk perception and whether the theory can explain risk perceptions and he argues that Cultural Theory is an even less successful attempt to explain risk perception than the psychometric model.

In summary, Cultural Theory has in practice a limited number of applications. Some studies that have adopted Cultural Theory have used positivistic research methodologies, such as the questionnaires developed by Dake (1991) but these appear to be inappropriate for Cultural Theory. Qualitative research methods are deemed more suitable for research using Cultural Theory. Although Cultural Theory is difficult to test empirically, it has provided a valuable contribution to risk perception research by highlighting that risk perception is related to broader social factors and processes. Researchers have begun to recognise that a purely psychological based analysis only accounts for a part of risk perceptions.

2.3.5 The Social Amplification of Risk and Other Theories

Many other risk perception theories exist which have attempted to address some of the limitations of the psychometric paradigm and Cultural Theory. This section provides a short synopsis of some of these other risk perception theories. The theories presented are:

1. The social amplification of risk theory;
2. The Simplified Conjoint Expected Risk theory (SCER) (Holtgrave and Weber, 1993);
3. Network theory of contagion (Burt, 1987, Monge and Contractor, 2000);
4. The basic risk perception model (Sjöberg); and
5. Mental models (Bostrom *et al.*, 1994).

The social amplification of risk theory: The theoretical foundations of the social amplification of risk framework (SARF) were developed in five principal publications (Kasperson *et al.*, 1988, Renn, 1991 , Kasperson, 1992, Burns *et al.*, 1993, Kasperson and Kasperson, 1996). SARF emphasises that when signals are sent from a source to a receiver, those signals often flow through intermediate transmitters that amplify or attenuate/distort the message. Through risk amplification, the impacts of an adverse event can sometimes extend beyond direct damages to victims and property and can cause massive indirect impacts such as legal proceedings against a corporation, increased regulation of an industry and so on. Figure 2.5 shows how the ripples can spread outward, firstly affecting the victims, then the responsible company or agency and in extreme cases reaching other companies, agencies or industries.

An important aspect of social amplification is that the direct impacts don't have to be large to trigger major indirect impacts (Slovic and Weber, 2002). An example of this is the 1982 Tylenol tampering incident. Seven deaths occurred due to this incident, but this resulted in over 125,000 media reports alone and the Johnson and Johnson company losing more than one billion dollars due to the damaged image of the product. Slovic and Weber (2002) predict that hazards that occur in the upper right quadrant of Figure 2.3 (i.e. high risk threats) are likely to have larger ripple effects.

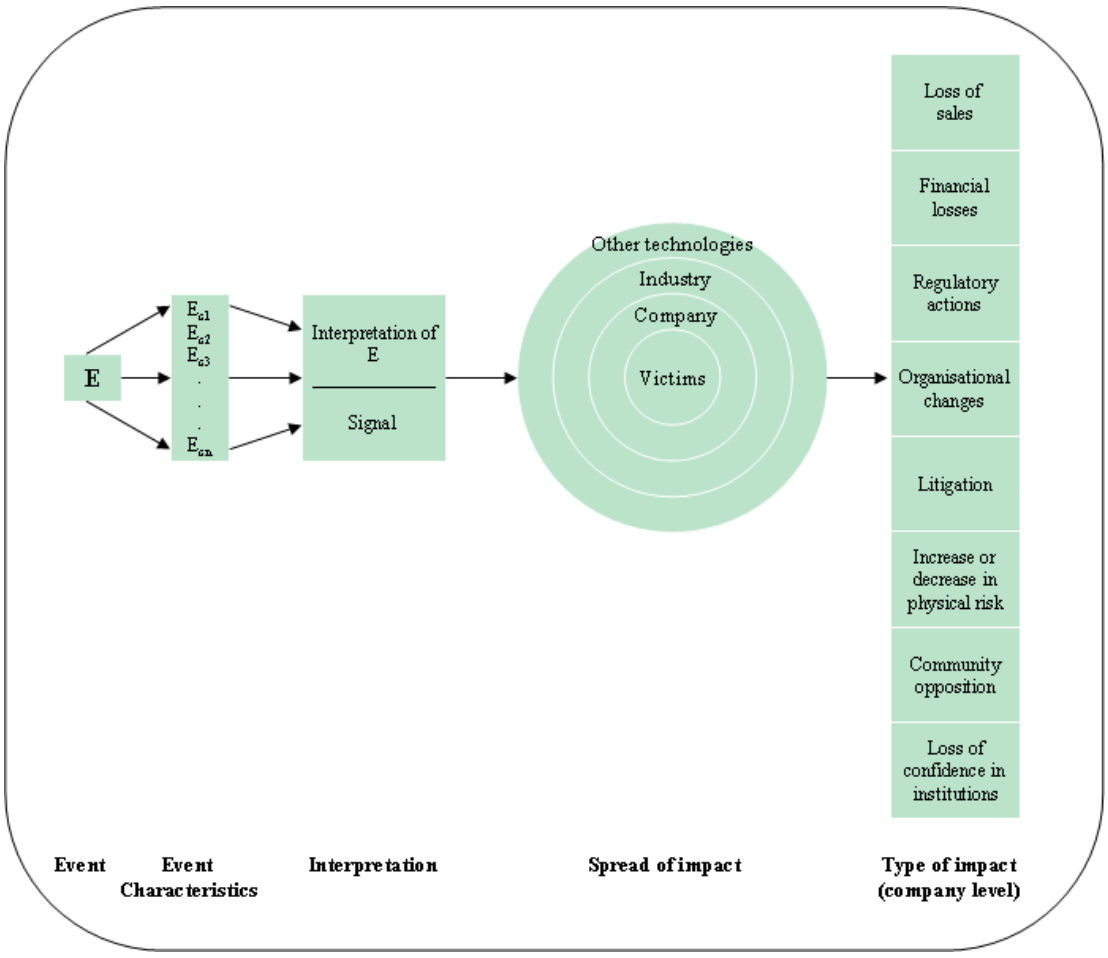


Figure 2.5 The social amplification of risk framework. (Source: Kasperson et al. (1993), p14**)**

There have been critics of SARF. Rayner (1992) questions what is being amplified or attenuated and argues that the framework implies that there is a baseline of objective risk transmitted by experts and the media which then gets distorted by the public. SARF provides a means of explaining risk communication rather than a means of understanding the reasons for responses and perceptions (Murdock *et al.*, 2003).

Leaving the criticisms aside, the SARF framework has generated a considerable body of generally supportive empirical research, because of its interdisciplinary orientation and because it integrates other factors that have been shown to influence risk perception such as social, organisational, institutional and political factors (Rosa and Freudenburg, 2001).

The Simplified Conjoint Expected Risk theory: Holtgrave and Weber (1993) extended the Conjoint Expected Risk (CER) model (Luce and Weber, 1986) to develop the Simplified Conjoint Expected Risk (SCER) model. This model attempts to bridge the gap between objective risk assessment and subjective models such as the psychometric

approach. The original CER model uses objective information to evaluate financial models. However, it is difficult to apply this model to domains such as health or technology where values cannot be easily quantified and are subjective in nature. The SCER asserts that perceived risk is a linear combination of the subjective judgments of the probabilities of harm, benefit and status quo and the expected harm and benefit of an activity. Carlstrom, Woodward *et al.* (2000) have empirically evaluated the SCER and have found that the model is viable with activities for which harm and benefit information is subjective. To date the SCER model has not been extensively applied in the risk perception literature.

Network theory of contagion: Risk perception approaches have mostly studied risk perception from an individual viewpoint and do not explain how perception of risk may vary among communities or social groupings (Scherer and Cho, 2003). One alternative is to use an approach based on a network theory of contagion (Burt, 1987). This theory has emerged from social network studies and suggests that it is individuals and their relations with social networks that should be the units of analysis. The theory suggests that individuals adopt the attitudes or behaviours of others in their social network and this forms a cultural system of norms, expectations, knowledge and behavioural support (Monge and Contractor 2000). Scherer and Cho (2003) have examined this theory to see if risk perception networks exist within social communities. They define a risk perception network as a "*relational grouping of individuals, who share and perhaps create similar risk perceptions*" (p261). Their analysis confirmed that social linkages in communities may play an important role in focusing risk perceptions.

Basic risk perception model: As previously discussed, Sjöberg has questioned whether the psychometric model and Cultural Theory models can adequately explain risk perception. Sjöberg (1993) thus proposed the basic risk perception model (BRPM). The BRPM expands on the psychometric dimensions and empirical studies have shown that BRPM explains more of the variance in risk perception (Sjöberg and Drottz-Sjöberg, 1994). This is achieved by adding the factors of risk sensitivity, attitudes, specific fear and sometimes trust and moral value (Sjöberg and Torell, 1993, Sjöberg, 2000, 2001). The methodology used in the BRPM approach is similar to that of the psychometric approach, i.e. questionnaires and factor analyses. To address Sjöberg's criticisms of the psychometric approach, the samples used are much larger and more representative of the general population. Another important difference is that in the statistical analyses, the

individual is used as the unit of analysis, not the mean of responses. A review of the literature suggests that the BRPM model has not been empirically tested by any other authors.

Mental models: The psychometric paradigm, provides only a surface level of description that leaves many important questions unanswered, such as why do adolescents engage in risky activities even when they are aware of the negative aspects (e.g. smoking)? Answering questions such as this requires methods that can attain a deeper understanding of specific issues. One approach is "*Mental Models*" (Bostrom *et al.*, 1994). The approach is based on both decision making and psychometric theories. Bostrom *et al.* used mental models to explain responses to evidence that appear irrational from other perspectives. Their research used open-ended interviews to construct influence diagrams and mental models to depict individual's knowledge, attitudes, beliefs, values, perceptions and inference mechanisms with respect to perceptions of climate change. Bostrom *et al.* found that the public displayed a variety of misunderstandings and confusions about the causes of climate change. Cox *et al.* (2003) used the mental models approach to analyse the different sets of beliefs held about chemical hazards by experts, workers and managers in the workplace. They found differing levels of the understandings of chemical risks. These knowledge gaps and misunderstandings helped them develop more effective chemical risk communication strategies.

Summary

Apart from SARF, the other theories discussed in this section have not been applied extensively in the risk perception literature. SARF is particularly suited for studies that examine the effect of risk communications on risk perception. Although the remaining theories are not widely applied, they have value in informing future research into risk perceptions. The network theory of contagion emphasises the importance of the social environment and how for example peer groups may affect risk perceptions. The basic risk perception model shows that adding additional factors such as attitudes, fear, trust and moral value can explain more variance in risk perceptions. Sjöberg also addresses some of the problems with previous studies by using larger, more representative samples. A technique such as mental models shows how it is possible to gain a deeper knowledge and understanding of risk perceptions.

2.4 Key Themes in Risk Perception

A number of other key themes have emerged in the risk perception literature. These are examined in the following sections.

2.4.1 Risk as Feelings

Risk can be approached in three different ways. "*Risk as analysis*" follows logical, statistical and scientific principles to arrive at a decision (as in objective risk assessments, see Section 2.3.1), "*risk as feelings*" refers to an instinctive and intuitive reaction to risks. When neither of these methods can aid us in arriving at a decision, the third option "*risk as politics*" comes in to play (Slovic *et al.*, 2004). This section examines in more detail the research findings into risk as feelings.

Early studies in the psychometric paradigm assumed risk perception followed rational decision making theories. This assumption has changed and researchers have realised that risk perception can be dependent on intuitive and experiential thinking, guided often by emotional and affective processes (Slovic, 2000b). These intuitive feelings are often the most predominant method by which individuals make decisions.

Many of the research papers that address risk as feelings focus on an emotion called "*affect*". Affect is an emotion defined as a positive (like) or negative (dislike) feeling towards an external stimulus. It can be viewed as a feeling individuals experience such as happiness or sadness, or it can be viewed as a quality assigned to a stimulus such as goodness or badness. These two conceptions tend to be related and thus research in this area has examined both conceptions. Although deliberation and analysis is important for decision making, individuals often use affect and emotion to help make quicker and easier decisions (Zajonc, 1980, Slovic *et al.*, 2004).

Alhakami and Slovic (1994) examined the importance of affect on risk perception. They observed that the inverse relationship between perceived risk and perceived benefit was linked to an individual's affective evaluation of a hazard. If an activity was "*liked*" individuals tended to judge its benefits as high and its risk as low. If the activity was "*disliked*" the judgements were the opposite. Other researchers have found a significant association between negative affect and risk perception (Johnson and Tversky, 1983,

Lerner and Keltner, 2000, 2001, Yuen and Lee, 2003). This work has been extended by Finucane, Alhakami *et al.* (1999), with the "*affect heuristic*". According to this heuristic, individuals consult an "*affect pool*" or common source containing all positive and negative images associated with the object being judged. A number of empirical studies have examined and found support for the affect heuristic such as (Finucane *et al.*, 1999, Ganzach, 2000, Lowenstein *et al.*, 2001, Slovic *et al.*, 2007a). As an example, an empirical study by Hsee and Kunreuther (2000) demonstrated that affect can influence decisions about whether to purchase insurance. They found that individuals were prepared to pay twice as much to insure a cherished antique clock (that doesn't work and cannot be repaired) than to insure a similar clock for which they have no attachment.

2.4.2 Gender Effects

A number of studies has shown that men tend to be less risk averse than women and men tend to judge risks as smaller and less problematic that women do (Slovic, 1997). Byrnes, Miller *et al*. (1999) conducted a meta-analysis of 150 studies in which the risk-taking tendencies of male and female participants were compared. Their results confirmed this. They found that certain topics (e.g., intellectual risk taking and physical skills) produced larger gender differences than others such as smoking. In addition, they found that there were significant shifts in the size of the gender gap between successive age levels and that the gender gap appeared to be growing smaller over time.

In a study of 25 hazards, Flynn, Slovic *et al.* (1994) found that males perceived the risks to be smaller than females. However non-white males and all females did not differ greatly in their perceptions. This finding has been replicated in a study by Finucane, Slovic *et al.* (2000). In this study, white males differed significantly from others in perceived risk even when age, income and education were taken into account. This has become known as the "*white-male effect*". The authors explain that this effect could be attributed to the fact that white males are more involved in creating, managing, controlling and benefiting from technology and other activities that are hazardous. Females and non-white males may perceive a greater risk because they tend to have less control and derive less benefit from these activities. This argument isn't entirely convincing. It would be surprising if males were greater risk takers in all contexts. Byrnes (2003) argues that for certain hazards, the results are quite different. For example, for smoking, results indicate that females take more risks than males. Males are more prone to take certain types of risk and females are

more prone to take others, so clearly context can be an important variable for gender differences in risk taking. Gustafson (1998) argues that explanations for gender differences should be related to gender research and gender theory and stresses the importance of the researcher being aware of the gender ideology and theory when interpreting the results of research.

2.4.3 Trust and Risk Perception

Trust is a concept that has been researched in many academic disciplines such as, sociology, psychology, economics, business and organisational management and more recently in the e-commerce literature. One of the difficulties encountered by researchers is that trust has proven complicated to define (Hosmer, 1995). Even in examining just the e-commerce literature, it is difficult to find a unified definition. Numerous definitions can be found in the e-commerce literature (e.g. Mayer *et al.*, 1995, Gefen, 2000, Jarvenpaa *et al.*, 2000, McKnight and Chervany, 2002, McKnight *et al.*, 2002, Grabner-Kräuter and Kaluscha, 2003). A succinct definition of trust is provided by McKnight, Choudhury *et al.* (2002, p299) as *"perceptions about others' attributes and a related willingness to become vulnerable to others*". A number of common elements emerge from the e-commerce trust definitions: there is a risk involved as the trustor has no control over the trustee and is therefore vulnerable. The trustor has to be therefore willing to take a risk and become vulnerable. Risk has a close relationship to trust as the need for trust is evident in risky situations (Mayer *et al.*, 1995).

One of the earliest researchers to examine the relationship between trust and risk perceptions was Paul Slovic. He contended that high public concern about a risk issue (e.g. nuclear power) is associated with distrust of the managers responsible whereas low public concern (e.g. x-rays) is associated with trust in risk managers (Slovic, 1993). In general, trust in risk management is negatively related to risk perception. Researchers believed that this relationship might prove to be a key to the development of more effective risk communications. Slovic even argued that without trust, risk communication seemed impossible (Slovic, 1993). Slovic also examined the nature of trust, he contended that trust is fragile and is easily destroyed, but it is considerably harder to rebuild and in some cases cannot be rebuilt, this has been termed the "*asymmetry principle*" (Slovic, 1993, 1997). There has been continued research interest in the relationship between risk perception and

trust. In these studies, trust in specific objects or entities (social trust) is measured rather than trust as a personality trait.

Two opposing schools of thought have emerged from this research. The first contends that trust is an important determinant of perceived risk (Flynn *et al.*, 1992). In contrast, Sjöberg (2000, 2001) has identified a number of factors, such as "*tampering with nature"* that he believes strongly affect perceived risk, as well as a large number factors that he believes have little effect, one of which is trust. In order to gain some insight into this dispute Siegrist *et al.* (2007a) conducted a meta-analysis of empirical studies from the previous 10 years that have examined the relationship between risk perception and trust. They found that some studies found risk perception to be strongly related to trust, others found a moderate relationship and others a weak one. This does lend support to Sjöberg's viewpoint. Their results suggest however, that the relationship between trust and risk perception in contingent upon certain contextual factors. The most important factors appeared to be:

a) the judged moral importance (to individuals) of the risk management issue and
b) the individuals judged personal knowledge of or familiarity with the issue.

2.4.4 Control and Risk Taking

There is a considerable literature in the psychology domain examining individual's perceived control with relation to risk taking. A number of the key concepts of relevance to this research are examined.

Unrealistic Optimism

Previous research has shown that individuals tend to believe that they are less likely to encounter negative events and more likely to encounter positive events than the average person (Weinstein, 1980). This phenomenon is known as "*unrealistic optimism*" or "*optimistic bias*". One implication of this is that individuals may believe that media/education campaigns about risky activities are directed at other members of society and not at them. For example, Tyler and Cook (1984) found that information campaigns about crime increased individual's perceptions of the danger of crime on a societal level, but not on a personal level.

Illusion of Control

Weinstein (1980) also found that if individuals felt they were in control of a situation, they were more optimistic about the outcome. Related to this is the "*illusion of control*" concept. This refers to the finding that the optimism about the outcome may be illusory in that "*an expectancy of a personal success probability is inappropriately higher than the objective analysis would warrant*" (Langer, 1975, p311). This implies that individuals might be willing to take more risks when they believe they are in control of a situation because of their belief in their own superiority when compared to the norm. Fenton-O'Creevy, Nicholson *et al.* (2003) carried out an empirical study to investigate the illusion of control concept for traders working in investment banks. They found that traders who had a high illusion of control had significantly worse performances on analysis, risk management and contribution to profits. They also earned significantly less.

Locus of Control

A similar area that has been extensively addressed in the psychology literature is "*locus of control*" (Rotter, 1966, 1990). Locus of control refers to the degree to which individuals believe that their fate is determined by their own abilities or by uncontrollable external factors such as luck. Individuals with an internal locus of control strongly believe in their self-efficacy, tending to be proactive, whereas those with an external locus of control are more likely to be doubtful and restrained. For example, students with a strong internal locus of control may believe that their grades were achieved through their own abilities and efforts, whereas those with a strong external locus of control may believe that their grades are the result of good or bad luck and are less likely to work hard for high grades. The locus of control theory has been applied in many domains. One area where locus of control has been examined is in assessing the risk taking behaviour of top executives and entrepreneurs. Research in this area has shown that internals are more likely to be entrepreneurial and more innovative than externals (Brockhaus, 1975). Internals also show a greater amount of risk taking, a tendency to be proactive (to lead rather than follow the competition) and are more likely to engage in planning (Miller *et al.*, 1982). There is a continuing argument in the psychology literature as to the causality of locus of control, whether it is an underlying personality construct or a learned construct.

Horswill and McKenna (1999) assert that the distinction between locus of control and illusion of control could be related to the comparison being made. With locus of control, individuals are asked to make a judgement whether causality is attributed to people in

general or to chance. With illusion of control, participants make a judgement of the extent to which they personally control a particular situation.

2.4.5 Risk Perception and Risk Propensity

An area that has been under researched to date is the possible link between risk perception and risk propensity. Keil, Wallace *et al.* (2000) assert that the two variables of risk perception and risk propensity appear to play a central role in decisions involving risk. Risk propensity refers to the idea that many decision makers have consistent tendencies to either take or avoid actions that they feel are risky (Sitkin and Pablo, 1992). Much of the academic research to date has investigated the effect of each of these variables on decision making separately, but some studies have examined the effects of both risk perception and risk propensity on decision making, the most cited being a study carried out by Sitkin and Weingart (1995). They found that risk propensity led to lower assessments of risk, which in turn led to riskier decision making, but other studies have found no significant relationship between risk propensity and risk perception (Palich and Bagby, 1995, Forlani and Mullins, 2000). There is also disagreement in the literature about the nature of risk propensity. Some argue that it is a general personality trait which causes individuals to demonstrate consistent risk-seeking or risk adverse tendencies across a variety of situations (Jackson *et al.*, 1972). Other research has shown that risk propensity is a situationally-specific variable which means that an individual's risk propensity can vary from one situation to another (Maccrimmon and Wehrung, 1985). If the latter is correct, it is important to measure risk propensity in context. From the literature the relationship between risk perception, risk propensity and decision-making is not clear. It is evident that further research is needed in this area.

2.4.6 Experience and Risk Perception

In a report on public perceptions of risk for the UK Foresight Office of Science and Technology, Eiser (2004) asserts that perceptions of risk are based on, and learnt from, experience. He argues that it is necessary to consider what kinds of experiences individuals have and how these contribute over time to their views on risky activities. Individuals can learn from the activities they engage in and those they listen to and trust. In practice, many of the activities that individuals engage in provide poor feedback. As an example, most of the time speeding drivers reach their destinations safely – and therefore

learn that the risks associated with speeding do not apply to them. However, to date few studies have examined the relationship between experience of a risk and general risk perceptions and these studies provide few coherent conclusions (Breakwell, 2007).

Some studies suggest that prior experience and in particular repeated exposure can lead to a desensitisation to risk where the negative effects of the risk become normalised and this leads to a lower estimation of risk (Zuckerman, 1979, Richardson *et al.*, 1987, Benthin *et al.*, 1993, Halpern-Felsher *et al.*, 2001), but in contrast other studies suggest that prior experience does not lower estimates of risk (Breakwell, 1996, Siegrist and Gutscher, 2006). Studies have found that prior experience appears to decrease optimistic bias (Perloff, 1987, Weinstein, 1987, Helweg-Larsen and Shepperd, 2001) in that people that have experienced a negative event believe they are equally vulnerable to negative events. Other studies have examined risk perceptions at a societal level and suggest that habitual experience of a risk may reduce risk perception whereas a more recent experience of the risk can enhance risk perceptions (Lima *et al.*, 2005, Breakwell, 2007). Twigger-Ross and Breakwell (1999) examined the relationship between risk experience and a number of the dimensions of risk perception defined by the psychometric paradigm. They found the effect of experience depended on whether the risks were voluntary or involuntary. Experience was primarily correlated with perceiving involuntary hazards to be uncontrollable and was correlated with perceiving voluntary risks to be better known to science and to be taken voluntarily. They found the desensitisation hypothesis was relevant for voluntary hazards but not for involuntary hazards.

It is clear that there is no consensus on the effect of prior experience on risk perceptions. As stated by Breakwell (2007), the relationship is complex. The intensity, frequency, outcome and timing of prior experience may all have an effect on risk perceptions. Further research is needed to assess how the quality of risk experiences can influence risk perception. Another consideration highlighted by Breakwell (2007) is that the experience of a risk may also be tied to risk perceptions through the information that exposure offers.

2.5 Risk Perception and IS/ICT Research

There is an extensive literature on risk management with relation to IS and ICT systems, much of which is related to managing the security of computer systems. Research in this area has found that typically organisations have not made IS risk management a priority and have not linked IS risks to business strategy (Vitale, 1986, Wah, 1998, Bandyopadhyay *et al.*, 1999, Gerber and von Solms, 2001, Smith *et al.*, 2001, Stewart, 2004). Studies have examined how risks are assessed in organisations (Rainer *et al.*, 1991, Keil *et al.*, 1998, Schmidt *et al.*, 2001, Suh and Han, 2003b) and suggestions have been made that risk assessments should take into account more of the social and human dimensions of risk (Suh and Han, 2003a, Gerber and von Solms, 2005). This area provides little of relevance to risk perception research except to note that there is a recognition that additional information can be obtained by including subjective and social measures of risk. There is also an academic literature that concentrates on software project risk, IS implementation risks and eliciting risk factors (Boehm, 1991, Kemerer and Sosa, 1991, Keil *et al.*, 1998, Lyytinen and Mathiassen, 1998, Barki *et al.*, 2001, Schmidt *et al.*, 2001, Scott and Vessey, 2002, Sherer and Alter, 2004). A review of this literature is beyond the scope of this thesis.

This section presents an overview of the literature on risk perception as applied in the IS/ICT domain. IS/ICT researchers have examined risk perceptions in an organisational context, from an end user perspective and with relation to online shopping applications.

2.5.1 IS/ICT Risk Perceptions (organisational perspective)

Some studies have examined the risk perceptions of organisational users of IS and ICT. Although the research question of this thesis is not directed at the organisational users of IS/ICT, this research is useful in providing guidance on where and how computer users and managers perceive risks in ICT systems and where organisations can mitigate these risks. Of more interest is the theory and methods applied in these studies.

In her PhD thesis, Bener (2000) using Cultural Theory examined how, in an organisational context, users discern risks and enter into communication about them. She examined risk in a project that aimed to launch an Internet banking product in a top-tier global bank. A field study and a questionnaire confirmed that individuals and institutions developed risk

perceptions according to their previous experience, the social and economic climate, their cultural backgrounds and the trust they placed in the messages and their sources.

Tsohou, Karyda *et al.* (2006) also based their research on Cultural Theory. Their paper argues that by identifying the different worldviews shared by users, security experts will be in a better position to make informed decisions on the most appropriate strategies for applying security management in different cases. For example, for individualists they suggest that methods based on cost benefit analysis are the most appropriate, whereas those with a hierarchical cultural bias would be better served by methods based on expert decisions. The findings of their research are based on theoretical analysis and are not supported by empirical research. Further research is needed to validate these claims.

The way business managers perceive and manage risks can have an impact on an organisation. An interesting and often cited paper by March and Shapira (1987) found that the way managers think about risk does not fit into classical theoretical conceptions for risk. They observed that managers' risk perceptions were based more on the magnitude of potential loss as opposed to the probability that a loss will occur. This finding was supported by a study carried out by Keil, Wallace *et al.* (2000) who examined IS managers decision making about whether or not to continue a software development project. They also explored the relationship between risk perception and risk propensity and found like Sitkin and Weingart (1995) that a managers willingness to pursue a risky project was influenced more by their risk perceptions than their risk propensities. Caution does need to be exercised in generalising findings from the Keil, Wallace *et al.* (2000) study as it was based on a sample of undergraduate business studies with limited work experience. The authors have defended this sample as previous research has shown (Ashton and Kramer, 1980) that students are an appropriate substitute for managers when the task being studied involves basic human information processing and decision-making.

Coles and Hodgkinson (2008) used the psychometric paradigm to examine end-users perceptions of IT risks in the workplace. Their study was based on a small sample of 57 end-users. Their result differs from the commonly found two factor solution of unknown and dread risks and indicated that a six dimensional solution was required. The dimensions reflected the extent to which the risk scenarios were perceived as: (1) serious or minor in nature; (2) having a high or low probability of occurrence; (3) causing a high or low degree of stress; (4) deliberate or accidental; (5) having an impact on the

organisation or on individuals and (6) the product of human or technological causes. Coles and Hodgkinson explain that this is because the subject being investigated is more complex than those investigated in previous studies and some previous studies of risk perceptions in homogeneous domains have produced similarly complex solutions. An obvious limitation with this study is the small sample size. Although the findings of this study hold little relevance for the research topic of this thesis, the study does show a successful application of the psychometric paradigm in the IS domain.

2.5.2 IS/ICT Risk Perceptions (users' perspective)

The research literature examining end users' risk perceptions with relation to IS/ICT, although limited has examined risk perceptions from a number of different angles. These include how users perceive IT risks, how IT risks are communicated to users and risk perceptions with relation to specific IS/ICT issues such as the millennium bug.

Risk Perceptions of IS/ICT Users

A number of studies has compared IS/ICT risk perceptions to other risk areas. Frewer, Howard *et al.* (1998) carried out empirical research to assess attitudes to various technologies such as nuclear energy, food additives, solar power and IT. They found that the perceived benefits of IT were quite high in comparison with the other technologies and the perceived risks were quite low. This finding in itself is not surprising when a comparison is made between IT and a technology such as nuclear energy. Sjöberg and Fromm (2001) examined a mix of IT risks such as fraud, privacy intrusion, criminal behaviour and technical problems (e.g. viruses) and a variety of other risks such as alcohol, smoking and pollution. Their study was based on a random sample of the entire Swedish population. They found that the ratings for personal risk and general risk for IT risks were similar to other controllable lifestyle risks such as smoking and alcohol, but differed from other uncontrollable risks such as nuclear power. They found that the use of IT was strongly related to a general attitude towards computers rather than risk perception. This finding is in contrast with risk perception studies in other domains, where risk perception has a dominant influence on behaviour. Sjöberg and Fromm argue that this could be because users have a feeling of personal control over the technology and this can counteract the perceived risk. Another possible explanation is that the perceived benefits of IT outweigh the perceived risks, but this aspect was not addressed in this study. Sjöberg

and Fromm found that IT risks were seen as more pertinent for others, showing evidence of an optimistic bias.

An empirical study by Campbell *et al.* (2007), although only based on a sample of 97 students, also found support for an optimistic bias. They examined 31 IT events, 14 of which were positive and 17 were negative. They found that students believed positive Internet events were more likely to happen to them and negative events were less likely to happen to them compared to the average student, this was particularly evident for intensive computer users. They also found that controllability, desirability and personal experience were correlated with unrealistic optimism.

A study investigating the factors that can influence a user's perception of different threats to information security was carried out in China by Huang, Rau *et al.* (2007). They categorised the common threats to information security using 12 categories proposed by Whitman (2003) and measured these against 20 risk factors that they derived from the psychometric risk perception literature. They found that the factors of "*Knowledge*", "*Impact*", "*Severity*" and *"Possibility*" had significant effects on the perceived overall danger of the threats. The authors did not present any further discussion of these findings, their implications for information security or how they relate to previous findings of other psychometric studies.

A UK survey by Furnell, Bryant *et al*. (2007) addressed user's awareness of computer security threats and the safeguards available to them. The findings showed that although respondents were aware of the threats and used the relevant safeguards, many respondents lacked a deeper knowledge and understanding of these threats and safeguards. This was most prominent amongst novice users, but was also evident amongst users who considered they had advanced levels of computing experience.

Communicating Risks

Studies have examined how users learn about IS/ICT security risks. Furnell, Bryant *et al.* (2007) found that the majority of users gained their awareness of security threats from informal sources such as family and friends and not from professional sources. Sjöberg and Fromm (2001) found that informal sources were important, but also found that some media (TV, radio, specialised magazines) had a role in informing individuals about

security threats. Sjöberg and Fromm found that computer vendors and software developers were the least trusted for information on security threats.

Dowland, Furnell *et al.* (1999) addressed the impact of the media in shaping individuals perceptions and opinions of computer crime. They found that the media was successful in terms of making people aware of computer crime, but the media has not been successful in raising awareness of possible corrective actions. The authors warn that the media could have negative effects upon those who are less familiar with the area.

In the Social Amplification of Risk Framework (SARF), it is clear that the way in which a risk message is communicated can have an influence on risk perception. Pattinson and Anderson (2006, 2007) have used SARF to examine how IT risk behaviour can be changed by risk communications. Their basic premise was that if user's perceptions of the risk associated with information security threats are heightened, then it was likely that they would act in a more desirable manner. They tested this assumption by adding human factor variables (such as symbols and graphics relating to information security) to risk communications to see if they influenced the risk perceptions of end users. Unfortunately their empirical research presented no statistically significant differences between messages sent with embedded graphics and those with none.

Millennium Bug

A number of authors have examined users risk perceptions in relation to the Millennium bug.

Goldstein *et al.* (2002) examined the role of personality characteristics and computer anxiety in predicting reactions to millennium bug. They found that the millennium bug was particularly anxiety provoking for individuals who generally tend to be anxious, who are strongly religious and who lack a strong desire for control. Although religiosity may seem a strange construct to be included in a study of IS and ICT, it is a construct that has been found to be important in perceptions of technological hazards such as nuclear power. It is unclear whether it has such a logical role with respect to IS/ICT risks. Another interesting finding in this study is that individuals who do not have a strong desire for control were more anxious about the millennium bug, although intuitively this does not seem to make sense. Goldstein *et al*. suggest that this may be due to the fact that their study was carried out in late 1999 and many individuals that had a strong desire for control

would have already implemented controls to cater for the millennium bug. The study also found that computer use and age were not significant predictors of Y2K anxiety.

MacGregor (2003) carried out an empirical analysis using concepts from the social amplification of risk framework (SARF) to examine the Y2K issue. He found that media reporting of Y2K tended to lead to a decrease in the perceived severity of Y2K problems for society and for individuals personally, but increased awareness of the Y2K issue. He argues that the greater awareness of Y2K led individuals to protect themselves (by for example stockpiling food and water, getting alternative forms of power, avoiding air travel etc.) and thus attenuating the potential impact of Y2K on their personal lives.

Gutteling and Kuttschreuter (2002) examined if there was a difference between laypeople and experts risk perceptions relating to the millennium bug. They found some differences but not as large a difference as was found by other studies using the psychometric paradigm. They suggest that this may be due to the fact that the millennium bug was not politically controversial. They (Kuttschreuter and Gutteling, 2004) carried out another study 10 months and a few weeks before the millennium to see if risk perceptions, the ability to mitigate the risks and the availability of information differed between the two time periods. Not surprisingly, the authors found that there was a significant decrease in the perception of risk, a significant increase in the perceived risk mitigation at the personal and societal level, a significant increase in the perceived awareness of the problem among the general public and a significant decrease in the need for information. Kuttschreuter and Gutteling (2004) contend that this research shows that it is possible for risk communicators to design a risk strategy that can successfully inform the general public about computer risks. The study did not examine the role of informal sources such as family and peers to see if they have a larger effect on risk communications as suggested by Furnell, Bryant *et al.* (2007) and Sjöberg and Fromm (2001).

Summary

There is not an extensive body of research examining risk perceptions with relation to IS/ICT and such studies as there are have examined risk perception from a number of different angles. Some studies have addressed how IT risks compare to other risk areas and have found, quite predictably, that IT risks are perceived as small. A number of studies have examined if IT users are aware of security risks and have found support for the optimistic bias. Researchers who have looked at the way IT risks are communicated to

users have found that informal sources such as family and peers are an important and trusted source of information. Some studies investigated risk perceptions of the millennium bug. Most of these studies were carried out near to the millennium and thus found that users were aware of the issues. As these studies have examined different aspects of IS and ICT risk areas there is little benefit in examining if there is any commonality in the risk characteristics studied. A number of risk perception theories, including the psychometric paradigm, Cultural Theory and SARF, have been successfully applied in the IS/ICT domain. Appendix A summarises the papers presented in this section (including those from an organisational perspective) and shows the theory underlying each of these studies, the sampling details, the research question and the main findings.

From a methodological viewpoint, the majority of these studies have utilised questionnaires. Although some studies have used random samples from nationally available databases (Sjöberg and Fromm, 2001, Gutteling and Kuttschreuter, 2002, MacGregor, 2003, Kuttschreuter and Gutteling, 2004), others have used convenience samples of students (Keil *et al.*, 2000, Goldstein *et al.*, 2002, Campbell *et al.*, 2007, Pattinson and Anderson, 2007) or posted their questionnaires on web sites with the consequence that the sample becomes self-selecting (Furnell *et al.*, 2007, Huang *et al.*, 2007). This lack of representativeness means that generalisations cannot safely be made from these studies and this is further exacerbated by the gender and age imbalances in some of the studies.

Although there are not many risk perception studies in this area, authors have commented on how risk perception theories could be applied in the IS/ICT area. As already stated, in the psychometric paradigm two common factors have emerged repeatedly in empirical studies, the dread and unknown risk factors. Jackson, Allum *et al.* (2004a) assert that the second factor is of more relevance in IS/ICT research. They contend that many users of IS/ICT are overconfident, feel in control of the technology and can see the benefits of technology and this may prevent them from seeing the risks involved with technology. At the other extreme, some IS/ICT users may not be as confident and thus have a lower level of trust in these systems. This means that they can be vulnerable to the risks of the technology. The psychometric paradigm could be used to determine whether intensive users of IS/ICT have a sense of familiarity and control that desensitises them to the risks of the technology (Collins and Mansell, 2004).

Jackson, Allum *et al.* (2004a) have suggested several ways that research into heuristics and biases could be useful for future research into cyber crime. Using a judgement based on the *availability heuristic* means that a dramatic or well-publicised cyber crime could be more easily brought to mind and therefore judged to be more likely to occur. For example, an incident involving paedophilia and chat rooms might give the impression that such incidents are widespread. Policy makers need to be aware of this effect and stress the unusual nature of such instances. For judgments based on *representativeness*, the importance of individual events can take precedence over expert assessments, this means that individual experiences of various forms of cyber crime can have a greater impact on an individual's perception of cyber crime. In this instance it can be very difficult to change public perception. *Prospect theory* shows that the pain from a loss is greater than the satisfaction from a similar amount of gain. For cyber crime there are benefits to using ICT, however, Jackson, Allum *et al.* contend that perceived losses will affect the overall evaluation of the technology to a greater extent than perceived benefits.

A number of authors have emphasised the point that concern over IS/ICT risk tends to be technical and does not address the social aspects (Adams and Sasse, 1999, Gonzalez and Sawicka, 2002, Backhouse *et al.*, 2004, Besnard and Arief, 2004, Dourish *et al.*, 2004, Cranor, 2008). Information systems are essentially social systems that rely on an important technical component, but it is important that studies of IS/ICT risk also address the social aspects.

2.5.3 Risk Perceptions of Online Shopping

There is one domain in the IS literature where risk perception has been extensively researched and that is in examining the risk perceptions of consumers with relation to Internet shopping transactions. Perceived risk has been examined in this literature as it is useful in identifying and explaining the barriers to Internet shopping (Forsythe and Shi, 2003). This section provides a synthesis of the literature in this area and suggests how this research can inform the research topic of the thesis.

Research into the perceived risk of online consumer behaviour can be broadly broken down into three areas where:

1. perceived risk is studied as part of the trust construct;

2. perceived risk is studied in the context of the technology acceptance model (TAM); and
3. perceived risk is studied as a construct as defined by consumer behaviour researchers.

Trust and Perceived Risk in Internet Shopping

As discussed in section 2.4.3, trust and risk are closely interrelated (Mayer *et al.*, 1995) Trust is considered to be of critical importance for success in e-commerce, particularly because of the high degree of uncertainty and risk present in most Internet transactions (Jarvenpaa *et al.*, 1999, Reichheld and Schefter, 2000). A number of online shopping studies have examined perceived risk as part of the trust construct. As pointed out by Gefen *et al.* (2003), these studies have differed in how they have addressed the relationship between trust, risk perception and behaviour. Some studies have examined the effect of perceived risk and trust on behaviour but have not hypothesised on the relationship between risk and trust, for example Kim and Prabhakar (2000). McKnight *et al.* (2002) proposed the Trust Building Model which suggests that the constructs for both risk and trust should be studied as distinct variables. Other studies, for example Jarvenpaa *et al.* (2000) have proposed a mediating relationship, in that trust affects perceived risk which in turn affects behaviour.

These studies have found that trust reduces perceived risk and this in turn influences intentions to purchase online (Grazioli and Jarvenpaa, 2000, Jarvenpaa *et al.*, 2000, Pavlou, 2003). McKnight *et al.* (2002) found that perceived Internet risk had a significant impact on intentions to share information and to purchase.

Perceived Risk and the Technology Acceptance Model

A number of researchers have examined trust and perceived risk in the context of the technology acceptance model (TAM). Pavlou (2003) argues that because e-commerce and Internet shopping requires consumers to interact with web sites and use Internet technologies, it is justifiable to consider the variables of the TAM in predicting intentions to transact online. The TAM suggests that two external variables, perceived usefulness and perceived ease of use influence the acceptance of Internet technology (Davis, 1989b, Venkatesh *et al.*, 2003). Pavlou (2003) and Van der Heijden *et al.* (2003) have suggested models which integrate the variables of trust and perceived risk with the TAM constructs. Other studies have not included the trust construct and have just examined perceived risk

in the context of the technology acceptance model (TAM), for example Liu and Wei (2003).

Similarly to the previously reported studies, Pavlou (2003) found that trust and perceived risk were direct antecedents of the intention to transact. He also found that perceived usefulness and ease of use had a significant effect on transaction intentions. Van der Heijden *et al.* (2003) present contradictory findings. They found that perceived risk and perceived ease of use were direct antecedents of the intention to purchase, but they did not find a positive effect for trust or perceived usefulness. Liu and Wei (2003) found different results depending on what was being purchased. Their results showed that when considering purchasing goods over the Internet, consumers decisions were more strongly influenced by their perceptions of risk. In contrast, when considering purchasing services over the Internet, consumer's decisions were more strongly influenced by their perceptions of ease of use.

Perceived Risk and Consumer Behaviour Research

Perceived risk has been a central concept that has been examined in the consumer behaviour literature (Cox and Rich, 1964). Researchers in this area define perceived risk as a consumer's perceptions of the uncertainty and adverse consequences associated with buying a product or service (Cunningham, 1967). Research has shown that individuals perceive risks in most purchase decisions (Cox, 1967). Consumer behaviour researchers see perceived risk as multidimensional. As described in Table 2.3, perceived risk is commonly decomposed into six components; these are financial, product performance related, psychological, physical, social and time related risks (Roselius, 1971, Jacoby and Kaplan, 1972, Kaplan *et al.*, 1974). Subsequent research has identified further components of perceived risk, some of which are relevant to Internet shopping, as shown in Table 2.4.

Perceived Risk Categories	Description
Financial	Financial risk is defined as the danger of economic loss.
Product performance	Product performance risk is defined as the loss incurred when a brand or product does not perform as expected.
Psychological	Psychological risk refers to how a consumer may be affected psychologically by a purchase, for example disappointment or shame if personal information is disclosed.
Physical	Physical risk involves the potential threat to an individual's safety, physical health and well-being.
Social	Social risk is felt when consumers feel that their reputation or social standing is at risk.
Time Related	Time-related risk refers to the possibility that a purchase will take too long or waste too much time.

Table 2.3 Common Categories of Perceived Risk

Perceived Risk Categories	Description
Privacy	Privacy risk is related to the potential loss of control over personal information, such as when personal information is used without knowledge or consent.
Technological	Technological risk refers to the fear of technologically complicated innovations.
Opportunity cost	Opportunity cost risk refers to the possibility that an improved or lower cost product may be available at a future time which would be precluded by a current purchase
Information	Information risk refers to the possibility that an individual is operating in an environment of asymmetric information.

Table 2.4 Further Categories of Perceived Risk

A number of researchers have used these categories of perceived risk to identify and explain the barriers to Internet shopping. Forsythe and Shi (2003) examined the types of risks perceived by Internet shoppers and their potential impact on Internet patronage behaviour. They examined the common categories of perceived risk, see Table 2.3, but did not examine the physical or social components of perceived risk. A study by Featherman and Pavlou (2003) also examined risk perception and the TAM but decomposed risk perception into its components in order to examine what types of risks are important for Internet consumers. The study excluded the physical safety risk as the authors felt this was irrelevant in an online setting, but they included a privacy risk component (see Table 2.4). Lu *et al.* (2005) also examined risk perception and the TAM with relation to the acceptance of online antivirus applications. They decomposed risk perception into the components of physical risk, performance risk, social risk, time-loss risk, financial risk and added the components of opportunity cost risk and information risk, as described in Table 2.4. They did not include the privacy risk component.

These studies have also found a negative relationship between perceived risk and purchasing intentions (Tan, 1999, Bhatnagar *et al.*, 2000), but Forsythe and Shi (2003) found that although current Internet shoppers perceive several risks, these risks did not influence their shopping behaviours in an extensive and systematic way. They did find however, that perceived risk had an impact on potential Internet shoppers. Featherman and Pavlou (2003) found that the performance, financial, privacy and time related risk categories were the most salient as they lead to a reduced system evaluation and adoption.

Other Studies of Risk Perception and Internet Shopping

Miyazaki and Fernandez (2001) studied perceived risk as it relates to privacy and security and its effect on online shopping. They investigated whether higher levels of Internet experience are related to lower levels of perceived risk and concern regarding the privacy and security of online shopping. They found that having a higher level of Internet

experience lowered perceived risk towards online shopping. Like Forsythe and Shi (2003), they found that respondents were aware of and concerned about the privacy issues and potential fraudulent behaviour of online retailers, but these concerns were not predictive of online purchase rates.

Liebermann and Stashevsky (2002) expanded on the work of Miyazaki and Fernandez. They too looked at usage behaviour but included other demographic variables, such as gender, age, marital status and education. They found that both demographics and usage behaviour have an effect on perceived risk, but that these perceptions differed depending on the risk. For example, they found that females and Internet users that do not purchase online perceived a higher risk with Internet credit card stealing. Those that perceived a higher risk with supplying personal information were older individuals (age>35), married individuals, Internet users that do not purchase online and lower level Internet users. The main finding of their study was that two perceived risks: Internet credit card stealing and supplying personal information had a crucial effect on online shopping usage.

At the time of writing, an extensive review of the literature has only found one paper that has used the psychometric paradigm to empirically examine online shopping risk perceptions. Gabriel and Nyshadham (2008) examined 21 online shopping hazards and 14 risk characteristics. They found that subjects distinguished online shopping risks using four dimensions: direness of consequences, ability to control or avoid risks, observability/immediacy of risk consequences and unfamiliarity of risks. They also constructed a cognitive map of respondents' online risk perceptions and attitudes. The top five risky hazards were: identity theft; unauthorised use of credit or debit cards; theft of a customer's login information; unauthorised use of consumers' personal data and dealing with a fake web site. This study shows that the psychometric paradigm can be successfully applied in the online shopping domain.

Summary and Discussion

As this literature does not directly relate to the main focus of this research, this section has not extensively examined the empirical research in this area but rather has reviewed the most commonly cited papers in this area. The findings of these studies are not of major significance to this research, except to note that these studies have generally found that risk perceptions negatively affect a consumer's intention to transact or purchase online. The main findings and the samples used for each study are presented in Appendix B.

Reviewing the theoretical underpinnings of these studies has been more informative and has highlighted a number of areas of concern as to how risk perception has been addressed in the online shopping area. There are three main approaches that have been adopted by researchers examining the risk perceptions of Internet shoppers. The first approach has examined how risk perception and trust are related to a consumer's intention to transact online. The second approach examines how risk perception and the TAM affect online shoppers. The third approach builds on research developed by consumer behaviour researchers and how this applies in an Internet shopping setting. Some other studies have examined online shopping risk perceptions from a privacy perspective and only one study has used the psychometric paradigm.

A criticism of the studies that have examined perceived risk and trust and perceived risk and the TAM, is that these studies have treated perceived risk as a unidimensional construct despite the fact that a large body of literature indicates that it is a complex, multidimensional construct. The studies that have examined risk perception as defined by consumer behaviour research have recognised the multidimensional nature of risk perception and have examined risk perceptions at a more granular level. Some of these studies have included other factors such as Internet usage but do not seem to fully recognise the complexity of risk perception. Only one study employed the psychometric paradigm but did not account for the many psychosocial factors that are now recognised as having an impact on risk perception.

No consensus has been reached in the models presented regarding the relationship of perceived risk with other constructs. As an example, the relationship between perceived risk and trust, for some perceived risk and trust are not related (Kim and Prabhakar, 2000, McKnight *et al.*, 2002) and for others perceived risk has a mediating relationship between trust and intention to transact/purchase (Jarvenpaa *et al.*, 2000, Pavlou, 2003, Van der Heijden *et al.*, 2003). A similar lack of consensus is evident in the risk perception and the TAM literature.

A further area of concern is the extensive use of students as subjects in these studies (see Appendix B). The use of university students has been justified in studies of this nature as students are generally quite experienced Internet users and similar in age to general Internet consumers. This argument has some validity, but it is still questionable as to whether students are representative of Internet shoppers, as they do not have the financial resources of working adults and their purchasing patterns may also differ.

2.6 Risk Perception and Adolescents/Emerging Adults

This section examines the risk perception research literature related to adolescent and emerging adults risk perceptions. The section begins with a summary of the main findings from the adolescent risk taking and risk perception literature. This is followed by a discussion of the literature pertaining to emerging adults. The section concludes with a discussion of a number of concerns with relation to studies in this area.

2.6.1 Adolescents

A substantial body of research has examined risk taking in adolescence as it is believed that adolescence is a relatively high-risk stage of life especially with regard to health risks such as smoking, drinking, having unprotected sex and drug taking (Jessor, 1984). Arnett (1992) makes a distinction between "*risk*" and "*reckless*" behaviour. "*Risk*" behaviour refers to thrill seeking and socially approved risks such as motorbike riding, snowboarding and bungee jumping. "*Reckless*" behaviour refers to those actions that are not socially approved such as substance use and abuse, dangerous driving and unprotected sex. The decision for adolescents to engage in risk taking can stem from curiosity, thrill seeking, peer pressure, an escape from stress, rebellion against authority, a desire for self-discovery, self-improvement, creativity or an expansion of consciousness (Ben-Ari, 2004). Many researchers believe that risk taking is an essential part of the transition from adolescence to adulthood and can be viewed as a positive aspect of the development process (Jessor, 1984, Baumrind, 1987, Chassin *et al.*, 1989, Jessor, 1991). Adolescents should therefore not avoid all risks in their environment, but should learn to discriminate between risks that should be taken and risks that should be avoided (Miller and Byrnes, 1997). It is important to acknowledge that the negative connotations that adults associate with risky behaviour are not necessarily viewed in the same manner by adolescents (Furby and Beyth-Marom, 1992).

A large body of research literature exists that has explored the experiences, perceptions, attitudes, emotions and motivations of adolescence in order to get a better understanding of their risk taking. This section presents the key findings from the adolescent risk taking literature and in particular the literature that has examined risk perception. This section has been divided into the internal and external influences on risk behaviour.

Internal Influences

A number of internal factors can influence an adolescent's risk behaviour. These include biological factors, psychological and behavioural factors.

Biological Factors

Biological factors refer to the physical characteristics of individuals that are not modifiable by environmental or social forces.

Age: It is a well establishing finding that older adolescents (late teens and early 20's) are more likely than younger adolescents to engage in more reckless behaviours (Arnett, 1996, DiClemente *et al.*, 1996, Goldberg *et al.*, 2002), but do risk perceptions and judgements also change with age? With regard to risk judgements, some studies have found age differences with older age groups outperforming younger age groups (Chassin *et al.*, 1989, Smith and Rosenthal, 1995, Halpern-Felsher and Cauffman, 2001) but others have found none or a few age related differences (Beyth-Marom *et al.*, 1993, Quadrel *et al.*, 1993). Millstein and Halpern-Felsher (2002a) found that risk perception showed an inverse relationship to age, where younger adolescents perceived greater risk than did older adolescents and adolescents perceived greater risk than did young adults. Other studies have confirmed these findings (Gullone and Moore, 2000, Gullone *et al.*, 2000). Care has to be taken in generalising the results from these studies as some of these studies have used young adults or parents as representative of adults in general, but it would appear that as adolescents mature they have the ability to judge risks in the same way as adults and that risk perceptions decrease with age.

These findings present something of a paradox. Intuitively it would make sense to assume that as adolescents mature and cognitive decision making and risk judgements improve that this should decrease the likelihood of participation in risks. A number of possible explanations have been presented for this paradox. One possible explanation is the affect heuristic (as discussed in section 2.4.1), where individuals don't always use "*risk as analysis*" methods which use logic, reason and scientific deliberation but instead use "*risk as feelings*" methods where they adopt fast, instinctive and intuitive reactions to risk. Another possibility is that adolescents may perceive the benefits of the risk to be greater than the negative aspects of the risk and thus continue to engage in a risky behaviour. Adolescents may perceive themselves to be invulnerable and that the risky behaviour will not affect them. The effect of peers can also be substantial in adolescence and it is

understandable that adolescents may succumb to peer pressure to engage in an activity even though they perceive the risks. Each of these explanations is discussed in detail in further sections.

Gender: As stated in section 2.4.2, it is a common finding in risk perception research that males perceive less risk than females. Many studies of adolescents confirm this view, as an example Parsons *et al.* (1997) found that adolescent females perceived greater risks and fewer benefits associated with drug use, alcohol use and sexual behaviour than adolescent males. Although as highlighted in section 2.4.3, context is important. Care has to be taken not to assume that females' risk perceptions will be higher for all risky behaviours.

Race: Although many studies assessing adolescent risk perceptions have collected data on ethnicity, as can be seen in Appendix C, few studies have presented findings on ethnic differences. It is not clear whether ethnic differences were found in these studies or whether they were not reported. It is likely to be the former as the samples taken were usually within one school or university and are thus confounded with socio-economic status (SES) so it is probably unlikely that ethnic differences would be evident.

Psychological and Behavioural factors

Relationship between Perceived Risks and Behaviour: There are a number of theories that assert that an individual's beliefs about the consequences of their actions and their perceptions of risk play a key role in their subsequent behaviour. These theories include Social Cognitive Theory (Bandura, 1986), the Theory of Reasoned Action (Fishbein and Ajzen, 1975), the Theory of Planned Action (Ajzen, 1985) and Self-Regulation Theory (Kanfer, 1970). These theories agree that a high perceived risk of harm should encourage people to take action to reduce their risk. The difficulty arises when it comes to testing these theories. To validate these hypotheses it would be necessary to study an individual's beliefs before they engage in a risky behaviour and then it would be necessary to follow them longitudinally to see whether they eventually engage in the specific behaviour (Millstein and Halpern-Felsher, 2002b). Few studies have adopted such a longitudinal approach. One such study by Gerrard *et al.* (1996a) found that health cognitions did predict risk behaviour in adolescents. Most research studies have looked at the differences in risk perception between people who engage in risky behaviours and those who do not. The majority of empirical studies on adolescents have found positive associations between risk perceptions and behaviours (Moore and Rosenthal, 1991, Lavery *et al.*, 1993, Cohn *et*

al., 1995, Gerrard *et al.*, 1996b), but some studies have found a negative relationship (Benthin *et al.*, 1993).

These findings do not appear to fully support the argument that adolescents engage in more risky behaviours as they get older. There is the possibility that these findings are context specific. For example, a meta analysis carried out by Brewer *et al.* (2007) examined the relationship between risk perception and vaccinations, not surprisingly they found a positive relationship between risk perceptions and vaccination behaviours. In other behaviours such as smoking, the relationship may not be so clear cut. Although adolescents and particularly adolescent smokers appear to be aware of the risks of smoking (Viscusi, 1990, Viscusi, 1991, Viscusi, 1992), they continue to engage in the behaviour. Explanations include the adolescent's optimism bias in thinking that the negative effects won't happen to them, the failure of smokers to consider the cumulative nature of the risk and the fact that many adolescents don't think they will become addicted to cigarettes (Slovic, 2000a).

Invulnerability: Adolescent risk behaviour is often attributed to exaggerated feelings of invulnerability, i.e the negative consequences associated with risky behaviours will happen to others but will not happen to them. Elkind (1967) provided a theoretical basis for this view with his concept of adolescent egocentrism. He postulated two phenomena that occur when adolescents try to conceptualise the thoughts of others:

1. *The imaginary audience*: in which adolescents fail to differentiate others' thoughts from their own (seeing themselves as being as central to others' thinking as they are to their own);
2. *The personal fable*: this is the view that adolescents feel they are special and in some way immune to the natural laws that pertain to others and are thus invulnerable to harm.

Although Elkind's theory is intuitively appealing, empirical studies of the relationship between perceived invulnerability and adolescent risk taking have produced mixed results. Some studies have found that only a small minority of adolescents perceive themselves to be invulnerable and that most adolescents report feeling some degree of vulnerability to negative outcomes (Quadrel *et al.*, 1993, Millstein and Halpern-Felsher, 2002b, a). Other researchers have found no age differences and that adolescents and adults seem to rate the

likelihood of negative consequences similarly (Beyth-Marom *et al.*, 1993, Cohn *et al.*, 1995).

Unrealistic Optimism: Researchers have examined the related concept of unrealistic optimism (also known as optimistic bias) as previously described in section 2.4.4. This is where individuals believe that they are less likely to encounter negative events and more likely to encounter positive events than the average person (Weinstein, 1980). Unlike invulnerability, many studies of adolescent risk perceptions have found support for this concept (Hansen and Malotte, 1986, Benthin *et al.*, 1993, Cohn *et al.*, 1995). Research has shown that unrealistic optimism is higher for risks that are judged to be controllable by personal action, such as lifestyle risks. It is also higher when individuals believe (often incorrectly) that if the problem has not yet appeared, it is unlikely to occur in the future (Weinstein, 1987). Smoking fits into both of these categories and it is a common finding that adolescents underestimate the risk of smoking to themselves (Slovic, 2000a).

Some studies have examined whether unrealistic optimism differs between adults and adolescents. Cohn *et al.* (1995) compared unrealistic optimism between adolescents and their parents. Their results indicated a stronger optimism for adolescents, as adolescents were less likely than their parents to believe that taking part in various risky activities might result in harm. Arnett (2000b) compared unrealistic optimism between adolescent and adult smokers and non-smokers and found a stronger optimism for adolescents. He also found that a majority of adolescent and adult smokers and non-smokers agreed that smoking is addictive and caused death for "*most people*" who smoke. However, for themselves personally, adolescent and adult smokers were more likely than non-smokers to doubt that they would die from smoking even if they smoked for 30 or 40 years.

Affect. Research into adolescent risk-taking has also begun to examine the role of affect. Affect has been described in section 2.4.1. Findings indicate there is evidence that affect is also relevant for adolescents (Arnett *et al.*, 1997, Hussong *et al.*, 2001, Pardini *et al.*, 2004, Sigfusdottir *et al.*, 2004, Curry and Youngblade, 2006).

Researchers of the "*affect heuristic*" have developed a technique called affective image analysis, which uses a structured form of word association and content analysis. It has proved a useful method to investigate the relationship between affect, imagery and perceived risk. Benthin *et al.* (1995) used this methodology to examine the ways in which

adolescents perceived risks and benefits related to health-threatening and health-enhancing behaviours. Cigarette advertising and promotion has been designed to present young people with positive images of smoking. Research has demonstrated how powerful such imagery can be in suppressing perception of risk and manipulating behaviour (Finucane *et al.*, 1999, Slovic *et al.*, 2007a)

Sensation Seeking. Zuckerman (1994, p27) defines sensation seeking as "*a trait defined by the seeking of varied, novel, complex and intense sensations and experiences, and the willingness to take physical, social, legal and financial risks for the sake of such experience*". Research has shown that there is a significant association between sensation seeking and risk taking (Zuckerman and Neeb, 1980, Zuckerman *et al.*, 1990, Arnett *et al.*, 1997). In addition, high sensation seekers tend to perceive less risk in many activities and to anticipate more positive potential outcomes that do low sensation seekers (Igra and Irwin, 1996). Sensation seeking, which peaks in adolescence, is associated with adolescents and young adults participating in a range of risky activities (Arnett, 1996, Donohew *et al.*, 2000, Hampson *et al.*, 2001, Bradley and Wildman, 2002).

Perceived benefits versus perceived risks. In the past, some researchers labelled adolescents as "*irrational*" because they engaged in risky behaviours despite their knowledge of the risks (Loewenstein and Furstenberg, 1991). This may be due to the fact that many studies did not include a benefits component addressing the perceived benefits of the high-risk behaviour itself (Goldberg and Fischhoff, 2000, Goldberg *et al.*, 2002). Studies that have examined the benefits of risks have found that adolescents perceived benefits to self are more predictive of risk taking behaviour than are perceived risks (Furby and Beyth-Marom, 1992, Benthin *et al.*, 1993, Benthin *et al.*, 1995, Gerrard *et al.*, 1996a, Moore and Gullone, 1996, Parsons *et al.*, 2000) and that this is more prevalent amongst older adolescents (Lavery *et al.*, 1993, Siegel and Cousins, 1994, Parsons *et al.*, 1997). This finding is not particularly surprising, as Jessor (1991) states, individuals choose to engage in risky behaviours such as smoking not because they are seeing if they can avoid lung cancer but because they offer an immediate gain or benefit, which the individual judges (consciously or unconsciously) to be worth the long-term risk of negative consequences.

Problem behaviour syndrome. One theory that has emerged from research into adolescent risk-taking is "*Problem-Behaviour Theory*" (Jessor and Jessor, 1977, Jessor,

1984, 1987). This theory examines the psychological, social and behavioural characteristics of adolescent risk taking. One finding of studies using this theory is that risky-behaviours tend to be inter-related, so a trait (e.g. honesty) will exist in all contexts that call for this trait. Researchers that support this view have found that behaviours such as regular smoking, binge drinking, illicit drug use and unprotected sex are often moderately correlated (Donovan *et al.*, 1988, Osgood *et al.*, 1988, Benthin *et al.*, 1993, Biglan and Cody, 2003). An alternative view is that behaviour is much more situation specific (e.g. honest in one situation but dishonest in another), empirical research that back up this view has found low correlations between various measures of risk and have found multiple-factor solutions for risky behaviour (Shaw *et al.*, 1992, Boverie and Scheuffele, 1994, Gullone *et al.*, 2000).

External Factors

A number of external factors can also influence an adolescents risk taking behaviour. This can include parental influences and influences outside the family such as peers and school environments. Clearly other social influences such as the mass media and other cultural, economic and societal systems can also exert influence on behaviour. For example there is a literature that has addressed the effects of role models on risk taking behaviour (Perry *et al.*, 1992, Yancey *et al.*, 2002). However, it is believed that the impact of these macro-systems permeate through micro-level systems such as the self, family, peer and school effects (Bronfenbrenner, 1979), thus this discussion concentrates on these external factors.

Parental influence. Parents and guardians have been identified as an important source of influence on adolescent's risky behaviour. Parental influence can be divided into family structure variables and family process variables. In general the latter has received more attention, but structural variables, such as single parent families, SES and parental education should not be ignored. For example, research into risky sexual behaviour by Baumeister *et al*. (1995) found that a predictor of adolescent pregnancy was having a non-intact family. Devine *et al.* (1993) showed that parental divorce during early adolescence was a significant predictor of sexual risk behaviour in later adolescence.

Most research has been carried out on family process variables. Numerous studies have shown that parental monitoring and control are inversely associated with involvement in risk-taking behaviours (Barnes and Farrell, 1992, Dishion and McMahon, 1998, Beck *et al.*, 1999, Wright and Cullen, 2001, Borawski *et al.*, 2003). However the optimum level of

parental control has not been determined and exerting too much control can lead to negative consequences (Rodgers, 1999). The way adolescents perceive their relationship with their parents is another important predictor of risk-taking behaviour. Research has shown that negative family relations increase adolescents' involvement in risky behaviour (Igra and Irwin, 1996, Resnick *et al.*, 1997, White *et al.*, 2000, Repetti *et al.*, 2002) and poor parent-child communication is also related to adolescent's risky behaviour (Turner *et al.*, 1993, Baumeister *et al.*, 1995, Whitaker and Miller, 2000, Blake *et al.*, 2001).

Peer influence. Peers are an important source of reinforcement, modelling and support during adolescence and peer influence is acknowledged as a major variable in adolescent risk-taking. A study by Jessor and Jessor (1977) found that adolescents who engage in high-risk behaviour perceived greater support for their risk-taking behaviour from their peers and also reported having more friends who engage in such behaviours. Research has shown that adolescents' perceptions of their peers behaviours predict their own behaviour (Benthin *et al.*, 1993, Romer *et al.*, 1994, Miller *et al.*, 2000). It is also commonly acknowledged that peers can exert pressure on others into risk-taking behaviours, and many studies have demonstrated that adolescents who associate with peers that engage in risky behaviours are themselves more likely to engage in risky behaviours (Benthin *et al.*, 1993, Gerrard *et al.*, 1996a, Gardner and Steinberg, 2005).

School. Although the majority of adolescent risk perception studies have involved school students, few have examined the influence of the school. One exception is a study by Smith and Rosenthal (1995). They found that the nature of the school system had a marked influence on risk perceptions. Students who attended private schools displayed a strong tendency to rate activities as more risky both to themselves and to others and to downplay the benefits of activities. They also rated their ability to control risks as lower when compared with students attending state schools. Smith and Rosenthal contend that these students view their risk environment in a more conservative and perhaps realistic way and they suggest that this may be because private schools devote more resources to health and life education or because these students may have better educated parents who provide more accurate information to their children concerning risky activities.

2.6.2 Emerging Adults

As shown in section 2.6.1 there is considerable interest in the risk taking and reckless behaviours of adolescents. In comparison, few researchers have examined these problem behaviours in what Arnett (2000a) refers to as "*emerging adulthood*" (18-25 year old). Arnett contends that the social, economic and demographic changes over the past 50 years have resulted in dramatic changes in what occurs between the late teens and early to mid-20s for most people in Western society. Most people finish their education, obtain employment, marry and have their children much later in life. Arnett suggests that it makes more sense to split the period from the beginning of puberty to the full attainment of adulthood into adolescence (roughly ages 10-17) and emerging adult (roughly ages 18-25). Numerous scholars in the US and Europe agree with this new stage of life course between adolescence and young adulthood (e.g. Chassin *et al.*, 2002, Piquero *et al.*, 2002, Shiner *et al.*, 2002, Cohen *et al.*, 2003, Bynner, 2005, Douglass, 2005). Research has shown that young people in this age period feel like neither adolescents nor fully adult but somewhere in between (Arnett, 1994). Emerging adulthood is characterised as a time of self-focused enjoyment where young people pursue the pleasures of living in a affluent consumerist society while having few responsibilities or restrictions (Arnett, 2004, Douglass, 2005).

As Bynner (2005) points out, not everyone has the resources to enjoy their late teens and early twenties in this way and the experiences of emerging adults who are poor or working class may be quite different from those who are middle or upper class. As this is an emerging area of research, scholars are only beginning to examine what precisely this period holds developmentally and issues such as this have not been fully addressed.

However, it is understood that problem behaviours are no less common and may be even more common in this age group (Arnett, 1991, Arnett, 2000a, Greene *et al.*, 2000). Bradley and Wildman (2002) examined if sensation seeking and peer pressure were predictors of problem behaviours in emerging adults. Bradley and Wildman (2002) found that risk behaviours were reliably predicted by sensation seeking but not by peer pressure, but the reverse pattern was true for reckless behaviours. They also found that being male, older and less highly educated were also strong predictors of engagement in reckless behaviour. Overall the findings show that gender roles and peer pressure are influential beyond the adolescent years. The study also showed the importance of distinguishing risk from reckless behaviour as these behaviours appear to have different predictor variables.

A similar study was carried out by Teese and Bradley (2008), but they only examined reckless behaviours. Their findings backed up those of Bradley and Wildman. Teese and Bradley (2008) suggest that recklessness during emerging adulthood may be more strongly related to peer factors than any other social variables such as parents or college and work environments and assert that this is due to the fact that emerging adults tend to move away (physically and/or emotionally) from their parents.

Appendix C presents a summary of a number of the empirical studies that have been cited in this section. Table C.1 shows the theory underlying each of the studies and the risk characteristics that have been examined in each study. Table C.2 shows the sampling details and the main findings of each study.

2.6.3 Discussion of Risk Perception Research into Adolescents and Emerging Adults

Risk taking and risk perceptions of adolescents and emerging adults have been examined from a number of different theoretical perspectives. Some studies have focused on the cognitive processes that underlie risk perception and interpretation, and have examined the cognitive abilities of adolescents and whether they differ from adults. Other researchers have analysed affect and emotion to see if these might predispose adolescents to greater risk engagement. Others have examined the social antecedents of risk-taking such as parental and peer influences. Many studies have combined elements from each of these groups. As noted by Boyer (2006), each perspective has produced interesting findings and he suggests that a more descriptive and accurate explanation for risk perception and risk taking in adolescence is to assume elements of each perspective. To date, there is no model or theory that suggests how each of these different perspectives can be combined, the influence of each of these characteristics or how these characteristics may interact. It is evident from Table C.1, Appendix C, that there is little commonality in the risk characteristics examined in these empirical studies.

Two difficulties had been suggested with applying the psychometric paradigm to adolescents: the first is that the risks that the original model studied were not of immediate relevance to adolescents, for example nuclear weapons and DNA technology and the second was that the psychometric paradigm did not include risk characteristics such as the role of peers and parents in shaping risk perceptions (Smith and Rosenthal, 1995). Benthin *et al*. (1993) addressed both these issues and tested the psychometric paradigm on

adolescents using more relevant risks. The authors also extended the nine risk characteristics commonly used in the psychometric paradigm to include characteristics of relevance to adolescents such as peer influence and parental control. Although their study was based on a small self selecting sample of 41 high school students, their findings were consistent with many other studies that have examined risk-taking in adolescents. A number of studies have subsequently used modified versions of the psychometric paradigm to assess risk perceptions in adolescence (Smith and Rosenthal, 1995, Hampson *et al.*, 2001, Curry and Youngblade, 2006). It is clear that the psychometric paradigm can be modified and used successfully with adolescents.

A criticism of empirical studies in this area is that most studies have examined a limited number of risks which have usually been determined by the researcher (Moore and Gullone, 1996, Millstein and Halpern-Felsher, 2002a). As research has shown that adolescent and adult opinion often differ in what is perceived as risky behaviour (Furby and Beyth-Marom, 1992), it is important that an adolescent view is sought when developing a list of risk behaviours. Some researchers contend, however, that adolescents may not be fully aware or knowledgeable about the risk environment (Slovic, 2000c, Byrnes, 2003) so caution has to be exercised when totally depending on an adolescent viewpoint. A preferable approach is to combine risks identified by a literature review, expert opinion and also gathering views from adolescents.

Some methodological weaknesses are evident with regard to the empirical studies of adolescent risk taking and risk perceptions. From Table C2, Appendix C it can be seen that some empirical studies have used samples of an inadequate size, samples with a gender imbalance or sampled within a single school or university. It is clear that many studies have not used random sampling or generated samples that are representative of the larger population and thus allow some generalisability.

2.7 Discussion & Summary

The field of risk perception research is marked by considerable theoretical and methodological differences. The two most influential areas of risk perception research have been the psychometric paradigm and Cultural Theory. The psychometric paradigm examines risk as a subjective concept and has been successful in eliciting the factors that determine risk perception. Many studies using the psychometric paradigm have examined the risk perception differences between the public and experts, and found that public risk perceptions are valid and should be included in informing risk assessments and communications. There have been many criticisms of the psychometric approach, the most important being that it does not take account of socio-cultural characteristics such as age, gender, ethnicity, emotion and trust and places too much emphasis on individual perceptions and interpretations of risk. Cultural Theory on the other hand presents a theory of risk perception that focuses on culture rather than individual psychology and the central theme of Cultural Theory is that risk is "*culturally constructed*". One difficulty with this theory is that there are only a limited number of applications of the theory and to date the theory has been difficult to test empirically.

Recent research has been directed at the interaction between the psychological and social cultural paradigms in an attempt to bridge the paradigmatic gap. This has led leading exponents of the psychometric approach to begin to take account of social, political and cultural factors such as gender, race, emotions, control, and trust in shaping risk perception. Other developments include the emergence of new tools to assess risk perceptions such as the Social Amplification of Risk Framework (SARF) which can be used to assess the effects of risk communications. Other risk perception theories have also been proposed that place more emphasis on socio-cultural aspects of risk perception and techniques such as Mental Models allow researchers gain a more in-depth knowledge of risk perceptions.

Apart from research into risk perceptions of E-commerce, and Internet shopping in particular, there has been little research into risk perceptions in the IS/ICT domain. The limited studies that have been carried out in this area do suggest, however, that risk perception theories such as the psychometric paradigm, Cultural Theory and SARF can all be applied successfully in the IS/ICT domain.

A substantial body of research has examined the risk perceptions and risk taking behaviours of adolescents. It has been shown that risk perception theories such as the psychometric paradigm can also be applied successfully to adolescents. Risk perception research on adolescents has also examined biological factors such as age, gender and ethnicity; psychological and behavioural factors such as invulnerability, unrealistic optimism, sensation seeking, the role of perceived risks and benefits and external factors such as parental and peer influence and the influence of schools. More recently some of this research has been extended into emerging adulthood (18-25 year old).

The risk perception field is now a multidisciplinary field of research including such disciplines as psychology, decision theory, economics, anthropology, geography and sociology. The complex nature of risk perception is captured in the definition proposed by the Royal Society in 1992, which defines risk perceptions as involving " *people's beliefs, messages, judgment and feelings, as well as the wider cultural and social dispositions they adopt towards hazards and their benefits*" (Pidgeon *et al.*, 1992, p. 89). It has been suggested that researchers should no longer tie themselves to a single risk perception paradigm and should apply a number of theories to gain a better and deeper understanding of the risk environment.

3 Literature Review Social Networking

3.1 Introduction

This chapter examines the research literature relating to social networking sites (SNSs). SNSs are a relatively new phenomenon and research in this area is at an embryonic stage. There is still a shortage of published research articles in the academic literature, but these are complemented by reports commissioned by government departments and other interested parties. The main aim of this chapter is to review the literature pertaining to the risks with SNSs. A substantial part of the literature examines the risks to children and university students from SNSs as it is felt that they are the predominant users of SNSs. The risks to adults haven't been addressed to the same extent. The positive benefits of SNSs are not discussed in any detail in this literature review; therefore a balanced judgement on the benefits versus risks of SNSs is not presented.

This chapter starts by defining SNSs and introducing their main functions. There are some aspects of the Internet that contribute to it being a risky environment and these are discussed in Section 3.3. Section 3.4 examines current research into SNSs with a particular emphasis placed on the strands of this research that are relevant to risk. Section 3.5 examines in detail some of the risks that users of SNSs can encounter. The chapter concludes by presenting the research questions.

3.2 Social Networking Sites: Definition & Functionality

The term social network site and social networking site (SNS) are terms which are both used in the literature. The term social network site was suggested by boyd (sic) and Ellison (2007); because they argued the term "*networking*" has the connotation of making contacts, often with strangers. Beer (2008) has argued that putting social networking sites under the umbrella of social network sites makes the definition too broad. Using boyd and Ellison's (2007) definition, the term social network site can encompass blogging and wiki sites. Beer (2008) has suggested that in place of creating the general category of social network sites, the term Web 2.0 should be used and categories such as wiki's, blogs,

mashups[4] and social networking sites can fit under this umbrella term. In agreement with Beer and because it is a term in common use, the term "*social networking site*" will be used in this thesis.

Most SNSs share a set of common functions:

1. Developing a profile;
2. Building a social network; and
3. Communicating on this social network.

Developing a Profile

To use a SNS a user needs to create a profile. Profiles typically contain basic information such as name, gender, location and contact details, but can also contain other information such as race, religion and sexual preference. Users are not required to enter in all these personal details, however many users do fill in their profiles in great detail and most users upload a photo profile. SNSs encourage users to fill in their details and regularly prompt users to complete their profile. A study by OFCOM asserted that users fill in their profiles in great detail because they enjoy doing so and also in order to help them to get in touch with others and project their identity (OFCOM, 2008). Studies show that populating profile fields on a SNS is positively related to the number of friends a user will have listed (Goodings *et al.*, 2007, Lampe *et al.*, 2007). Many users, particularly younger users, personalise the appearance of their profiles as a form of self-expression (Livingstone, 2008).

The visibility of a profile can vary by SNS and can be controlled by the user. Bebo and MySpace allow users to choose whether they want their profile to be public or only available to their friends. Facebook takes a slightly different approach, by default, users who are part of the same "*network*" can view each others profiles unless the user has explicitly denied permission to those in their network. For minors, Facebook limits the visibility of their profile to friends of friends and networks.

Building a Social Network

Once a user has set up a profile, they can begin creating their social network and invite others to be their friend and accept friendship invitations from others. The definition of

[4] A mashup is a web application that combines data from more than one source into a single integrated tool; one example is the use of cartographic data from Google Maps to add location information to real-estate data, thereby creating a new and distinct web service that was not originally provided by either source.

friends on SNSs is different from that in the offline world (boyd, 2004). On a SNS a friend is anyone who either accepts an invitation or has their invitation accepted to be friends. These can be offline friends, family, people a user has lost touch with, friends of friends or complete strangers. Friend connections in a SNS are publicly displayed online and users can be judged by these lists of online friends far more so than is the case in the offline world (Donath and boyd, 2004). Many users, especially children collect friends and having the highest number of online friends is seen as highly desirable (OFCOM, 2008).

Most SNSs have a similar model of how social networks are built. According to Donath and boyd (2004), friendship links in SNSs can be mutual, public, unnuanced and decontextualised:

- links are *mutual* if A has B as a connection, then B has also agreed to show A as a connection;
- the links are *public*: they are permanently on display for others to see;
- the links are *unnuanced*: there is no distinction made between a close friend and a near stranger;
- the links are *decontextualised*: there is no way of showing only a portion of one's network to some people.

Some SNSs, for e.g. Orkut allow users to distinguish groups of friends but as stated by Donath (2008) people do not like to explicitly define the parameters of their friendships, as they often do not want to embarrass another person. Asking people to do this can lead to increased social discomfort. It is also possible to restrict areas of your network to certain friends, though SNSs have typically made this hard to do.

Communicating with Others

The primary reason that most people use SNSs is to communicate with known contacts and friends (Acquisti and Gross, 2006, boyd, 2007, Ellison *et al.*, 2007, Lenhart and Madden, 2007, Anchor, 2008a, OFCOM, 2008, Young and Quan-Haase, 2009, Livingstone *et al.*, 2010b, O'Neill *et al.*, 2011). Communications can be private among users or can be in a public forum such as writing on someone's "*public wall*" or comment board, which can be seen by anyone who has access to the user's profile. Some users, although not the majority, use SNSs to communicate with strangers. Adults in this category tend to use

SNSs for dating purposes as SNSs offer greater opportunities and a cheaper alternative to online dating.

The functionality inherent in SNSs has been available on the Internet for some time, such as creating personal web pages and communicating with others in chat rooms etc., but as illustrated by Rau *et al.* (2008) SNSs differ from other online communities in three major aspects:

1. SNSs have been designed specifically to help users to establish an online presence and build social networks, whereas the majority of traditional online forums or communities have been built around understanding or discussing a particular topic (Preece *et al.*, 2004);
2. Users in SNSs are connected in networks rather than hierarchical groups as in traditional online communities. This reflects more accurately how offline communities are developed (Scott, 2000). Mayfield (2005) provides a framework, shown in Table 3.1, to illustrate the differences between an online community and a SNS;

SNS	Online communities
Bottom-up	Top-down
People-centric	Place-centric
User-controlled	Moderated
Context-driven	Topic-driven
Decentralized	Centralized
Self-organizing	Architected

Table 3.1 Comparison of Online Communities and SNS (Source: (Mayfield, 2005)**)**

3. SNS users are connected in a person-to-person manner and the relationships between members are more explicit and visible than in other online communities. In SNSs connections come before content, whereas in online communities content comes before connections (Mayfield, 2005).

As stated by Ellison *et al.* (2009, p6) it is the "*articulated social network*" that really differentiates SNSs from earlier technologies. Social networks allow users to create a digital representation of their connections with other users.

3.3 Impact of the Internet

There is a considerable amount of research literature that examines the social and psychological impacts of the Internet. This is a vast literature and a comprehensive synthesis of this literature is beyond the scope of this thesis, however many aspects of this literature contribute to the discussion of the risks for SNS users and are discussed below.

3.3.1 Internet Use and Well-Being

A number of researchers has examined the effect of Internet use and online communications on well-being. Two opposing explanatory hypotheses have been proposed. The *displacement hypothesis* which suggests that online communication reduces well-being because it displaces time spent with existing friends. Proponents of this hypothesis contend that the Internet motivates users to form online contact with strangers rather than maintaining friendships with their peers. In contrast, the *stimulation hypothesis* argues that online technologies encourage communication with existing friends. A number of studies has examined this with some finding support for the displacement hypothesis (Kraut *et al.*, 1998, Nie, 2001, Nie and Hillygus, 2002) some finding support for the stimulation hypothesis (Wellman *et al.*, 2001, Kraut *et al.*, 2002, Shaw and Gant, 2002, Kavanaugh *et al.*, 2005, Ellison *et al.*, 2007, Valkenburg and Peter, 2007a, Valkenburg and Peter, 2007b, Bessière *et al.*, 2008) and others finding no significant results (Sanders *et al.*, 2000, Wästlund *et al.*, 2001, Gross, 2004, Jackson *et al.*, 2004b). Valkenburg and Peter (2007b, 2009) suggest that many of the studies that found a displacement effect were conducted in the early stages of the Internet and as stated by Kraut *et al.* (2002, p68) the difference was the Internet itself as "*Simply put, the Internet may have become a more hospitable place over time*". The difference could be attributed to the fact that more friends and family were likely to be online and new services such as instant messaging had been developed that encourage communication with existing ties (Kraut *et al.*, 2002, Valkenburg and Peter, 2009).

Shklovski *et al.* (2006) carried out a meta-analysis of 16 studies that examined how the Internet can effect social interaction and concluded that the Internet has no effect on social interactions with family members. With regard to friends they found contradictory evidence. Studies using cross sectional designs suggest that increased Internet use is sometimes associated with less interaction with friends, whereas longitudinal studies show

a slight increase in interactions with friends. Shklovski *et al.* (2006)s suggest that the results from longitudinal studies are more credible as the ability to study the same people over time mitigates several major threats to casual inference.

Researchers have examined the existence of the stimulation and displacement hypotheses with regard to SNSs, with strong support for the stimulation hypothesis, as the majority of SNS users report using these sites to stay in touch with existing friends (Acquisti and Gross, 2006, boyd, 2007, Ellison *et al.*, 2007, Lenhart and Madden, 2007, Anchor, 2008a, OFCOM, 2008, Young and Quan-Haase, 2009, Livingstone *et al.*, 2010b, O'Neill *et al.*, 2011).

Two further opposing hypotheses have been proposed based on the antecedents of online communication. The first is the "*social compensation*" or "*poor can get richer*" hypothesis which asserts that the effects of the Internet on well-being are positive but only for introverts or socially anxious individuals. Individuals who perceive their offline social networks to be inadequate compensate for them with more extensive online social networks (McKenna and Bargh, 2000, Valkenburg *et al.*, 2005). The competing hypothesis, the "*rich get richer*" hypothesis asserts that Internet use primarily benefits extroverted users who use the Internet to expand their existing network of friends and contacts (Kraut *et al.*, 2002, Valkenburg *et al.*, 2005). Both the stimulation and displacement hypotheses do not address the antecedents of online communication. Of the studies that have focussed on the relationship between loneliness or social anxiety and Internet use most tend to support the rich get richer hypothesis (Moody, 2001, Wästlund *et al.*, 2001, Weiser, 2001, Peter *et al.*, 2006) but some studies have found evidence for the social compensation hypothesis (Amichai-Hamburger *et al.*, 2002, Amichai-Hamburger and Ben-Artzi, 2003, Wolak *et al.*, 2003).

These hypotheses have been examined with regard to SNS communications, with no conclusive results. Some studies have found evidence of the social compensation hypothesis (Ellison *et al.*, 2007, Stamoulis and Farley, 2010), some for the rich get richer hypotheses (Sheldon, 2008, Ross *et al.*, 2009, Correa *et al.*, 2010), some found support for both hypotheses (Zywica and Danowski, 2008, Desjarlais and Willoughby, 2010) and some found no support for either hypothesis (Tufekci, 2010).

A number of studies (Guadagno et al., 2008, Ross et al., 2009, Amichai-Hamburger and Vinitzky, 2010) have examined the Five Factor Model (FFM) of personality traits (Costa and McCrae, 1992) in order to examine if these personality traits are associated with different types of Internet usage. The FFM of personality traits contends that personality can be characterised by five traits: neuroticism; extraversion, openness to experience, agreeableness and conscientiousness. Some studies have investigated how the FFM personality traits are related to specific Facebook use (Ross et al., 2009, Amichai-Hamburger and Vinitzky, 2010) and have found relatively few significant findings in relation to the personality variables. Ross et al. (2009) suggest that the FFM of personality traits may be too broad and not the best way to understand specific Internet behaviours. Amichai-Hamburger and Vinitzky (2010) suggest that other factors besides that of personality, for example social norm, may be more important factors for Facebook use. Studies have also examined the influence of cognitive style on Internet use. Cognitive style research is based on Jung's (1923) premise that people have different ways of perceiving and judging the world and is commonly measured using the Myers-Briggs type indicator (Myers *et al.*, 1998). McElroy *et al*. (2007), for example tested the effect of the FFM and cognitive style on Internet use and found support for personality style but not for cognitive style.

Researchers have also examined the effect of Internet use on self-esteem. Again there is disagreement in the literature with some studies reporting negative effects on self esteem (Kraut *et al.*, 1998, Rohall *et al.*, 2002), others showing a positive relationship (Kraut *et al.*, 2002) and others finding no significant relationship (Gross *et al.*, 2002, Harman *et al.*, 2005). Some studies have found that users with lower self esteem engage more with SNSs (Steinfield *et al.*, 2008) whereas other studies indicate users with higher self-esteem are more likely to be frequent users of SNSs (Lenhart and Madden, 2007). Some studies found no self-esteem effect on SNS usage levels (Baker and White, 2010).

Overall there is little consensus with regard to the effect of Internet use on well-being. This could reflect the possibility that these models oversimplify online communications and do not fully address why, with whom and about what users communicate online (Valkenburg and Peter, 2007b, 2009), but it is more likely as suggested by Tufekci (2010) that these models unrealistically assume that all people will be similarly affected by Internet use.

3.3.2 Computer Mediated Communication

Early research in this area compared groups that communicated by means of computer (CMC) with face-to-face (FtF) communications and generally emphasised the disadvantages of CMC. For example, empirical research carried out by Siegal *et al.* (1986) found higher percentages of remarks containing swearing, insults, name calling and hostile comments in online communications than in FtF communications. Research by Kiesler and Sproull (1992) found that groups using CMC had greater difficulty attaining a shared point of view. Explanations for these negative effects were attributed to the anonymity of the Internet and the reduced social cues available on the Internet.

The Internet allows individuals to be anonymous. People usually think of anonymity as meaning they are not *identifiable* (Joinson, 2001). On the Internet, there are differing levels of anonymity. It is possible to have visual anonymity as the user cannot be seen, but that does not mean that the user is unidentifiable. In some situations it is possible for users to have an anonymous e-mail name while in others a user may use their real name though they can still be relatively anonymous when interacting with people they do not already know. Thus on the Internet, anonymity is not an either-or phenomenon and there are always degrees of anonymity which can vary from situation to situation (Thurlow *et al.*, 2004). The feeling of being anonymous on the Internet can lead users to a feeling of deindividuation. Deindividuation describes how an individual's sense of self can be subsumed by the power of the group (Thurlow *et al.*, 2004). This can lead to a weakened ability for the individual to regulate their behaviour and the individual is less likely to care what others think of them. These effects can result in impulsive and disinhibited behaviour (Zimbardo, 1969) or what Suler (2004) calls the "*the online disinhibition effect*". This disinhibition effect can be positive or negative. Sometimes individuals share personal information (e.g. feelings, secrets etc.) about themselves or they can show unusual acts of kindness and go out of their way to help others. On the negative side, individuals can be rude, angry, hateful and threatening. Suler (2004) does acknowledge that the online disinhibition effect is not the only factor that determines how much people self disclose or act out on the Internet. Other personality variables such as the intensity of a person's underlying feelings and their personality styles all have an impact.

Early research also argued that online communication was more difficult because many offline social cues were missing. One such theory, the Reduced Social Cues model (RSC),

was proposed by Keisler and Sproull (1986). Their argument was that the reduction of social cues made interactions between people more difficult to manage and that communication ended up more task-focussed, more self-absorbed and uninhibited. They argued that Internet communication undermined social norms and influences and there was less pressure on people to play by the rules and to behave appropriately. Thurlow *et al.* (2004) argue that RSC does not account for the fact that other forms of communication with reduced cues, such as letter writing, do not evoke aggressive or inappropriate behaviour. Subsequent researchers have disagreed with the RSC model and have developed more optimistic models. One such example is the *social information processing theory* posited by Walther (1992). Walther contends that users are able to gain impressions from online communications, but doing so requires more time and more exchanges of messages.

More recent research has challenged the opinion that CMC is characterized by impersonality and hostility and studies have found increasing evidence that personal relationships can be formed successfully online (Parks and Floyd, 1996, McKenna and Bargh, 1998). An increasing body of evidence (Joinson, 2001, Tidwell and Walther, 2002) suggests that Internet activity can be characterised by high levels of self-disclosure, higher than that of FtF communication. As stated by Valkenburg and Peter (2009) the finding that CMC enhances self-disclosure is one of the most consistent outcomes in CMC research. Although the research has pointed towards the positive aspects of CMC, there are still some negative aspects to online communications. The anonymity provided by the Internet can also be used a cover for racial hate groups and harassment and can even to lead in extreme cases to physical harm and death as has been evidenced by the murder of Matthew Pyke supposedly after an argument on a web forum (BBC, 2008).

Internet based support groups have been found to have positive effects in many diverse areas including support groups for the elderly (Wright, 2000) and adolescents (Gould *et al.*, 2002) and for those with medical problems and those with serious and stigmatized illnesses (e.g., AIDS, alcoholism, breast and prostate cancer) (Davison *et al.*, 2000, Cummings *et al.*, 2002, McKay *et al.*, 2002, Winzelberg *et al.*, 2003).

3.3.3 Internet Privacy

With ICT and the Internet, personal information can be "*accessed, stored, manipulated, data mined, shared, bought and sold, analysed and potentially lost, stolen or misused by countless government, corporate, public and private agencies, often without our knowledge or consent*" (Buchanan *et al.*, 2007, p157). Regularly reports of the theft, loss and misuse of personal information held on computer are hitting the headlines and accordingly privacy research in this area is increasing.

A difficulty for researchers has been to find a universal definition of privacy. This is because of the many different contexts in which privacy is found. For example, in a legal context, privacy has been defined as "*the right to be let alone*" (e.g. Warren and Brandeis, 1890, p205). In philosophy and psychology, privacy is defined by a state of limited access or isolation (e.g. Schoeman, 1984). In social science and information systems, privacy has been defined with respect to control of personal information and to what extent information about them is disclosed to others (e.g. Westin, 1967, Culnan and Armstrong, 1999). In order to overcome these definitional difficulties, some researchers such as Burgoon et al. (1989) and DeCew (1997) have proposed definitions that reflect the multidimensional nature of privacy. DeCew for example (1997) distinguishes three dimensions of privacy:

1. Informational privacy covers personal information such as finances, medical details etc. that an individual can decide who has access to and for what purposes.
2. Accessibility privacy refers to physical or sensory access to an individual. It allows individuals to control decisions about who has physical access to them.
3. Expressive privacy concerns an individual's ability to freely choose how to act, self-express and socially interact.

With regard to the Internet the dimensions of informational and expressive privacy are the most relevant. Another consideration on the Internet is the privacy of communications. Numerous researchers in information systems have examined privacy issues and in particular understanding what motivates Internet users to disclose or not disclose personal information (e.g. Culnan and Armstrong, 1999, Cranor *et al.*, 2000, Phelps *et al.*, 2000, Sheehan and Hoy, 2000, Miyazaki and Fernandez, 2001). Findings from a number of studies suggest that Internet users express a high level of concern about their online

privacy (Cranor *et al.*, 2000, Phelps *et al.*, 2000, Han and Maclaurin, 2002, Earp and Baumer, 2003), but it is not entirely clear whether these high levels of privacy concern actually translate into behaviour. There is some evidence to suggest that individuals that are concerned with privacy are willing to trade their privacy for convenience (Spiekermann *et al.*, 2001, Chellappa and Sin, 2005). A number of popular press articles have highlighted experiments that show people are often willing to reveal their passwords in exchange for a small token such as a bar of chocolate (Worthen, 2008, BBC, 2004). A paradox seems to exist between user's intentions and their actual behaviour and this area has been examined by a number of researchers (Syverson, 2003, Acquisti, 2004, Acquisti and Grossklags, 2005, Norberg *et al.*, 2007). However, these studies were carried out on small non-representative samples. Although caution has to be exercised in generalising findings from these results, it does appear that the level of actual disclosure significantly exceeded individuals' intentions to disclose. This finding has important implications for users of SNSs as so much personal information is revealed on these sites. Research related to the privacy aspects of SNSs are discussed in Section 3.4.2.

3.3.4 Addiction

The terms "*Internet Addiction*" (Young, 1998, Pratarelli *et al.*, 1999), "*Internet Dependency*" (Scherer, 1997), "*Pathological Internet Use*" (PIU) (Morahan-Martin and Schumacher, 2000), "*Problematic Internet Use*" (Shapira *et al.*, 2000), "*Excessive Internet Use*" (Griffiths, 2000b) and "*Compulsive Internet Use*" (Greenfield, 1999) have all been used to describe the same concept, i.e. that an individual could be so involved in their online use that they neglect other areas of their life (Widyanto and Griffiths, 2006). Among these terms Internet addiction is the most popular. Niemz, Griffiths *et al.* (2005) describe the symptoms of Internet addiction as an increased preoccupation with online activities, tolerance (e.g. spending increased amounts of time online) and symptoms of withdrawal such as anxiety and depression when not online. Griffiths (1998) also includes the symptoms of salience (where the Internet becomes the most important thing in a person's life), mood modification (where the Internet is used to change mood states) and relapse (where a person returns to the addictive behaviour, even after a period of abstinence).

Widyanto and Griffiths (2006) carried out a meta-analysis of research into Internet addiction and suggested that academic research in this area can be roughly divided into five categories:

1. Survey studies that compare excessive and non-excessive Internet users e.g. (Young, 1996a, Brenner, 1997, Greenfield, 1999, Cao and Su, 2007, Yang and Tung, 2007);
2. Survey studies that examine vulnerable groups of excessive Internet use, most notably students e.g. (Scherer, 1997, Chou and Hsiao, 2000, Morahan-Martin and Schumacher, 2000, Anderson, 2001, Niemz *et al.*, 2005, Ceyhan, 2008);
3. Studies that examine the psychometric properties of excessive Internet use e.g. (Pratarelli *et al.*, 1999, Charlton, 2002);
4. Case studies of excessive Internet use and treatment case studies e.g. (Young, 1996b, Griffiths, 2000a); and
5. Studies that have examined the relationship of excessive Internet use with other behaviours, e.g. self-esteem and depression e.g. (Young and Rogers, 1998, Shapira *et al.*, 2000, Yang and Tung, 2007).

A number of different scales have been developed to measure Internet addiction. The most commonly used scales are shown in Table 3.2. Some of these scales are based on recognised DSM-IV[5] criteria for other addictions, such as substance abuse and pathological gambling (Young, 1996a, Brenner, 1997). Griffiths (2000c) has criticised these scales as they have no measure of severity, have no temporal dimension and they do not consider the context of Internet use (i.e. it is possible for some people to be engaged in excessive use because it is part of their job or they are in an online relationship).

[5] The Diagnostic and Statistical Manual of Mental Disorders (DSM) is an American handbook for mental health professionals that lists different categories of mental disorders and the criteria for diagnosing them, it is published by the American Psychiatric Association. It is used worldwide by clinicians and researchers as well as insurance companies, pharmaceutical companies and policy makers.

Paper	Measure Used	Items	Scale
YOUNG, K. S. (1996)	Internet Addiction Test (IAT)	8	Yes/No
SCHERER, K. (1997)	Clinical symptoms of Internet dependency	10	Yes/No
BRENNER, V. (1997)	Internet-Related Addictive Behaviour Inventory (IRABI)	32	Yes/No
MORAHAN-MARTIN, J. & SCHUMACHER, P. (2000)	Pathological use scale (PIU)	13	Yes/No
CHOU, C. & HSIAO, M.-C. (2000)	Chinese-IRABI version II" (C-IRABI-II)	40	4 point likert
GRIFFITHS, M. (2000)	Addiction components criteria	6	

Table 3.2 Scales Used to Measure Internet Addiction

The level of Internet addiction predicted by studies varies quite considerably with estimates of Internet addiction ranging between 6 – 18%. Quite a number of studies have examined the existence of Internet addiction amongst students as these are a population that are considered to be particularly vulnerable. It is argued that this variability may be due to the different measurement scales used, but can also be attributed to differences in culture, age, sampling and methodology used. Although the increase in the numbers of Internet addiction centres in China, South Korea, Taiwan and the U.S. would indicate otherwise, there is a debate surrounding whether excessive use of the Internet can be defined as an addiction in clinical terms (Mitchell, 2000, Shaffer *et al.*, 2000, LaRose *et al.*, 2001, Charlton, 2002, Bessière *et al.*, 2008, Roman, 2009). Neither the DSM nor the World Health Organisation's International Classification of Diseases recognises Internet addiction as a disorder. Griffiths (1998) holds a firm belief that Internet addiction does exist, but that it affects only a small minority of users. Griffiths (2000c, a) contends that most of the individuals who use the Internet excessively are not addicted to the Internet itself, but use it as a medium to fuel other addictions. LaRose *et al.* (2010) suggests that Internet addiction would be better described as a habit forming Internet activity rather than a problematic one. A Harvard Professor, John Ratey, has suggested that people who are influenced by technology, have developed shorter attention spans. He suggests that people physically crave the bursts of stimulation from checking e-mail or voice mail or answering the phone. Professor Ratey compares these cravings to those of narcotics and states that "*it is like a dopamine squirt to be connected*"(Richtel, 2003).

Studies have found, not unsurprisingly, that addicted Internet users spend significantly more time online. Empirical studies have found that addicted Internet users tend to use more interactive functions (such as chat rooms or online games) than non-addicted users (Young, 1996a, Chou and Hsiao, 2000). Studies suggest that addicted users are more

likely to be males (Morahan-Martin and Schumacher, 2000, Anderson, 2001, Cao and Su, 2007, Ceyhan, 2008). Griffiths (2000c) argues that this could be because males are more likely to use the Internet to fuel other addictions such as gambling and computer games. Some studies have indicated that using the Internet for social interactions is correlated with Internet addiction (Yang and Tung, 2007, Ceyhan, 2008). This latter finding suggests that SNSs may pose a particularly risky environment for Internet addiction. Research into this area is discussed in Section 3.5.1.

Studies have found that Internet addiction, similar to other addictions, can interfere with other aspects of life (Young, 1996a, Brenner, 1997, Scherer, 1997, Chou and Hsiao, 2000, Anderson, 2001, Niemz *et al.*, 2005, Yang and Tung, 2007). Addicted Internet users can be more socially disinhibited online (Morahan-Martin and Schumacher, 2000, Niemz *et al.*, 2005) and tend to have a lower self esteem (Armstrong *et al.*, 2000, Niemz *et al.*, 2005, Yang and Tung, 2007). This relates back to the literature on the Internet and well-being as previously discussed in Section 3.3.1. Internet addiction often co-occurs with other psychiatric disorders (Young and Rogers, 1998, Shapira *et al.*, 2000, Cao and Su, 2007, Ceyhan, 2008). Armstrong, Phillips *et al.* (2000) argue that the nature of the relationship between self-esteem and addiction is not clear and there is a continuing debate as to whether low self-esteem is a cause or a consequence of addiction. Mitchell (2000) goes so far as to state that he does not believe Internet addiction deserves a separate diagnosis as it is unclear whether it develops of its own accord or if it is triggered by an underlying psychiatric illness. Chou et al. (2005) do warn however that it is difficult to conclude that heavy use of the Internet has an overall negative impact on addict's lives. There may be some negative impacts such as time-wasting, which can lead to interference with academic work and professional duties but the positive benefits of Internet use may outweigh these negative aspects.

3.4 Current Research into Social Network Sites

SNSs have gained much popularity in a relatively short period of time. Research in this area is at an embryonic stage; however certain strands of research are emerging. This section examines five areas of research into SNSs under the headings of:

1. Online and Offline Social Networks;
2. Personal Information Revealed on Social Networking Sites;
3. Trust on Social Networking Sites;
4. Impression Management on Social Networking Sites; and
5. Network Structure.

Other areas of research into SNSs include research into race and culture (Gajjala, 2007, Byrne, 2008), religion (Nyland and Near, 2007) and gender and sexuality (Geidner *et al.*, 2007, Cohen and Shade, 2008, Driscoll, 2008, Hussain and Griffiths, 2008, Jackson *et al.*, 2008) effects on SNSs. There is also a body of research that has examined risks and risky behaviour on SNSs, this research is presented in further sections.

3.4.1 Online and Offline Social Networks

A number of researchers has examined the relationship between online and offline social networks. Most users use SNSs to support pre-existing offline relationships rather than meeting new people (boyd, 2007, Ellison *et al.*, 2007, Lenhart and Madden, 2007, Lampe *et al.*, 2008, OFCOM, 2008, Subrahmanyam *et al.*, 2008, Barker, 2009, Kujath, 2011). boyd (2007) highlights four properties that separate online and offline social networks:

1. *Persistence*: online communications are recorded for posterity. This allows asynchronous communication, but also extends the period of existence of any communication;
2. *Searchability*: search and discovery tools allow users to find others online;
3. *Replicability*: online communications can be copied from one place to another verbatim with no way to distinguish the "*original*" from the "*copy*" (Negroponte, 1996); and

4. *Invisible audiences*: It is virtually impossible to ascertain the audience for an online communication, it could potentially consist of all people across all space and time, though this is unlikely to happen.

Some researchers have utilised social network theory to compare online and offline social networks. Social network theory views social relationships in terms of nodes and ties. Nodes are the individual actors within the network and ties are the relationships between the actors. The history and application of these theories are discussed in further detail in Scott (2000). Social network theorists have examined the depth and strength of ties in social networks and the importance of "*weak-ties*" in the flow of information across a social network (Granovetter, 1973, 1983). Network theory has also been used to explore how distant nodes can be interconnected through relatively few random ties, for example the "*small world problem*" presented by Milgram (1967). Hill and Dunbar (2003) estimated that in contemporary western society an average social network comprised about 150 individuals. This is sometimes known as "*Dunbar's number*". Wellman and Potter (1999) observed that a typical personal social network will have 3-6 close and intimate ties, 5-15 less close but still significant and active ties and could have about 1000 more distant acquaintances. Once an offline or physical social network is established, the number of members tends to change little over time. In contrast, one of the aims of SNSs is to increase the size of your social network and the goal for many users is to grow their online social network to be as large as possible. An online SNS user can often list hundreds of direct friends and include thousands of additional friends within three degrees of separation from the user (Gross and Acquisti, 2005). Donath and boyd (2004) argue that strong ties (i.e. close ties) are not greatly increased by SNSs, but the number of weak ties or distant acquaintances can be increased substantially. These weak ties can carry many benefits. Weak ties can present diverse perspectives and new information (Ellison *et al.*, 2009). Research has shown that people are more likely to receive information about employment opportunities from weak ties, Granovetter (1973) refers to this as "*the strength of weak ties*". Research by Ellison *et al.* (2007) found that Facebook was associated with higher levels of social capital and in particular bridging social capital.

Some researchers have warned that making a simple distinction between offline and online communications does not capture the complex nature of communications as online communications are increasingly embedded in everyday life and can no longer be

examined as a separate entity (Wellman, 2001, Wellman *et al.*, 2001, Bakardjieva, 2005, Beer, 2008, Livingstone, 2008).

In an online environment the communities that children are involved in are primarily made up of peers. This means that the role of peers is particularly important in the online environment (Withers and Sheldon, 2008). This has important implications for the peer effects of SNSs, where large networks of peers with similar interests can be easily organised. Withers and Sheldon (2008) suggest that peers online can influence each other more negatively and in a potentially more powerful way than in the offline world. They present the example of pro-anorexia groups on Facebook. Several of these groups have in excess of 200 members. However, Withers and Sheldon (2008) provide no empirical evidence to back up this assertion. Researchers have begun to examine the role of peers in determining SNS use (Pelling and White, 2009, Baker and White, 2010) and have found that those that perceive frequent SNS use to be normative among their friends have stronger intentions to engage in frequent SNS use themselves and that larger numbers of friends has a positive effect on continued intention to use a SNS (Lin and Lu, 2011).

3.4.2 Privacy and Personal Information Revealed on Social Networking Sites

The information revelation and privacy implications of SNSs have attracted much interest from both the media and the academic research community. The quantity of personal information revealed by SNS users in their profiles and by communicating on their public space can reveal aspects of their social and inner life. This information is valuable as a business commodity but also to fraudsters and can open users to risks such as stalking, identity theft, building a digital dossier, advertising, spam, phishing etc.

This section examines the current research thinking in the areas of:

1. Privacy settings on SNSs
2. The level of personal information revealed on SNSs;
3. The audience for this information; and
4. Attitudes to privacy on SNSs

Privacy Settings on SNSs

Users can protect their privacy on SNSs by setting more restrictive privacy controls and by controlling the amount of information they reveal and who they reveal this information to. However, SNSs are in the business of encouraging users to share as much personal information as possible and thus do not promote the privacy controls (Bonneau and Preibusch, 2010, Schneier, 2010, Furnell and Botha, 2011). Privacy policies on SNSs are often written using complex legal terms and are not easily understood by ordinary users (Bonneau and Preibusch, 2010). Privacy controls on SNSs are not always intuitive to use and studies have found that many users are not able to properly utilise the privacy settings, particularly younger and older users and those with less computer experience (Bonneau and Preibusch, 2010, Brandtzæg *et al.*, 2010). The privacy options offered on SNSs are limited to the options SNS companies provide and how easy they are to find (Schneier, 2010). As shown in the recent EU Kids Online study (Livingstone *et al.*, 2011b), younger children are more likely than older children/adolescents to have their profile set as "*public*". Findings also indicate that these users are more likely to post personal information. Many users accept the default settings on SNSs, but these settings are not set to be restrictive. On Facebook for example, for minors, the visibility of personal information is limited to "*friends of friends*" and "*networks*", but for adults the default privacy settings for certain types of information is set to "*everyone*". Matt McKeon (2010) presents an interesting graphic showing how Facebook's default privacy settings have changed between 2005 and April 2010, see Figure 3.1. In 2005, Facebook restricted the visibility of a user's personal information to just their friends and their "*network*" (college or school). Over the past couple of years, the default privacy settings for a Facebook user's personal information have become more permissive.

Furnell and Botha (2011) warn that at the time of writing (May 2011) that there was no access to any of the privacy and access control settings on the mobile versions of Facebook. This is of concern as users are increasingly using these devices to access Facebook and some users only access Facebook through a Smartphone application.

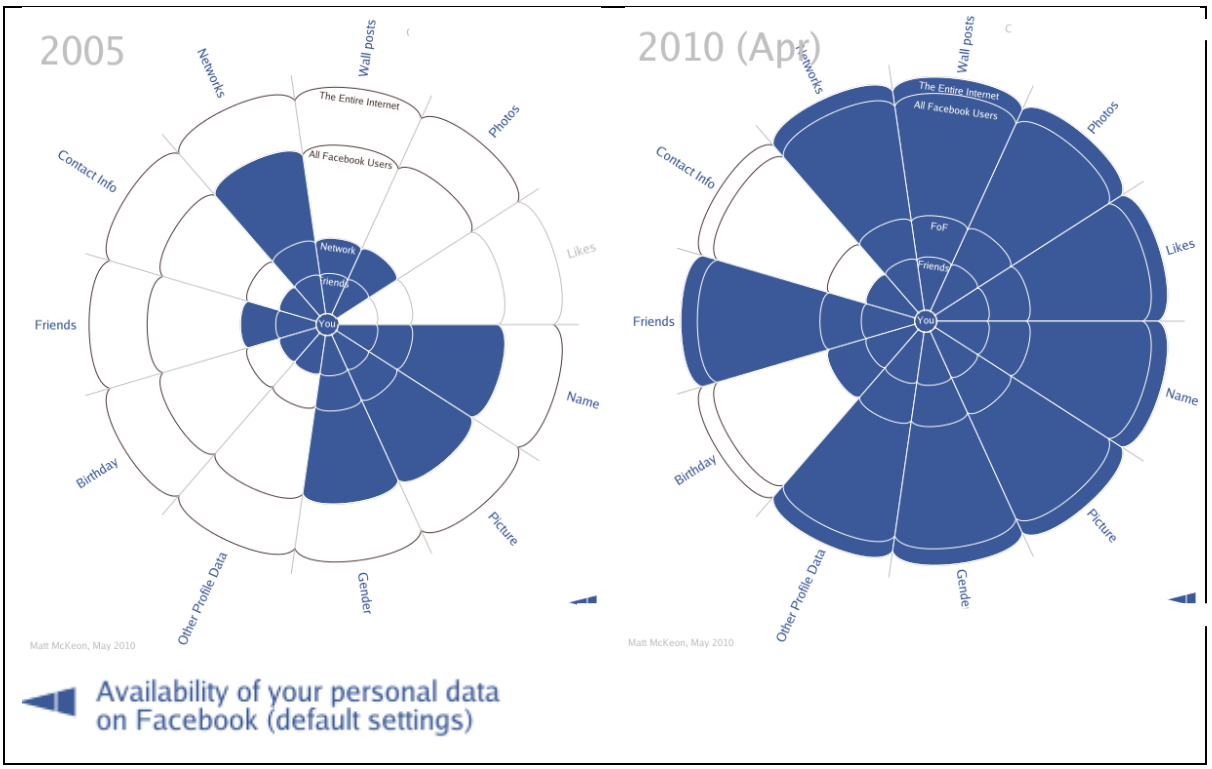


Figure 3.1 Facebook Default Settings 2005 and 2010. Source: (McKeon, 2010)

Personal Information Revealed on SNSs

Numerous studies (Gross and Acquisti, 2005, Jones and Soltren, 2005, Acquisti and Gross, 2006, Stutzman, 2006, Anchor, 2008b, Hinduja and Patchin, 2008b, Kolek and Saunders, 2008, Tufekci, 2008, Christofides *et al.*, 2009, Fogel and Nehmad, 2009, WEBWISE, 2009, Young and Quan-Haase, 2009, Nosko *et al.*, 2010) have found that SNS users are revealing substantial amounts of personal information. As an example Gross and Acquisti (2005) downloaded and examined the online Facebook profiles of over 4,000 Carnegie Mellon University students. They found that these students provided an astonishing amount of information for example, 89% of users provided their full name, 91% of profiles contained an image, 88% of users provided their date of birth and 40% provided a phone number. Studies of adolescents and children indicate that these age cohorts are more careful about revealing direct contact information on SNSs (Hinduja and Patchin, 2008b, Livingstone *et al.*, 2010b, O'Neill *et al.*, 2011). This perhaps indicates the success of Internet safety awareness campaigns.

Some studies have found that males are more likely than females to provide contact information (Gross and Acquisti, 2005, Tufekci, 2008, Fogel and Nehmad, 2009). Gross and Acquisti (2005) attributed this to single males "*signalling*" their interest in making the maximum amount of contact information easily available. A study by Nosko *et al.* (2010) found that age and relationship status were important factors in determining information

disclosure on SNSs. They found that as age increased, the amount of personal information revealed decreased. Nosko *et al.* suggest that older adults may be less likely to reveal personal information due to less familiarity and trust with the technology or due to more experience and concern about revealing personal information. Nosko *et al.* found that those seeking a relationship were the most at risk as they revealed a higher amount of sensitive information. A recent European study (EUROBAROMETER, 2011) found that younger users (aged 15-24), what they termed "*digitial natives*", those born and raised with digital technology, show less concern about disclosing personal information online. They are also the most likely to disclose various types of personal information on social networking sites and do not usually read privacy statements on the Internet.

The choice of SNS can be an important differentiator in the amount of information users reveal, as Facebook is aimed at particular social networks, e.g. all students in a particular university, all members in a company, users may feel they are revealing information in a more bounded network. The structure of the SNS can also be important, for example Facebook encourages users to identify themselves using their real names.

In some cases users may be careful not to expose their identities. Researchers have found that even when users are careful in hiding personal identifying information they can still provide enough information to identify themselves. This can happen, for example, through face re-identification technologies, such as the Facebook app, Photo Finder[6] or through harvesting information from a number of social network profiles (Hogg and Adamic, 2004, Liu and Maes, 2005). Users also underestimate the magnitude of what they disclose when it is aggregated over time (Conti and Sobiesk, 2007).

Audience

As stated in Section 3.4.1 the audience for information on SNSs can be vast. The hosting site obviously has access to this information and can use it for other purposes. For example the privacy policy for Facebook (accessed June 2011) states that Facebook collects personal information that the user discloses and information as the user interacts with the web site. They also collect browser type and IP address and use session ID cookies to store login information. Their policy also advises that Facebook may collect information about users from other sources including the applications hosted by third parties on Facebook and other users of the Facebook service. They assert that this is in

[6] http://face.com/about.php

order to provide users with more useful information and a more personalised experience. Debatin *et al.* (2009) compare Facebook's data gathering to a iceberg and suggest that 1/8th of the iceberg is visible to users and is maintained to be interesting and fun for the user, the remaining 7/8^{ths} of the data collection, although containing information provided by users, is invisible to users.

The information users provide on SNSs is also of interest to third parties (from hackers to government agencies) (Gross and Acquisti, 2005). Technically, it is easier to access data in SNSs than in conventional e-commerce systems (Preibusch *et al.*, 2007). The privacy policy for Facebook (accessed June 2011) clearly states that they cannot and do not guarantee that content users post on the site will not be viewed by unauthorized persons and they are not responsible for circumvention of any privacy settings or security measures contained on the site. Furthermore, they warn that even after removal, copies of user's content may remain viewable in cached and archived pages. This implies that information provided even on private social networks can become publicly available and can also exist for as long as someone has an incentive to maintain it or even fails to remove it. Another concern, is that the privacy policies of SNSs tend to be centered around the individual and do not take into account that rich sources of data can be revealed by the network and social graph or "*friends*" aspects of SNSs (Preibusch *et al.*, 2007). Although, users can control what appears on their profile, they cannot control what appears on a friends' profile (Dwyer *et al.*, 2007).

Numerous researchers have examined the ease at which it is possible to collect or "*crawl*" information from the personal profiles and social graph data available on SNSs (Chau *et al.*, 2007, Mislove *et al.*, 2007b, Krishnamurthy and Wills, 2008, Bonneau *et al.*, 2009, Balduzzi *et al.*, 2010) and how even data that is presented in anonymous form can be re-identified (Backstrom *et al.*, 2007, Narayanan, 2009). It is possible to crawl information from personal profiles and social graph data regardless of a user's privacy settings (Bonneau *et al.*, 2009).

Social engineering techniques can be also be used on SNSs to become friends with users and gain access to their personal information. A college student showed how easily this can be achieved, he wrote a computer program that sent messages to 250,000 Facebook users across the US and asked them to add him as a friend, 75,000 users agreed and thus made their profile information available to a random stranger (Jump, 2005). Jagatic *et al.*

(2007) discuss how phishing attacks can be honed by harvesting publicly available personal identifying data on social networks. They simply harvested freely available acquaintance data for Indiana University students by crawling social network web sites. They performed an actual phishing attack on these students and found that users are four times more likely to become victims of phishing attacks if they are solicited by someone who appears to be a known acquaintance. They found that females and younger targets were more likely to become victims. They also found that phishing attacks were more successful if the spoofed message appeared to be sent by a person of the opposite sex. A study by Bitdefender (Datcu, 2010) sent friend requests from a young female to 2,000 adult users of SNSs and found that 94% accepted the friend request. The experiment revealed that after a 2 hour online conversation, 73% revealed what appears to be confidential information from their work place, such as future strategies, plans, and unreleased technologies/software.

Researchers have examined user's perception of the audience on SNSs. Lampe, Ellison and Steinfield (2006) in a study of undergraduate students found that users of Facebook assumed their profiles were being searched and viewed by peers rather than non-peer members of networks (academic staff and administrators) or outsiders. In further follow up studies in 2007 and 2008 Lampe *et al*. (2008) found that this perception remained. Research in this area has examined how users define their private and public spheres on SNSs. Findings indicate that in the context of SNSs the notions of public and private spheres are not simple or straightforward. Studies have found that users often do not perceive two distinct realms, and their perceptions of a "*public*" sphere appeared to be the individual's private social world (Livingstone, 2008, Phippen *et al.*, 2009, Pike *et al.*, 2009, West *et al.*, 2009). The lines between the public and private spheres are not clearcut, for example Livingstone (2008) reports on an adolescent viewing his own profile as private which he wanted to be "*public*" to his friends but "*private*" to his parents. Most users are generally unaware of the potential audiences for their personal information and the limited amount of privacy afforded to them by SNSs (Bonneau *et al.*, 2009, Debatin *et al.*, 2009).

Attitudes to Privacy on SNSs

Some studies have examined the strategies that users employ to protect themselves on Facebook. Young and Quan-Haase (2009), in their study of 77 undergraduate students, found that the privacy protection strategies employed most often were the exclusion of personal information, the use of private email messages and changing the default privacy

settings. Tufecki (2008) found, in a study of 704 undergraduate students, that users adjusted profile visibility but tended not to restrict the information within the profile. A qualitative study of 18 university students carried out by Strater and Lipford (2008) found that users privacy decisions are generally an all-or-none, one-time process. They found that users with privacy concerns restricted access to all their information or restricted their profile to friends only whereas other users left the privacy settings at the default settings. The participants also reported that many of their privacy or disclosure decisions were made early in profile creation and rarely reconsidered or altered. They only changed their disclosure and privacy strategies if something negative happened, such as being contacted by a stranger. Debatin *et al.* (2009) investigated this further and found that users were more likely to take action to protect themselves if the negative experience happened to them personally as opposed to hearing about it from others, indicating that a personal violation of privacy is what actually prompts a change.

Early studies examining user's privacy settings on SNSs found that the majority of users were not setting their profiles to be restricted or private (Gross and Acquisti, 2005, Anchor, 2007, Dwyer, 2007, Hinduja and Patchin, 2008b, OFCOM, 2008). There is evidence that this trend is changing and in particular with younger users (boyd and Hargittai, 2010, Livingstone *et al.*, 2010b, Madden and Smith, 2010, O'Neill *et al.*, 2011). Although not empirically examined, boyd and Hargittai (2010) suggest that these changes may be due to increased media attention of privacy matters or could be due to the improved changes in Facebook's default settings, particularly for minors. These changes could also be attributed to Internet safety awareness campaigns directed to children and adolescents. Studies have found that women/girls have greater online safety concerns and are more likely than men/boys to alter their privacy settings (Lewis *et al.*, 2008, Fogel and Nehmad, 2009, Phippen *et al.*, 2009, Livingstone *et al.*, 2010b, O'Neill *et al.*, 2011). Frequency of use (Lewis *et al.*, 2008, boyd and Hargittai, 2010), Internet skill level (boyd and Hargittai, 2010), and type of Facebook use (boyd and Hargittai, 2010) have been found to be correlated with restricting privacy settings. A study by Lewis *et al*. (2008) which analysed downloaded profiles of students in a university found that students were more likely to have a private profile if their friends and roommates have them.

A number of studies have examined, using surveys, users' attitudes to privacy on SNSs and have found significant dichotomies between specific privacy concerns and the information that was actually revealed (Acquisti and Gross, 2006, Dwyer *et al.*, 2007, Livingstone,

2008, Tufekci, 2008, Debatin *et al.*, 2009, Fogel and Nehmad, 2009, Young and Quan-Haase, 2009). This reflects the "*privacy paradox*" that is evident in other Internet applications (see Section 3.3.3).

Many reasons have been suggested as to why users of SNSs willingly provide personal identifying information and do not restrict their privacy settings:

1. Signalling: providing selective information to present oneself in a positive light or to be seen in a certain way (Donath and boyd, 2004, OFCOM, 2008);
2. Peer pressure: when peers are sharing certain types of information, the user may feel obliged to do so as well (Gross and Acquisti, 2005);
3. Lack of awareness of the risks (Gross and Acquisti, 2005, OFCOM, 2008);
4. Assume SNS has taken care of privacy issues (Gross and Acquisti, 2005, OFCOM, 2008);
5. Difficulties with understanding and manipulating privacy settings on a SNS (Gross and Acquisti, 2005, Anchor, 2007, OFCOM, 2008);
6. Accept default privacy setting of SNS which are often not restrictive (Gross and Acquisti, 2005).
7. Other online sites and facilities (such as online banking and e-commerce sites) were perceived to carry more risks (OFCOM, 2008);
8. Younger users felt they were "invincible" and even if they were affected by the risks discussed, they would be able to deal with them (OFCOM, 2008).

Few studies have empirically tested why users disclose information on SNSs. De Souza and Dick (2009) in a study of 263 high school students in Australia, examined how certain factors contributed to information disclosure on SNSs. They examined the factors of peer pressure, signalling, trust, view of privacy risks, web site design and attitude to privacy. They found that information disclosure on MySpace was driven by three factors: peer pressure, website interface design and signalling. Their study also suggested that children who are taught to value privacy are less likely to disclose sensitive information on-line. Utz and Krämer (2009) carried out a study to examine if there was a trade off between privacy concerns and impression management and found that impression management motives and narcissism led to less restricted profiles.

In an ethnographic study of emerging adults, Raynes-Goldie (2010) found that SNS users were concerned about privacy, but specifically "*social privacy*" rather than "*institutional privacy*", i.e. they were more concerned about controlling access to their personal information rather than how Facebook the company might use that information. Raynes-Goldie (2010) suggests that privacy pragmatism can be used to explain why users continue to use Facebook despite their concerns about their social privacy. Privacy pragmatists are defined by Westin (1996) as people who are concerned about privacy but are willing to sometimes trade it for other benefits. Debatin *et al.* (2009) found that Facebook was so integrated into the daily life of the students in their study that it had become an indispensible tool and that the benefits of Facebook far outweighed any privacy concerns.

Summary

SNSs are businesses where revenue is generated from targeted advertising. SNSs want to ensure that users share as much personal information as possible. This means that privacy settings on SNSs can be difficult for users to manage and understand and often users accept unrestrictive default settings. Users of SNSs willingly reveal substantial amounts of personal information, but there is evidence to suggest that younger and older users are more careful about revealing personal information. Even when individual users are careful about the information they reveal, it is still possible to find personal information about them by aggregating information found in other sources and searching information posted by their friends and colleagues. Personal information can also be gleaned using new technologies such as face recognition software. This information can be aggregated over time. Users of SNSs assume that the audience on SNSs is their peer group and are unaware how easy it is for others to gain access to their personal information. Early studies into privacy attitudes on SNSs suggested a privacy paradox in that users expressed concern about their privacy on SNSs, but were not protecting their SNS profiles. Recent studies suggest the notion of a privacy movement (Lewis *et al.*, 2008). This may be due to increased awareness or experience of negative events on SNSs, but also that users have gained more experience with the technology. These changes are reflected in the tightening of privacy settings but are not so evident in the amount of information revealed. Although many users express concern about their privacy on SNSs, there appears to be a disconnect between expressions of privacy concern and the amount of personal information they reveal. Many reasons have been proposed as to why users reveal such personal information, from ignorance of the risks to acts of defiance. There has been little empirical research in this area and further research is needed to explore this disconnect.

3.4.3 Trust on Social Networking Sites

Trust and its relationship with risk perceptions and in particular with online shopping transactions have already been discussed in Chapter 2, Sections 2.4.3 and 2.5.3 respectively. As users of SNSs reveal substantial amounts of personal information and create far reaching networks of friends, researchers have begun to examine whether trust also plays an important role in SNSs. To date research in this area is limited and studies have reached no consensus.

An examination of the literature in this area reveals only a handful of studies that have examined trust on SNSs. A study of 117 SNS users by Dwyer *et al.* (2007) examined how trust in a SNS and its members affected a user's willingness to share information and develop new relationships. The study created two trust measures, one for trust in the site and the other for trust in the other members of the site. Both these scales were tested for reliability using Cronbachs' alpha and neither scored above the recommended cut-off of 0.7 and thus do not appear to be reliable measures of trust. The authors, however, suggest that their results show that in SNS transactions, trust is not as necessary in the building of new relationships as it is in FtF encounters. Interestingly, a recent Eurobarometer (2011) study found that younger users (aged 15-24) are more trusting of all authorities, institutions and commercial companies and hold the SNSs responsible for the safe handling of their data. Research into trust in Internet shopping systems indicates that individuals with a higher propensity to trust place more trust in e-commerce systems (Gefen, 2000, McKnight *et al.*, 2002). Utz and Krämer (2009) examined dispositional trust in SNSs and its influence on the choice of privacy settings on SNSs. They found dispositional trust had no significant effect.

Some studies have found that trust has an effect on SNS use. A study by Fogel and Nehmad (2009) of 205 undergraduate students used a consumer trust scale developed by Pan and Zinkhan (2006). Their study found that Facebook attained greater trust ratings than MySpace, they assert that this may be because until 2006 Facebook was restricted to students while MySpace was open to all users. Christofides *et al*. (2009) found evidence of a negative relationship between trust and information control on SNSs.

It is clear that trust in SNSs is an area that has not yet been adequately addressed in the research literature. As trust has been shown to be a factor in online shopping and is an important component of FtF communication, trust may also play an important part in communications on SNSs, further research is needed in this area. As suggested by Brandtzæg *et al.* (2010) it is important to consider "*social trust*" (e.g. "I trust my friends") as well as "*site trust*" (e.g. "I trust Facebook"). As SNS users add friends from different social circles (both weak ties and strong ties) there is a potential for social distrust.

3.4.4 Impression Management on Social Networking Sites

Research on identity development of children has shown that children actively explore and question various beliefs, boundaries, goals and roles before assimilating those that provide a sense of uniqueness (distinction from others) and a sense of unity (sameness with others) (Erikson, 1968, Bosma and Kunnen, 2001). Many elements on the Internet can facilitate identity development. A number of researchers have examined the ways in which SNSs can facilitate elements of identity development, and have particularly looked at what is sometimes referred to as impression management (Goffman, 1959).

In SNSs, the creation of a profile is an important aspect of impression management; this is because one way to gain an impression of a user is to examine their profile, their friends and their comments. Some researchers assert that users present a socially appropriate representation of themselves rather than a truthful representation by selecting how and what to convey to viewers (boyd, 2004, Manago *et al.*, 2008, Zhao *et al.*, 2008). They attribute this to the fact that users are often afraid that their employer, parents, teacher etc. will see their profile and consequently they present themselves in a way they want to be perceived rather than a truthful representation. A contrasting view is that SNSs self-presentations are accurate and authentic (Gosling *et al.*, 2007, Back *et al.*, 2010).

As stated by Back *et al*. (2010) it is difficult to create an idealised identity on a SNS as friends and wall posts and the system itself provide further reputational information and cues about a user's identity. Viewers of SNS profiles often look at these features to gain an impression of a user. Walther and Parks (2002) refer to this as the "*warranting principle*". The warranting principle asserts that a viewer's impression of a user relies more heavily on information that the user cannot manipulate than on self-descriptions. For example, the list of friends made by users on SNSs allows viewers to validate the identity

information presented in profiles (Donath and boyd, 2004). A study by Tong *et al*. (2008) of 153 university students found that having too few or too many friend connections can raise doubts about a Facebook user's popularity and desirability. Another study carried out on university students, found not surprisingly, that the physical attractiveness of a user's friends has a significant effect on the physical attractiveness of the profile's owner (Walther *et al.*, 2008). The study also found that comments written by others on a user's profile can also be revealing, in that complimentary comments by friends improved the profile owner's social attractiveness as well as their credibility. Other studies have compared the influence of self-generated and other-generated statements and found support for the warranting principle (Walther *et al.*, 2009, Utz, 2010).

Gender differences have also been found in the creation of profiles (Peluchette and Karl, 2008, Strano, 2008). Peluchette and Karl (2008) who surveyed 433 university students, found that males were significantly more likely than females to place self-promoting and risqué pictures or comments (involving sex or alcohol) on their profile, whereas females were significantly more likely than males to post romantic pictures and comments. Strano (2008) found that females tend to change their profile image more often and tend to emphasize friendship in the images they choose to display. In one of the few studies that have examined an adult population, Strano found that older users are less likely to change their profile images frequently and more likely to display images of themselves alone.

3.4.5 Network Structure

A number of researchers have studied the network structure of friendship on SNSs. Kumar *et al.* (2006) carried out a mathematical analysis of the entire lifetime of two SNSs, Flickr and Yahoo! 360. Their research suggests that there are three different categories of SNS users:

- Passive members of the network;
- Inviters who encourage offline friends and acquaintances to migrate online; and
- Linkers who fully participate in the social evolution of the network.

Qualitative research by OFCOM (2008) suggests that users of SNSs fell into five distinct segments based on how they used and interacted with others users, see Table 3.3.

	Style of use	Gender	Age	Typical sites	Number of people
Alpha socialisers	Flirting, meeting new people	Mostly male	Under 25s	Bebo, MySpace, Hi5	Minority of the sample
Attention seekers	Posting photos to get comments from others	Mostly female	Teens to 35+ (esp. mothers)	Bebo, MySpace, ICQ	Some of the sample
Followers	Keeping up with friends	Male and female	All	Bebo, MySpace, Facebook, Hi5, ICQ	Many in the sample
Faithfuls	Finding old friends	Male and female	Older 20+	Facebook	Many in the sample
Functionals	Pursuing interests and hobbies	Mostly male	Older 20+	Facebook, MySpace, Bebo	Minority of the sample

Table 3.3 Summary of SNS User Segments (source: OFCOM (2008, p28)**)**

This research highlights that SNS users are not a uniform group in terms of use, attitude and behaviour. Survey research carried out by Hargittai (2007) on over a thousand university students found that certain demographic characteristics (such as gender, ethnicity and parental education) can affect the choice of SNS. Other research in the area of network structure has examined topics such as the problem of predicting, classifying, and annotating friend relations (Hsu *et al.*, 2007, Mislove *et al.*, 2007a) and examining what motivates users to join particular communities (Backstrom *et al.*, 2006).

OFCOM (2008) carried out qualitative research to explore the attitudes of non-users of SNSs and to ascertain their reasons for not using them. They categorised the reasons into three broad groupings: concerned about safety, technically inexperienced, and intellectual rejecters. These are summarised in Table 3.4.

	Gender	Age	Reason for non-use
Concerned about safety	Male and female	Often older and parents	Anxious about safety risks to themselves and/or their children
Technically inexperienced	Male and female	Often older and parents	Lack of confidence with the Internet and computers generally
Intellectual rejecters	Male and female	Older teens and young adults	Thought that SNS were a waste of time and beneath them

Table 3.4 Categories of Non-Users of SNS ((source: OFCOM (2008, p32)**)**

3.5 Risks with Social Networking Sites

This section examines in detail some of the concerns and risks in using SNSs. Producing a definitive list of risks associated with SNSs is difficult as this is a rapidly evolving environment. The negative effects of SNSs are still emerging. One recent example is the UK court case where a juror contacted a defendant in a multi-million-pound drugs case, this resulted in the trial collapsing and the juror being in contempt of court and facing an eight month jail sentence (Carter, 2011). A further example is how social media was used to enable and coordinate the August 2011 London riots, prompting the UK government to consider banning people thought to be plotting criminal activity from using SNSs (Halliday, 2011). These examples illustrate that what is said online and how social media is used can have serious real-world effects, but also the difficulty in predicting how people will potentially use the technology.

From reviewing the literature a number of general risk categories can be identified:

- Threatening Risks;
- Personal Information Risks;
- Technology Risks;
- Excessive use of SNSs;
- Reputational Risks; and
- Other risks.

3.5.1 Threatening Risks

Threatening risks have been categorised as those risks that can potentially cause serious physical or mental harm for individuals. These risks include:

1. Cyberbullying and Stalking;
2. Strangers Online;
3. Encountering Inappropriate and Harmful Content; and
4. Sexual Harassment.

As these risks can have serious consequences, much of the research examining the risks associated with SNSs has concentrated in this area.

Cyberbullying

A risk facilitated by SNSs is online bullying or cyberbullying, this is a threat that is considered particularly risky for children and adolescents, as children and adolescents lack the emotional skills necessary to deal with cyberbullying. Smith *et al.* (2006, p1) define cyberbullying as: "*an aggressive, intentional act carried out by a group or individual, using electronic forms of contact, repeatedly and over time against a victim who can not easily defend him or herself*." Cyberbullying can take place using many electronic forums including SMS and MMS messages, instant messaging, email, chat rooms and other web sites including SNS sites. SNSs can further enable bullying as the personal information contained in SNSs can be passed on or manipulated by bullies. Cyberbullying can take many forms including flaming (aggressive or hostile communication occurring via CMC), harassment, cyberstalking, denigration (put-downs), impersonation of target, outing, trickery and exclusion (Willard, 2007). Cyberbullying is distinct from real world bullying in a number of ways:

- Cyberbullying offers some anonymity for the bully (Ybarra and Mitchell, 2004b, Deboelpaep and EPTA, 2006, Millwood Hargrave *et al.*, 2007), but on the other hand a degree of publicity for the victim. An episode of cyberbullying can reach a wide audience (O'Moore and Minton, 2010);
- The bullying message can be quickly spread among a peer group and also amongst strangers;
- Those bullied can be targeted outside conventional time and space limits. The bully can target the victim anyplace, anytime even in the victim's private and supposedly safe place (their bedrooms, on their mobile phone, at home) (Keith and Martin, 2005, Patchin and Hinduja, 2006, O'Moore and Minton, 2010);
- One aspect of real world bullying is that the behaviour is not a one-off occurrence, but is a repeated harassment of the same individual. This is not necessarily the case with cyberbullying as a defamatory comment on a web page can stay online for a long period of time and can be read by many individuals (Deboelpaep and EPTA, 2006);
- There is a lack of physical and social cues with cyberbullying, this means that cyberbullies do not see the way their victims react and the consequences of their harassment (Postmes *et al.*, 1998, Deboelpaep and EPTA, 2006) and this lack of cues can lead to uninhibited, aggressive and impulsive behaviour (Kiesler *et al.*, 1984);

- Supervision is lacking in cyberspace and there is no monitoring or censorship of offensive content (Patchin and Hinduja, 2006);
- Teenagers tend to know more about technology than their parents do and are often able to use the technology without the worry that their parents will discover their participation or victimisation in bullying (Deboelpaep and EPTA, 2006, Patchin and Hinduja, 2006, O'Moore and Minton, 2010). On the other hand, cyberbullying can be digitally traced, providing levels of proof, in a way that conventional bullying cannot.

The consequences of cyberbullying are serious and can ultimately lead to physical, social and psychological problems (Ybarra, 2004, Patchin and Hinduja, 2006, Wolak *et al.*, 2006) and in extreme cases can lead to suicide (termed bullycide by Marr and Field (2001)) (Bramwell and Mussen, 2003, Riegel, 2007, Marlowe, 2010). This is compounded by the fact that many school teachers and administrators are aware of school bullying, but are unaware that students may be harassed and bullied through electronic communication (Beran and Li, 2005, O'Moore and Minton, 2010).

Recent comprehensive studies of children and adolescents in Ireland and Europe indicate cyberbullying rates of between 4% and 14% (O'Moore and Minton, 2010, Livingstone *et al.*, 2011a, O'Neill *et al.*, 2011). In a nationwide study of 2,794 Irish adolescents (12-16 year olds), 14% of respondents reported experiencing cyberbullying over the past couple of months and 9% reported that they had cyberbullied others (O'Moore and Minton, 2010). The Irish EUKids online study of 994, 9-16 year olds found that only 4% of Irish respondents had been bullied online (O'Neill *et al.*, 2011). The study found that older adolescents (15-16 year olds) reported the highest levels of cyberbullying (9%) and that SNSs were providing the main platform for online bullying. Overall EU averages suggest that 6% of 9-16 years olds are bullied online and 3% have bullied others but indications are that most bullying still occurs offline than online (Livingstone *et al.*, 2011a).

A number of exploratory studies have been carried out by academic researchers such as Li (Beran and Li, 2005, Li, 2006, 2007b, a) and others (Ybarra and Mitchell, 2004a, Patchin and Hinduja, 2006, Smith *et al.*, 2006, Dehue *et al.*, 2008). Many of these studies have been based on limited sample sizes. Li (Li, 2006, 2007b, a) found that over half the students surveyed knew someone that had been cyberbullied, over a quarter of students had experienced cyberbullying and one in six students had cyberbullied others. These results

are consistent with those found in other academic surveys, for example Patchin and Hinduja (2006) reported that almost 30% of the adolescents they surveyed had been victims of online bullying. This result is higher than some other surveys possibly because the authors included "*being ignored*" as a component of online bullying. It is difficult to ascertain the extent to which cyberbullying is a problem as varying definitions and conceptualisations of cyberbullying are used in studies, but the comprehensive nationwide and EU studies (O'Moore and Minton, 2010, Livingstone *et al.*, 2011a, O'Neill *et al.*, 2011) probably provide a closer estimate to the real extent of the problem.

The academic research in this area has produced some other interesting findings. Most cyber victims did not know who the bully was. Ybarra and Mitchell (2004a) found in a telephone survey of 1,498 10-17 year olds that the majority of bullies (84%) knew their victim in person, whereas only 31% of victims knew their harasser. This highlights one of the unique characteristics of cyberbullying – anonymity. This anonymity makes it easier for cyberbullying to happen and more difficult to prevent. Studies have examined the relationship between real world bullying and cyberbullying to see if the same patterns exist in the online and offline worlds. These studies have found that those who bully in schools tend to also bully using electronic means as well (Li, 2007b, Dehue *et al.*, 2008). The victims of offline bullying also tend to be cyber bully victims (Li, 2007b). There is thus a close tie between bullying and cyberbullying. Another aspect of bullying is that the bullied often become bullies themselves in a "*victim-bully cycle*" (Perry *et al.*, 1988, Ma, 2001). Studies have found (Deboelpaep and EPTA, 2006, Li, 2007b, Erdur-Baker, 2010, Gorzig, 2011) that this cycle also exists for cyberbullying. Contrary to the belief that females might prefer this medium for bullying (Keith and Martin, 2005), studies (Deboelpaep and EPTA, 2006, Li, 2006, 2007a, Dehue *et al.*, 2008, Erdur-Baker, 2010) have found that males are more likely to cyberbully than females, this is also the case in traditional forms of bullying. Studies of the victims of cyberbullying have found contradictory results, with some studies indicating that females are more likely to be the victims of cyberbullying (Smith *et al.*, 2006, Li, 2007b, Dehue *et al.*, 2008, O'Moore and Minton, 2010), some have found no gender differences (Li, 2006, 2007a, Gorzig, 2011, Livingstone *et al.*, 2011a) and others have found that males are more likely than females to be the victims of cyberbullying (Erdur-Baker, 2010). Studies have found (Li, 2006, 2007b, a, O'Moore and Minton, 2010) that the vast majority of students who were cyberbullied or knew someone who was cyberbullied chose to be quiet about it rather than inform adults. Some age differences are evident, victimisation rates were found to be generally lower in early

adolescence and higher in mid-adolescence (around age 14-15) (Ybarra and Mitchell, 2004a, Lenhart and Madden, 2007, Hinduja and Patchin, 2008a, O'Neill *et al.*, 2011).

The majority of research studies in this area have examined cyberbullying from a child/adolescent viewpoint, but workplace bullying is also an issue. Large organisations, male-dominated organisations, and industrial organisations show the highest prevalence of workplace bullying (Einarsen and Skogstad, 1996, Zapf *et al.*, 2003, Bowling and Beehr, 2006, Ortega *et al.*, 2009). In one of the few studies examining cyberbullying in the workplace, Privitera and Campbell (2009) found that in manufacturing environments 34% of respondents were bullied FtF and 11% were cyberbullied. They found that all victims of cyberbullying also experienced FtF bullying.

The consequences of cyberbullying are serious and can ultimately lead to physical, social and psychological problems. Cyberbullying provides facilities for the bullies that are not available in the offline world. The anonymity and a lack of visual cues in CMC can lead to more extreme forms of bullying. For the victim, the bully can harass them at anytime and in any place. Research studies indicate that cyberbullying is a serious problem for children and adolescents. Further research is needed to see if SNSs are enabling cyberbullying behaviour. Although this problem is not so serious for adults, work place bullying is an important concern and early studies in this area indicate that cyberbullying is also a problem in the workplace.

Stalking

Stalkers use many means to facilitate their pursuit, and one of the increasingly available means of intrusion is Internet technologies (Spitzberg and Hoobler, 2002). Cyberstalking has been defined as the use of electronic communication technologies including pagers, mobile phones, email and the Internet to bully, threaten, harass and intimidate a victim (Ellison and Akdeniz, 1998, Ogilvie, 2001). A study by Maple *et al.* (2011) found that stalkers use a combination of technologies to harass their victims, but the primary technologies used are SNSs (61%) and email (56%). Like cyberbullies, stalkers can benefit from the quantity of personal information available on SNS profiles. Researchers have only recently begun to empirically investigate the phenomenon of cyberstalking (Spitzberg and Hoobler, 2002, D'Ovidio and Doyle, 2003, Alexy *et al.*, 2005, Sheridan and Grant, 2007, Maple *et al.*, 2011). It is difficult to get reliable figures for the prevalence of cyberstalking, as studies have used differing definitions and sampling methods. Rates vary

from 3.7% reported by Alexy *et al.* (2005) to 7.2% (Sheridan and Grant, 2007) and 14.5% (Spitzberg and Hoobler, 2002). There is some agreement in that studies indicate that cyberstalkers were most likely to be a former intimate partner (Alexy *et al.*, 2005, Sheridan and Grant, 2007) and the victims were more likely to be female (D'Ovidio and Doyle, 2003, Sheridan and Grant, 2007, Maple *et al.*, 2011), but some studies have found that males are more likely than females to be cyberstalked (Alexy *et al.*, 2005). D'Ovidio and Doyle (2003) conducted a descriptive study on cyberstalking using official police records of the New York City Police Department (NYPD). They found that approx 80% of the perpetrators were male with an average age of 24, nearly a quarter of the perpetrators were juveniles under the age of 16. Research indicates that cyberstalking can cause as much serious harm to the victim as offline stalking (Maple *et al.*, 2011). In a study of 1,261 self-defined victims of stalking, Sheridan and Grant (2007) found that the psychological, social and financial effects did not differ significantly according to degree of cyberstalking.

Strangers Online

Another risk posed by SNSs is that individuals interact and may even meet strangers that they have communicated with online. One of parents' greatest concerns with online safety is the risk of "*predators*" and in particular the risk of online sexual solicitation and the possibility that this will lead to an offline meeting with a stranger.

A qualitative study covering 29 European countries, conducted as part of the EU Safer Internet programme (EUROBAROMETER, 2007b) found that children considered contact with adult strangers the highest risk activity on the Internet. Studies however show that a sizeable minority of adolescents meet in person strangers that they have initially met online. A recent Irish EU Kids Online study found that nearly one third of children have made contact with someone they did not previously know online (O'Neill *et al.*, 2011). Just 4% of respondents have gone to face to face meetings, but this rises to 10% for 15-16 year olds. The findings for Ireland are below the European average where 9% of respondents have met up with an online contact and this percentage rises to 16% in the 15-16 year age group (Livingstone *et al.*, 2011a). It is important to note that the majority of these meetings with offline contacts appear to be friendship related and tend to be between similar age groups (Wolak *et al.*, 2006), nevertheless some online contact can be intended as "*grooming*" (Kierkegaard, 2008).

Research by Peter, Valkenburg *et al.* (2006) examined the characteristics and motives of children who talk with strangers on the Internet. They examined whether characteristics such as age, gender, introversion and frequency and intensity of communication were significant characteristics of children who interacted with strangers on the Internet. They also examined five motives that might influence children's communication with strangers online: entertainment, social inclusion, maintaining relationships, meeting new people and social compensation. They found that younger adolescents (12 -14 year olds) were more likely to talk with strangers, but found no gender and introversion differences. The motives for these children to seek contact with strangers were a mix of being bored (entertainment motive), curiosity (meet people motive) and inhibited in FtF conversation (social compensation motive).

Studies have found that older adolescents are more likely to meet up with these contacts (Liau *et al.*, 2005). Research indicates that older children tend to be over confident and adopt more risky behaviour (particularly in meeting in person strangers that they have met online) and they were reluctant to warn their parents (or only in the last resort) (EUROBAROMETER, 2007b). It seems that although there is an awareness and understanding of the potential dangers of meeting these strangers, significantly high proportions of children still do. Millwood Hargrave, Livingstone *et al.* (2007) suggest that this may be because many children are confused about the relation between acquaintances, "*friends of friends*" and strangers and SNSs can compound this confusion with their emphasis on collecting large numbers of "*weak ties*".

Inappropriate and Harmful Content

In broadcast media it is possible to restrict access to certain material for certain ages. For example, films, DVDs and computer games all have age ratings and classifications and the watershed restricts when television programmes which have "*adult content*" can be shown. However, when it comes to the Internet, these restrictions do not exist. Popular press articles have portrayed the Internet as awash with pornographic and sexual material and that avoiding contact with it is virtually impossible (Elmer-Dewitt *et al.*, 1995). On the Internet children can easily get access to age-inappropriate content and in many cases can stumble across this content accidentally. Studies indicate that between a quarter and a third of children/adolescent Internet users had seen sexual material that they had not searched for (Mitchell *et al.*, 2003, NCTE/SAFT, 2003, Wolak *et al.*, 2006, WEBWISE, 2009). Studies found no significant gender differences in the levels of unwanted exposure

(Mitchell *et al.*, 2003), but boys were more likely to admit to voluntary exposure (Flood, 2007, WEBWISE, 2009).

Researchers have examined the impacts of viewing pornography. Research to date suggests that non-violent pornography exposure has few demonstrated effects, except to promote more permissive sexual attitudes amongst those repeatedly exposed (Davis and Bauserman, 1993). Research studies on violent pornography have suggested that viewing material of this nature may reinforce aggressive behaviour and negative attitudes towards women, particularly amongst those with some aggressive predisposition (Koop, 1987, Allen *et al.*, 1995). Most of this research has been based on college students and investigates voluntary exposure rather than unwanted or unexpected exposure. A study by Mitchell *et al*. (2003) examined children's and teenagers unwanted exposure to sexual material on the Internet and found that 25% of respondents in their study had experienced unwanted exposure to sexual material. Most respondents had no negative reactions to their unwanted exposure, but one quarter said that they were very or extremely upset. A recent EU Kids Online study found similar results. 14% of respondents had seen sexual or pornographic images online and one in three were bothered by the experience (Livingstone *et al.*, 2011a).

Sexual Harassment

Another form of bullying, sexual harassment is also found in cyberspace. Although this is an extremely serious threat for children and adolescents, it is also a serious treat for the adult population. Most victims of sexual harassment are female (Barak, 2005), but other target populations – men, homosexuals and children – are harassed too, although to a lesser extent. Barak (2005) describes the three types of sexual harassment that exist in the offline world. Gender harassment involves unwelcome verbal and visual comments and remarks that insult individuals because of their gender. Unwanted sexual attention refers to uninvited behaviours that explicitly communicate sexual desires or intentions towards another individual. Sexual coercion involves putting physical or psychological pressure on a person to illicit sexual cooperation. All three types of sexual harassment can exist on the Internet, but the most prevalent are gender harassment and unwanted sexual attention. Studies with children and adolescents have found that between 15 – 25% of respondents have been the target of unwanted sexual solicitation (Mitchell *et al.*, 2001, NCTE/SAFT, 2003, Wolak *et al.*, 2006, WEBWISE, 2009, Livingstone *et al.*, 2011a). Girls and older adolescents (14-17 year olds) were at most risk (Mitchell *et al.*, 2001, WEBWISE, 2009,

Livingstone *et al.*, 2011a). Although it is difficult to determine the exact content of these messages, it appears that most sexual messaging is relatively mild (Wolak *et al.*, 2006, Livingstone *et al.*, 2011a).

Ybarra and Mitchell (2008) have carried out research to assess whether sexual harassment is more prevalent on SNSs as opposed to other forms of online environments. Their survey (n=1588, 10-15 year olds) results found that 15% of respondents had received an unwanted sexual solicitation online in the last year and only 4% had reported an incident on a SNS specifically. Solicitations were more commonly reported via instant messaging and chat rooms. It would appear that the asynchronous communication and the fact that much of the communication on SNSs is publicly viewable would make SNSs unsuitable for solicitations of this nature. However, SNSs can still play a role by providing harassers with contact information and a way to make initial contact.

Sexting

"*Sexting*" (an amalgam of "sex" and "texting") is commonly used to describe the creation and transmission of sexual images by minors. It originated with mobile phones, but the term can also apply to any digital media such as e-mail, instant messaging and SNSs. A core concern about sexting is that the minors that create images of themselves and others can meet the criminal definitions of child pornography. This has led to a number of studies investigating the prevalence of this problem. (National Campaign to Prevent Teen and Unplanned Pregnancy and CosmoGirl.com, 2008, Associated_Press and MTV, 2009, Cox_Communications, 2009, Lenhart, 2009, Phippen, 2009, Livingstone *et al.*, 2011a, O'Neill *et al.*, 2011). Lounsbury *et al.* (2011) argue that some of these studies overestimate the prevalence of sexting as they have used unrepresentative samples, used varying definitions of sexting and introduce the potential for misinterpretation by the media. For example, the Teen Online and Wireless Safety Survey carried out by Cox Communications (2009) included 18 years olds in their sample. Sexting amongst this age group would not be illegal. The findings of this report are commonly summarised as "one in five teenagers (19%) has engaged in sexting", this is misleading as this figure is largely made up of teens who only received the images, only 9% of respondents had sent the images (Lounsbury *et al.*, 2011). A more rigorous study carried out by EU Kids Online provides a more accurate picture of the prevalence of this problem. The Irish study (O'Neill *et al.*, 2011) found that 3% of 11-12 year olds, 7% of 13-14 year olds and 21% of 15-16 year olds have seen or received sexting messages. Only 3% has posted such messages.

3.5.2 Personal Information Risks

The privacy aspects of SNSs have been discussed in detail in Section 3.4.2. Users of SNSs reveal substantial amounts of personal identifying information and many details about their personal life. This can make users more vulnerable to risks such as stalking (see Section 3.5.1), identity theft, building a digital dossier, advertising, spam, phishing (see Section 3.5.3) etc. This section examines the advertising and identity theft risks.

Advertising/Commercial Persuasion

There are clear commercial opportunities for businesses on SNSs, as SNSs offer a cheap way of reaching a potentially large audience. The large numbers involved in social networking and the dominance of the traditionally hard to reach cohorts of children/adolescents and emerging adults has raised interest in marketing to SNS users. The information that SNSs hold about their users enables marketers to target their message to specific demographics.

Over the past twenty years, children's and adolescent's consumer power has expanded and this has led to rapid increases in marketing targeted at younger age groups. Marketing to children in the offline world is regulated, but concerns have been expressed as advertisers are now targeting unregulated online environments. New forms of on-line marketing practices such as "*branded communities*", "*gamevertising*" and "*word of mouth (WOM)"* marketing techniques such as "*viral marketing*", "*guerrilla marketing*" and "*buzz marketing*" are all being used on SNSs to reach these previously difficult to access markets. One way of reaching consumers is for brands to set up their own profiles on SNS and accept "*friends*" who can keep up-to-date with the latest brand news, SNS users can choose to "*Like*" brands. Some commercial brands go so far as to set up their own SNSs to offer children and older consumers entertainment in "*branded communities*". One such example is the SNS Club Penguin, which is targeted at young children and is a commercial venture of the Disney Corporation. Gamevertising is advertising that is included in custom-made online games designed to promote a company's brand or products (Youn, 2008). Popular SNS games, such as Farmville, Pet Society and Café World generate revenues through advertising, sponsorship, and virtual money required to play the game. One of the largest producers of SNS games applications is the Zynga corporation. For 2011, Zynga expects revenue to reach $1.8 billion, from which it will make $630 million in profits (Fontevecchia, 2011). Another form of branded entertainment is the "*advergame*".

Advergames are online games designed for the specific purpose of marketing a single brand or product (Winkler and Buckner, 2006). These advergames have been shown to positively enhance brand impressions (Winkler and Buckner, 2006, Wise *et al.*, 2008). For example Mini Maps[7] is a Facebook app that allows users customise a virtual MINI and challenge their Facebook friends to time trials using a Google Maps "*mash-up*".

WOM marketing techniques harness the idea that a recommendation from an accepted member of a social group will be more credible than other forms of advertising. Viral marketing uses existing social networks by encouraging customers to share product information with their friends (Leskovec *et al.*, 2007). As an example, in January 2007, Domino's Pizza revealed that it was behind a viral video that had been placed on MySpace and other popular SNSs. The video, "*MacKenzie Gets What MacKenzie Wants*," featured a spoiled rich girl who wanted a blue car for her birthday but got a red one instead. She complained until her father got her the car she wanted and then, much to the surprise and delight of video viewers, she decided to offer her red car on eBay for only $9.99, the price of the Domino's Pizza offer. According to Domino's Pizza, the campaign was a hit with over two million views, and the MacKenzie video earned a top spot on several video sharing Web sites (Dominos Pizza, Jan 25, 2007). Buzz marketing is used to create publicity and excitement about a product, often through a creative event (Jobber and Fahy, 2002). OfficeMax for the past few Christmases have used a buzz marketing event called "*elf yourself*", that allows users to animate themselves (or their friends) as elves and send the results to friends (Fine, 2009). In 2007 there were 17 million unique visitors to the Elf Yourself website. SNS games are heavily reliant on buzz marketing, the more interesting the game, the better chance for a game user to recommend it to his/her network. A WOM marketing technique that can be used on social network sites is guerrilla marketing (Gafford, 2007). This term was coined by Jay Conrad Levinson (1984). This type of marketing relies on time, energy and imagination instead of big marketing budgets. Marketing campaigns tend to be unconventional, have a high entertainment value and often leave people unaware that they have been marketed to.

These online forms of marketing allows advertisers to interact with consumers for several minutes as opposed to traditional media advertising that normally only lasts for 30 seconds. It is estimated that gamers of all ages spend an average of 25 minutes on gaming websites (Bertrim, 2005). As these marketing messages can be embedded in games, videos or other

[7] http://www.facebook.com/apps/application.php?id=129955603741193

website activities, this can have the effect of blurring the line between entertainment and advertising (Montgomery, 2001, Moore, 2004, Henke and Fontenot, 2007) and the marketing message is thus more covert and can be less immediately apparent to children (Moore and Rideout, 2007). This is of concern as research indicates that younger children may not have the cognitive skills or experience to understand the commercial intent beneath these sites (Wilcox *et al.*, 2004). Further concerns have been expressed that there is a risk of privacy loss as users share personal information when they register with these web sites or SNS applications (Lenhart, 2005). Users can also be invited to take surveys which examine in more detail their consumer behaviour. Valkenburg (2004) expressed concern that in time the social and cultural needs of children could be primarily defined by commercial media products and manufacturers.

Fogg (2008) suggests that SNSs bring together the power of interpersonal persuasion with the reach of mass media, in a phenomenon he calls Mass Interpersonal Persuasion (MIP). He contends that using SNSs individuals have the potential to change attitudes and behaviours on a mass scale. These findings are based on the uptake of student applications developed for Facebook in a 10-week Stanford university course. At the end of the course the students had persuaded over 16 million Facebook users to install their applications. Fogg attributed the success to six components that have not been present in the one location until the launch of Facebook and other SNS platforms:

1. **Persuasive Experience**: an experience that is created to change attitudes, behaviours or both;
2. **Automated Structure**: digital technology structures the persuasive experience;
3. **Social Distribution**: the persuasive experience is shared from one friend to another;
4. **Rapid Cycle**: the persuasive experience can be distributed quickly from one person to another;
5. **Huge Social Graph**: the persuasive experience can potentially reach millions of people connected through social ties or structured interactions;
6. **Measured Impact**: the effect of the persuasive experiences is observable by users and creators.

MIP is important because it gives ordinary individuals the ability to reach and influence millions of people. Although this will have direct relevance for commercial users of SNSs,

it can also be used for any case where an individual or group wants to reach and persuade masses of people. This persuasion can be positive, but can carry a risk when it is negative, as for example when a terrorist organisation or hate group is attempting to spread propaganda.

Identity Theft

Another risk associated with revealing large quantities of personal identifying information is identity theft. Denning (1999, p54) defines identity theft as "*gaining access to another person's identifiers such as name, social security number, driver's license and bank details*". Stealing someone's identity allows the perpetrator to carry out financial and personal transactions in someone else's name, leaving the victim responsible for the repercussions. The impact on the victim can be devastating in terms of loss of funds, loss of reputation and also in terms of the time required to re-establish their credentials. Identity thieves only need a small amount of information to perpetrate crimes. Any activity in which identity information is shared and made available to others creates an opportunity for identity theft (Hammond, 2003). This makes the substantial personal information available on SNSs extremely attractive to identity theft fraudsters (Nugent and Dean, 2007, Martin, 2008, McLean, 2008). Studies have highlighted the ease with which information and identity theft can take place on SNSs (Sophos, 2007, Bilge *et al.*, 2009).

3.5.3 Technology Risks

The relative openness, ease of access to rich data sources and the large volume of users on SNSs has resulted in technology related risks such as spam, phishing, viruses and malware migrating to SNSs. SNSs are being used as new platforms for existing threats such as spam and phishing simply because these are places where people are spending time in cyberspace (Hunter, 2008). As previously discussed in Section 3.4.2, fraudsters are using social engineering techniques to target their victims. The phishers can harvest identity data on social networks (Jagatic *et al.*, 2007) and then send phishing messages that appear to come from a friend. These social phishing attacks contain contextual information that makes them more successful than ones where the sender is unknown. These social engineering attacks can be difficult to spot and can lead to infections from viruses and malware.

A recent security intelligence report from Microsoft (2011) states that phishing attacks have moved away from their traditional targets, principally financial targets such as PayPal to SNSs. They present dramatic figures, see Figure 3.2 showing that phishing impressions[8] on SNSs increased from 8.3% in January 2010 to 84.5% in December 2010.

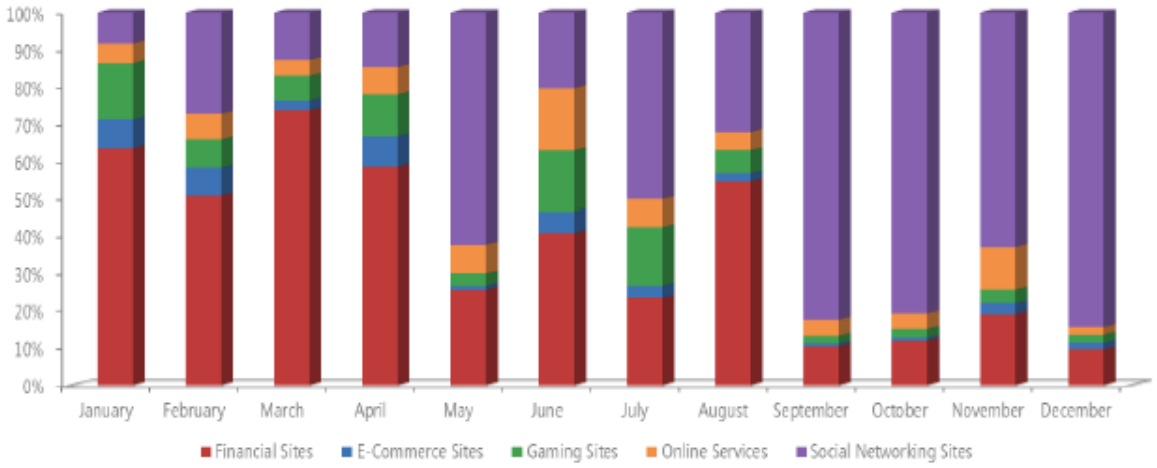


Figure 3.2 Impressions for Each Type of Phishing Site Each Month in 2010.
Source (Microsoft, 2011)

A survey carried out by anti-virus vendor, Sophos (2011) shows that users are experiencing increasing numbers of spamming, phishing and malware attacks on SNSs. Figure 3.3 shows that spamming attacks on SNSs rose further in 2010, with 67% of people surveyed receiving spam messages, up from 57% at the end of 2009 and just 33% in mid-2009. 43% of users had experienced phishing attempts and 40% had received malware.

[8] A phishing impression is a single instance of a user attempting to visit a known phishing site with Internet Explorer and being blocked.

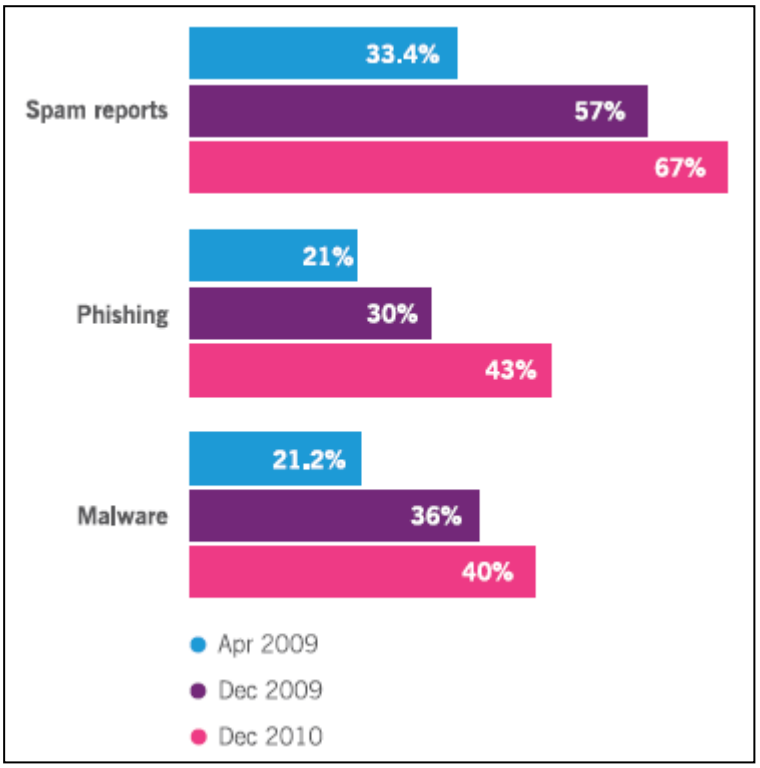


Figure 3.3 Social Networking Spam, Phishing and Malware Attacks.
Source (Sophos, 2011)

The fraudsters find many innovative ways to encourage users to part with their details or click on links that install viruses, trojans and malware on the PCs. High-tech skills are not required for these attacks (Cosoi, 2011). For example:

- The scammers commonly lure in users using humor, compromising pictures of celebrities and major news and entertainment events, but human tragedies are also used as lures. TrendMicro, an Internet Security firm, reported that within minutes of the March, 2011 earthquake in Japan, fraudsters had set up virus-laden sites and fake Facebook pages that showed up when users searched for "*earthquake in Japan*" (Owens, 2011). Many of these fake pages linked to "*scareware*" scams. Scareware scammers use legitimate looking pop-up adverts that falsely warn that a computer's security has been compromised. Users are directed to sites where they can purchase fake anti-virus software.
- Another common attack on SNSs is "*clickjacking*," or "*UI redressing*." Clickjacking uses social engineering techniques to lure new victims and trick them into clicking on a disguised link. These links can be used to spread spam, but users may also be granting access to valuable personal information and even making purchases. One such example is a scammed Facebook application that allowed users to install a "*Dislike*" button similar to the "*Like*" button already available in

Facebook. Users were sent a status update from a friend reading "I just got the Dislike button, so now I can dislike all of your dumb posts lol!!" or "Get the official DISLIKE button NOW!", this included a link to the rogue Facebook application. Once installed, the application gave scammers access to the users public information and to post to their wall. It automatically posted a status update forwarding the scam to the users Facebook friends (Richmond, 2010). The Sophos Security Threat Report (2011) states that this is a growing threat on SNSs and that on some days in 2010, cybercrooks introduced dozens of these new scams. It is estimated that at least half a million Facebook users fell for the "*see who viewed my profile*" application scam (Cosoi, 2011), this scam told users to follow a link and install a Facebook application that would allow them see who had been viewing their Facebook profile, instead users were scammed into visiting spam survey websites, signing up for expensive SMS or online services or parting with their personal information.

3.5.4 Excessive Use of SNSs

As discussed in Section 3.3.4, there is a continuing debate about whether excessive use of the Internet can be defined as an addiction in clinical terms. Regardless of the outcome of this debate there is a recognition that excessive use of the Internet is worth investigating. Researchers have begun to investigate the excessive use of SNSs and the effects of more frequent SNS use on other daily activities. Research is this area is limited and has primarily concentrated on the effects of excessive SNS use on academic performance.

Previous research has shown that low self esteem is correlated with Internet addiction (Armstrong *et al.*, 2000, Niemz *et al.*, 2005, Yang and Tung, 2007), see Section 3.3.4. Wilson *et al.* (2010) examined whether the role of personality and self-esteem predict emerging adults (n= 201, 17-24 year olds) addictive tendencies towards the use of SNSs. Their findings indicated that personality and self-esteem explained only a small amount of variance in both SNS use and addictive tendencies. Extraversion emerged as a positive predictor and conscientiousness as a negative predictor of both time spent using SNSs and SNS addictive tendencies. The authors argue that extroverts are drawn to the social interaction effects of SNSs. This finding lends further support for the "*rich get richer*" hypothesis as discussed in Section 3.3.1. Some studies have used extensions of the theory of planned behaviour (Ajzen, 1991) to predict users intentions to engage in high levels of

SNS use (Pelling and White, 2009, Baker and White, 2010). These studies found support for the subjective norm, indicating that users were more likely to be intensive users of SNSs if they perceived the behaviour to be normative among their peers. Pelling and White (2009) also found that attitude was a significant predictor of high levels of SNS use, indicating that the more a person identifies with being a SNS user, the greater the person's intention to engage in high-level SNS use.

Studies have examined whether there is a relationship between different levels of SNS use and other aspects of users daily life, in particular academic performance (Kolek and Saunders, 2008, Karpinski and Duberstein, 2009, Pasek *et al.*, 2009, Hargittai and Hsieh, 2010, Kirschner and Karpinski, 2010). Some have found evidence that intensive SNS users grades are lower and they spend fewer hours studying per week (Karpinski and Duberstein, 2009, Kirschner and Karpinski, 2010), conversely other studies have found no effect on academic grades (Kolek and Saunders, 2008, Pasek *et al.*, 2009, Hargittai and Hsieh, 2010). This is an area that requires further research and clearly causality is a question here.

Although not addressing SNS use specifically, the recent Irish EU Kids Online study (O'Neill *et al.*, 2011) examined whether excessive Internet use displaced children's social or personal needs. They found that 45% of respondents felt that they have spent less time than they should with friends, family or doing schoolwork because of the time they spent online and 46% of respondents had tried unsuccessfully to spend less time online.

3.5.5 Reputational Risks

As discussed in Section 3.3.1, Valkenburg *et al.* (2006) assert that social self esteem is more likely to be affected if the Internet is used for communication. In their study of adolescent SNS users (n=881, 10-19 year olds), they found that positive feedback on profiles enhanced adolescents' social self esteem, whereas negative feedback decreased self esteem. Combined with the fact that most SNS users aim to present a socially appropriate representation of themselves (boyd, 2004, Manago *et al.*, 2008, Zhao *et al.*, 2008), it is not surprising that SNS users can experience personal reputational damage from negative postings and embarrassing photos that have been placed online.

As discussed in Section 3.4.2, concern has been expressed about how much information SNS users reveal online and the fact that many users seem unaware of the potential audience for this information. This can also lead to some reputational risks for the user, but also can cause difficulties for their school/college/employer. One such concern relates to the types of images university students post on SNSs. The fact that employers now use SNS sites to screen potential employees adds to the concern. Watson *et al.* (2006) conducted a content analysis of 150 central photographs on Facebook profiles and found that alcohol was included in approximately 9% of the central photos, but a very small proportion of photos were sexually suggestive or contained partial nudity. The study can be criticised on the base of small sample sizes and that only central photographs were examined. A more detailed study carried out by Kolek and Saunders (2008), found contradictory results. Although alcohol was only represented in 7.2% of central photos, over half the profiles examined contained at least one picture of someone consuming an alcoholic drink. They found that nearly 9% of profiles had references to drugs. A study by Moreno *et al.* (2009) carried out a content analysis of publicly available MySpace profiles (n = 500, 18 year olds) to ascertain the prevalence of health risk behaviours. They found that over half of the profiles (54%) contained risk behaviour information, 24% referenced sexual behaviours, 41% referenced substance abuse and 14% referenced violence. In a study of undergraduate students, Peluchette and Karl (2008) found that 20% of the respondents indicated that there were items on their social network profile that they would not want current or prospective employers to see.

Reputational damage can also be caused to schools, colleges, universities and workplaces by comments made by students/employees. SNS postings can also violate rules and codes of conduct in institutions. These comments and violations cause problems for the institution but can lead to expulsion and job losses. Many examples have been cited in the popular press including:

- Virgin Atlantic took disciplinary action against 13 crew members who participated in a Facebook discussion that trashed the airline's safety standards and insulted passengers. All 13 crew members were sacked as their behaviour was considered to be inappropriate and had brought the company into disrepute (Conway, 2008).
- An experienced CNN editor, Octavia Nasr, was sacked for a tweet saying she "*respected*" a late Lebanese cleric, who was believed to have inspired Shia Muslim militant group and political party Hezbollah (Walker, 2010). Following the tweet,

Nasr (2010) explained in a CNN blog: "*Reaction to my tweet was immediate, overwhelming and provides a good lesson on why 140 characters should not be used to comment on controversial or sensitive issues, especially those dealing with the Middle East*"

- In February of 2010, Vodafone had to apologise profusely and suspend a member of its staff after the individual had hijacked the UK's official Vodafone Twitter feed and posted an obscene tweet (Wray and Arthur, 2010). Even though Vodafone removed the offending message as soon as it could, the tweet got retweeted numerous times, showing that deleted tweets don't necessarily disappear.

As far as it is known, no studies have examined the prevalence or the level of concern associated with this risk on SNSs.

3.5.6 Other Risks

This section discusses briefly some of the other risks that can be present on SNSs.

Hate Groups

Hate sites or "*cyberhate*" sites advocate hate towards groups on the basis of race, religion, ethnicity, gender and sexual orientation (Douglas, 2007). The Internet and SNSs allow hate groups to disseminate their message to a large audience at a low cost (Beckles, 1997, Perry, 2000, Leets, 2001) and in relative anonymity (Douglas, 2007). Researchers have studied these sites from a legal and political perspective to examine how these sites can be policed and regulated (Siegel, 1998, Leets, 2001, Levin, 2002, Timofeeva, 2002). Others have conducted content analysis of the hate rhetoric on these sites in order to examine the nature and purpose of these sites (Apple and Messner, 2001, Lee and Leets, 2002, Gerstenfeld *et al.*, 2003, Bostdorff, 2004, Douglas *et al.*, 2005). Research indicates that the main objective of these groups is to link, educate and recruit. Many of these sites provide content and games that are aimed specifically at children (Perry, 2000, Blazak, 2001, Back, 2002, Turpin-Petrosino, 2002, Tynes, 2005). These groups tend not to use insults or incite violence but state their views in a neutral manner in order to appear rational and balanced (McDonald, 1999, Douglas *et al.*, 2005). Few studies have examined the levels of exposure to these sites. The Irish EU Kids Online study (O'Neill *et al.*, 2011) examined whether children had encountered hate sites on the Internet. 16% of all children had encountered hate sites in the last year, this percentage rose to 20% for older boys and 32%

for older girls (age 14-16 year olds). This indicates that a sizeable proportion of children have had exposure to these sites but the effects of this exposure as yet have not been examined.

SNSs are now being used as a medium for these hate sites. A report from the Simon Wiesenthal Center (2009) indicates that hate sites on SNSs is an increasing problem. They examined over 10,000 problematic web sites, social networking groups, portals, blogs, chat rooms, videos and hate games on the Internet which promote racial violence, anti-semitism, homophobia, hate music and terrorism. They found a 25% increase compared to the previous year in problematic social networking groups on the Internet. To date this is an area that has attracted little research.

Self-harm Sites (suicide, anorexia etc.)

Research into self-harm sites on the Internet is increasing. These sites primarily provide information about suicide, self-injury and psychological issues (Prasad and Owens, 2001). Some argue that there is a positive side to sites of this nature as they allow individuals to get emotional support (Rochlen *et al.*, 2004, Barak, 2007) with some members reducing the frequency and severity of their self-harming behaviour as a consequence of group membership (Murray and Fox, 2006, Baker and Fortune, 2008). However many research studies have not found such positive benefit to these sites. Prasad and Owens (2001) found that these sites rarely offered e-mail support and online discussions.

With regard to online anorexia sites, Chesley *et al.* (2003) found three different types of web sites associated with anorexia: pro-anorexia ("*pro-Ana*" and "*pro-Mia*"), pro-recovery and professional organizations. The pro-anorexia sites were the most prevalent. Concern has been expressed about these sites, as they promote anorexia and related disorders as a lifestyle choice rather than a medical disorder. Some researchers have found that these sites have a positive effect as they allow participants a safe and positive place to gain further insight into their condition away from the judgement and scrutiny of their parents, friends and the medical community (Fox *et al.*, 2005, Lyons *et al.*, 2006, Mulveen and Hepworth, 2006, Csipke and Horne, 2007). Other researchers suggest that the negative effects surpass any positive effects and that these sites promote and support anorexia nervosa (Norris *et al.*, 2006, Wilson *et al.*, 2006, Tierney, 2008, Borzekowski *et al.*, 2010, Haas *et al.*, 2011, Rouleau and von Ranson, 2011). Research indicates that adolescents who are exposed to these pro eating disorder sites have higher levels of body

dissatisfaction and there are indications that these sites could lengthen the durations of eating disorders (Bardone-Cone and Cass, 2007, Harper *et al.*, 2008). The Irish EU Kids Online study (O'Neill *et al.*, 2011) found that over one fifth of older girls (age 14-16 year olds) had visited these sites on the Internet. Juarascio *et al*. (2010) investigated the prevalence and content of pro-eating disorder sites on Facebook and MySpace and found hundreds of groups on both sites. However, they found that the emphasis of these groups was more towards providing social support. Although this study indicates that pro-anorexia groups on SNSs may take a positive approach, this is one of the first studies carried out on SNSs and further research is needed to confirm these findings.

Cases of cybersuicide (attempted or completed suicide influenced by the Internet) have been published in the popular and academic press (Thompson, 1999, Beatson *et al.*, 2000, Rajagopal, 2004). There are examples of Internet suicide pacts among strangers who have met and then planned their suicide through the Internet. Concerns have been raised that passive individuals may be more likely to take their own lives due to group conformity effects (Rajagopal, 2004, Lee *et al.*, 2005). There is also a belief that the availability of information on effective methods of suicide can lead to an increase in completed suicides (Thompson, 1999, Becker and Schmidt, 2004, Alao *et al.*, 2006, Biddle *et al.*, 2008). While clearly these sites attract people that are already suicidal research indicates that media reporting of suicide can have an effect on adolescent suicide rates (Gould *et al.*, 2003). It is possible to regulate professional media outlets but it is not possible to regulate the Internet in this way (Becker and Schmidt, 2004). Due to the difficulties in researching suicide much of the research is based on anecdotal evidence rather than controlled empirical studies (Bell, 2007).

Biased/Misinformation

Web sites and SNSs can provide untrustworthy information. Much of the research in this area has concentrated on health information as the consequences of incorrect information in this area are serious. Research indicates that people tend to use some form of critical evaluation when evaluating online health information. Sites are perceived to be of a higher quality if they are endorsed by a government or professional body, if they are easy to understand and the presentation quality is high (Eysenbach and Köhler, 2002, Schwartz *et al.*, 2006). Research has shown that children in particular have difficulty in deciding whether information presented on the Internet is accurate or trustworthy (Livingstone *et al.*, 2005). In a study investigating whether adolescents could assess the accuracy of

Internet-based material, Kortnum *et al.* (2008) found that adolescents had a difficult time distinguishing trustworthy medical sites from untrustworthy ones. Research studies indicate that few people use SNSs to gather and share health information (Fox and Sydnes, 2009).

Terrorism

The term "*cyberterrorism*" was first coined by Barry Collin (1997). Pollitt (1998, p9) defines cyberterrorism as "*the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by subnational groups or clandestine agents".* However, to date, there have been few, if any, computer network attacks that meet this criteria for cyberterrorism (Denning, 2001). This does not mean, however, that the Internet and SNSs are not being used as a medium for terrorists. Terrorist groups are using the Internet to spread their message and to communicate and coordinate action. Many aspects of the Internet, including its anonymity, the lack of regulation, the ability to keep communications confidential by using encryption and the ease at which to reach a vast audience quickly make the Internet attractive for terrorists to promote their ideas (Weimann, 2005, Goodman *et al.*, 2007).

The core ways in which terrorists can use the Internet can be summarised as (Furnell and Warren, 1999, Thomas, 2003b, Weimann, 2005, Conway, 2006, Weimann, 2006):

1. Psychological effects: terrorists can use cyberspace to disseminate propaganda, display violent images, make threats and generate "*cyberfear*". Cyberfear is a sense of fear that arises when considering the effects of cyber terrorism.
2. Information provision: the Internet also provides an expanded forum for disseminating terrorist propaganda. Terrorist organisation can share pertinent information such as how to build chemical and explosive weapons.
3. Information gathering: terrorists can learn from the Internet a wide variety of details about potential targets such as transportation facilities, power plants, public buildings etc.
4. Financing: terrorist groups can use the Internet to raise funds, for example SNS profiles allow terrorists to identify users with sympathy for a particular cause or issue.

5. Recruitment: the Internet can be used to recruit and mobilize supporters to play a more active role in terrorist activities.
6. Networking: many terrorist groups are designed around semi-independent cells with no single commanding hierarchy. Through the use of the Internet, these groups are able to maintain contact with each other. Terrorists can also use the Internet to plan and co-ordinate specific attacks.

Some researchers have examined how terrorist cells can be identified in social networks (Dorogovtsev and Mendes, 2002, Krebs, 2002, Barabási, 2003). The use of the Internet as an enabling technology has also been examined (Furnell and Warren, 1999, Thomas, 2003b, Weimann, 2005, Conway, 2006, Weimann, 2006, Goodman *et al.*, 2007), but to date few researchers have explicitly addressed how SNSs can enable terrorist activities and the risks inherent in this. It is clear that SNSs can provide an environment that could be of use to terrorists.

3.5.7 Harm from Risk

Although there are many reports and academic studies investigating the prevalence of individual risks associated with SNSs, few studies have examined which risks are potentially more serious and harmful than others. The Eurobarometer qualitative study in 29 EU countries (EUROBAROMETER, 2007b) asked children to rank the risks associated with the Internet and mobile phones and highlight the most worrying risks and problems. This study did not look at SNSs in particular. The findings were uniform across all the member states. The children ranked the risks attached to the Internet as:

1. Possibility of contact with adult strangers;
    a. Taking part in open chats/discussion forums;
    b. Reading and replying to blogs/websites of someone you have never met;
    c. Using instant messaging/chats with friends (ill-intentioned adults may intrude);
2. Risks that could affect the computer or cause the user problems;
    a. Downloading music, films, videos etc. (viruses and illegal downloads);
    b. Exchanging files (viruses and illegal downloads);
    c. Downloading screen backgrounds, playing games on-line (unexpected costs, frauds, viruses).

The EU Kids Online survey also addressed the harm associated with various online risks. They assessed harm by asking children if they had been bothered by the risks, they defined bothered as something that "*made you feel uncomfortable, upset or feel that you shouldn't have seen it*" (Livingstone *et al.*, 2011a, p6). They found that experiencing a risk does not necessarily result in harm. They found that being bullied online, the least common risk, is the risk most likely to upset children. Other risks such as seeing sexual or pornographic content and receiving sexual messages, although more commonly experienced, were seen by the majority of cases to cause little or no harm. Most of the respondents that had met online contacts offline had not experienced any harm from the meetings.

Some studies have found that children did not show any anxiety about the risks of Internet and SNS usage and tended to reveal a degree of sang-froid (Brennan and CEOP, 2006, EUROBAROMETER, 2007b). Studies have also found evidence of optimistic bias (Brennan and CEOP, 2006, Livingstone *et al.*, 2011a), where users of SNSs reported that it was others at risk of victimisation, such as the weak and vulnerable and in particular younger inexperienced users. Studies indicate that most children felt that they were sufficiently in control of their online environment and were able to manage any risky situations themselves (Brennan and CEOP, 2006, EUROBAROMETER, 2007b, Livingstone *et al.*, 2011a).

3.5.8 Discussion

It is clear that there are a considerable number of risks that can be encountered on SNSs. The risks in using SNSs are increasingly covered in the media, in particular how the use of SNSs by children increases their likelihood of encountering risks such as paedophile contact, stalking, bullying etc. (Van Duyn, 2006, Palmer, 2008). Invoking fears about children in this way is a powerful way of commanding public attention and support (boyd, 2007) and thus parents, governments and schools etc. have to be seen to be doing something to reduce these risks. This has meant that much of the research to date has focussed on the risks to children and has concentrated on the threatening risks. However, the negative events that can be encountered on SNSs can pose a risk for all users and to date studies have not addressed the extent to which these risks can pose a threat for adults. Some risks associated with SNSs can cause reputational damage and can pose a danger for business organisations, schools and colleges. Although recent surveys indicate that businesses are concerned about the risks posed by social media (Ernst&Young, 2010,

Sophos, 2011), it would appear that the majority of businesses have not assessed the impact of social networking (Ernst&Young, 2010).

Much of the research of online risk has been successful in analysing the types and prevalence of online risk, but has been less successful in researching the relation between risk and harm (Staksrud and Livingstone, 2008). Studies examining the consequences of online risks are limited. To date the risk agenda has been set by adult society and researchers (Livingstone and Haddon, 2008) and this does not necessarily address risks that are of concern to users of SNSs. This has led to a focus on the more threatening risks such as cyberbullying, encountering pornography, paedophiles, stranger contact etc. and has meant that there is less available research on commercial risks, personal information risks, reputational risks or the impact of excessive use of SNSs. Few studies have addressed the broad range of risks that can be encountered on SNSs.

A further consideration is the other risk factors associated with SNS use. As stated by Hasebrink *et al.* (2008), children's access to and use of SNSs occurs in a broader social context and there are many factors that can influence children's exposure to risk. Many academic studies of online risk have concentrated on a limited number of risk factors, the most prominent being age (comparing younger and older children) and gender. As part of the EU Kids Online project, Hasebrink *et al.* (2008) developed an initial framework to organise the array of factors that could influence the online risks and opportunities children encounter. The framework was developed as a working hypothesis, as the authors recognised that other factors may arise as the research progressed. This framework was developed for all online risks and opportunities and was not specific to SNSs. The initial framework is depicted in Figure 3.4. The framework proposes that the experience of online risk is expected to vary according to children's age, gender as well as the socio-economic status (SES) of the household (or other stratifying factors such as parental education or urban/rural location). These factors are the main independent variables. These independent variables can influence children's Internet access, online usage and the related attitudes and skills. These are considered mediating variables as they are influenced by the independent variables and may in turn influence online risks and opportunities. Additional mediating variables are introduced by the activities of others: parents, teachers and peers. There are contextual variables that can affect children's online experiences. These include: the media environment; ICT regulation; the public discourse

on children's Internet use and possible risks of the Internet; general values and attitudes regarding education, childhood and technology and the educational system.

Further in to the project the framework was further refined as shown in Figure 3.5. The core element of the model has been changed to reflect a path from Internet use (amount, device and location of use) through online activities (opportunities taken up, skills developed and risky practices) to the risk encountered, termed Risk factors in the framework. The final core element examines how the respondents cope with these experiences. The model has been expanded to examine psychological factors such as emotional problems, self-efficacy and risk-taking behaviour.

The framework provides a valuable model for examining online risks as they pertain to children, in particular because it recognises that risk is a multidimensional concept that is influenced by social, cultural and psychological factors.

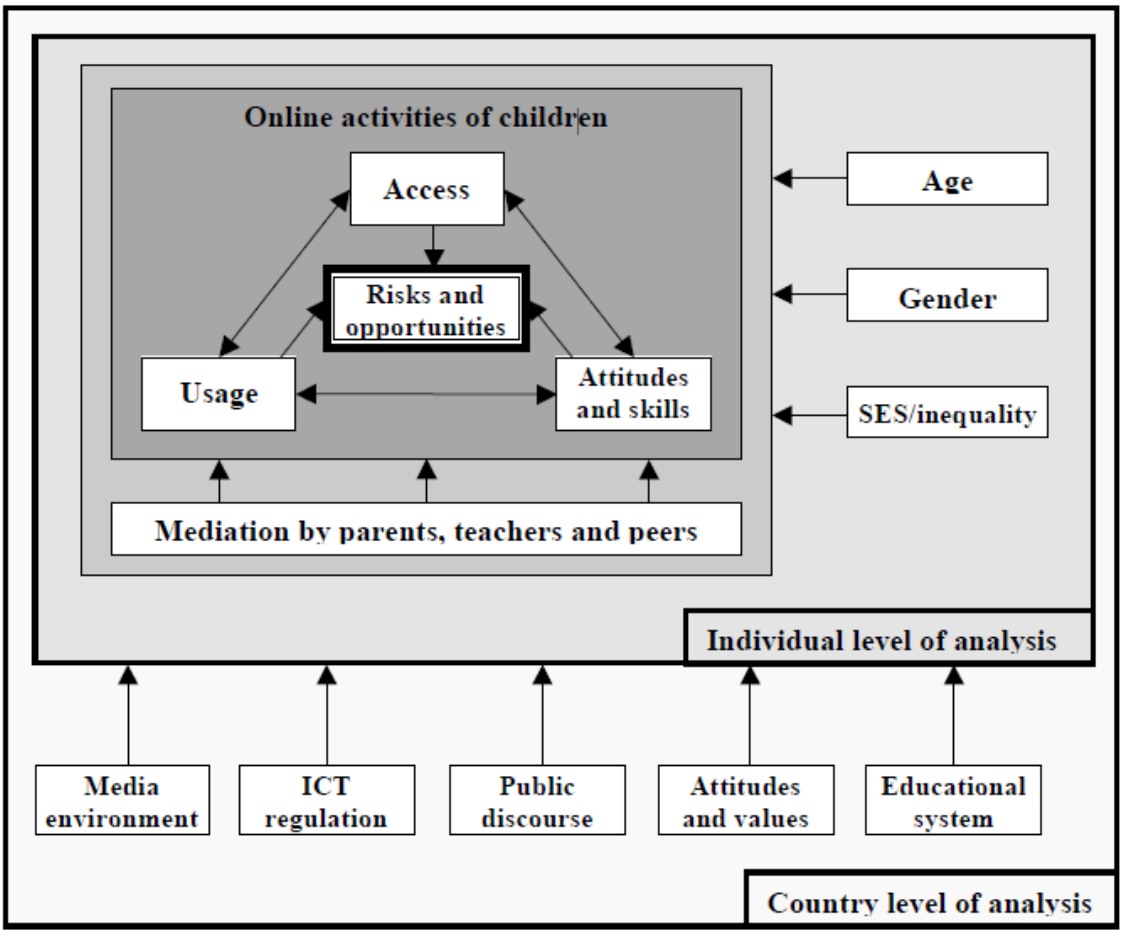


Figure 3.4 Factors Influencing Children's Exposure to Online Risks and Opportunities.
Source: (Hasebrink *et al.*, 2008, p7)

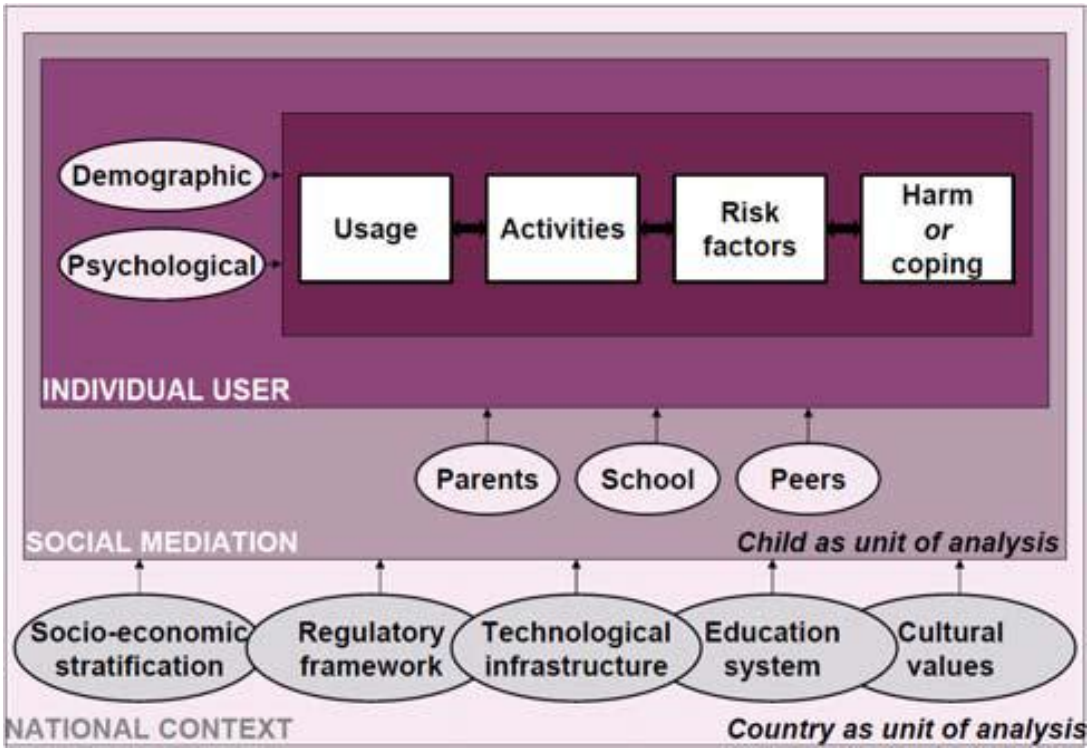


Figure 3.5 Relating online use, activities and risk factors to harm to children. Source: (Livingstone *et al.*, 2011a, p15)

3.6 Summary of SNS Literature Review

Although SNSs are a recent development, they have quickly become a popular environment for individuals to maintain an online social network of friends. Research indicates that the primary use of SNSs is to communicate and maintain relationships with existing friends rather than meeting strangers (Acquisti and Gross, 2006, boyd, 2007, Ellison *et al.*, 2007, Lenhart and Madden, 2007, Anchor, 2008a, OFCOM, 2008, Young and Quan-Haase, 2009, Livingstone *et al.*, 2010b, O'Neill *et al.*, 2011). SNSs offer many benefits to users, but there are also many risks in using these sites.

This literature review has highlighted a number of characteristics about the Internet and SNSs that can make them risky environments for users:

1. Anonymity: users on the Internet can be effectively anonymous and can thus hide their identity or assume false identities (Joinson, 2001, Thurlow *et al.*, 2004);
2. Disinhibition: users can be less inhibited and can thus act out in ways that they wouldn't in FtF communications (Suler, 2004);
3. There is a lack of physical and social cues and this can lead in some cases to uninhibited and aggressive behaviour (Sproull and Kiesler, 1986);

4. Communications on SNSs are persistent, searchable and easily replicated (boyd, 2007);
5. It is virtually impossible to ascertain the audience for an online communication and it could potentially consist of all people across all space and time (boyd, 2007);
6. SNSs give access to a large numbers of users where messages can be shared very quickly from one friend to another;
7. Privacy controls on SNSs are generally not intuitive to use (Bonneau and Preibusch, 2010, Brandtzæg *et al.*, 2010);
8. The default settings on SNSs tend not to be restrictive (McKeon, 2010);
9. Users reveal substantial amounts of personal information on SNSs (Gross and Acquisti, 2005, Jones and Soltren, 2005, Acquisti and Gross, 2006, Stutzman, 2006, Anchor, 2008b, Hinduja and Patchin, 2008b, Kolek and Saunders, 2008, Tufekci, 2008, Christofides *et al.*, 2009, Fogel and Nehmad, 2009, WEBWISE, 2009, Young and Quan-Haase, 2009, Nosko *et al.*, 2010);
10. The information revealed on SNSs can be aggregated over time and can be easily combined with other data sources to build up profiles of users (Conti and Sobiesk, 2007);
11. It is easy for others to gain access to personal information on SNSs (Jump, 2005, Chau *et al.*, 2007, Jagatic *et al.*, 2007, Mislove *et al.*, 2007b, Preibusch *et al.*, 2007, Krishnamurthy and Wills, 2008, Bonneau *et al.*, 2009, Balduzzi *et al.*, 2010, Datcu, 2010).

This is further exacerbated by the difficulties in regulating the Internet and the lack of monitoring and censorship on the Internet.

Although research in SNSs is at an embryonic stage, a number of research strands are emerging. The most prominent research streams relate to the effect of SNSs and online communications on well-being; the privacy implications of SNSs and the risks associated with SNSs. With regard to well-being, as the majority of SNS users report using these sites to stay in touch with existing friends (Acquisti and Gross, 2006, boyd, 2007, Ellison *et al.*, 2007, Lenhart and Madden, 2007, Anchor, 2008a, OFCOM, 2008, Young and Quan-Haase, 2009, Livingstone *et al.*, 2010b, O'Neill *et al.*, 2011), there is strong support for the stimulation hypothesis, i.e. online technologies encourage communication with existing friends. However it is not clear if the effects of SNSs on well-being are positive for all Internet users. Some studies suggest that the effects of SNSs on well-being are positive but only for introverts or socially anxious individuals (Ellison *et al.*, 2007, Stamoulis and

Farley, 2010), others suggest SNS use primarily benefits extroverted users (Sheldon, 2008, Ross *et al.*, 2009, Correa *et al.*, 2010), some found support for both groups (Zywica and Danowski, 2008, Desjarlais and Willoughby, 2010) and some found no support for either group (Tufekci, 2010). Researchers that examined whether personality traits are associated with different types of SNS activity (Ross *et al.*, 2009, Amichai-Hamburger and Vinitzky, 2010) and the effect of Internet use on self-esteem (Lenhart and Madden, 2007, Steinfield *et al.*, 2008, Baker and White, 2010) have also found no conclusive results. Overall there is little consensus with regard to the effect of SNS use on well-being, as suggested by Tufekci (2010) this could be due to the fact that these studies unrealistically assume that all people will be similarly affected by SNS use.

The privacy aspects of SNSs have attracted a considerable amount of research interest. Researchers have examined how users are implementing privacy controls on SNSs, the level of information revealed and user's attitudes to privacy on SNSs. SNSs are in the business of getting users to share as much information as possible and thus do not promote the privacy controls (Bonneau and Preibusch, 2010, Schneier, 2010, Furnell and Botha, 2011). This creates a number of difficulties for users. A privacy paradox is evident on the Internet and SNSs in that although users express high levels of privacy concern, this does not always translate into behaviour online (Syverson, 2003, Acquisti, 2004, Acquisti and Grossklags, 2005, Acquisti and Gross, 2006, Norberg *et al.*, 2007, Tufekci, 2008, Debatin *et al.*, 2009, Fogel and Nehmad, 2009, Young and Quan-Haase, 2009). Although users are now more likely to restrict their privacy settings on SNSs there appears be a disconnect between their expressions of privacy concern and the amount of personal information they reveal. Few studies have empirically tested why users disclose information on SNSs (De Souza and Dick, 2009, Utz and Krämer, 2009, Raynes-Goldie, 2010), further research is needed to explore this disconnect. Users also show a lack of awareness of the audience on SNSs and assume that the audience on SNSs is their peer group (Lampe *et al.*, 2006, Lampe *et al.*, 2007, Lampe *et al.*, 2008, Livingstone, 2008, Phippen *et al.*, 2009, Pike *et al.*, 2009, West *et al.*, 2009).

There is quite a number of risks associated with the use of SNSs. There is a difficulty in producing a definitive list of risks associated with SNSs as this is a rapidly evolving environment, the features provided by the SNSs are continuously updated and the way in which users interact with SNSs is also changing. This means that new risks are still

emerging. For the purposes of this research, the risks that can be encountered on SNSs are categorised as:

1. Threatening Risks (risks that can potentially cause serious physical or mental harm for individuals, e.g. cyberbullying, meeting online contacts offline);
2. Personal Information Risks (risks due to personal information revealed on SNSs, e.g. commercial risks, identity theft);
3. Technology Risks (risks associated with technology, e.g. viruses and malware, spam);
4. Excessive use of SNSs (risks associated with spending too much time on SNSs, e.g. addictive tendencies, displacement of time spent with friends/family or studying);
5. Reputational Risks (risks to personal reputation or organisations reputation, e.g. embarrassing information and photos on SNSs);
6. Other risks (this includes hate groups, self-harm sites, biased/misinformation etc.).

To date, the risk research agenda has been set by adult society (Livingstone and Haddon, 2008) and this has resulted in much of the research being focussed on the risks to children and on the threatening risks. However, the negative events that can be encountered on SNSs can pose a risk for all users, to date studies have not addressed the extent to which these risks can pose a threat for adults. There is limited research available on the commercial risks, personal information risks, reputational risks or the impact of excessive use of SNSs. Few studies have addressed the broad range of risks that can be encountered on SNSs. A further criticism is that few studies have researched the relationship between risk and harm (Staksrud and Livingstone, 2008).

Although trust has been recognised as an important factor in e-commerce systems and is an important component of FtF communication, there has been a limited amount of research examining the trust construct on SNSs (Dwyer *et al.*, 2007, Christofides *et al.*, 2009, Fogel and Nehmad, 2009, Utz and Krämer, 2009). A number of factors can influence the online risks that users of SNSs can encounter. Apart from the EU Kids Online Project that have developed a framework that recognises risk is a multidimensional concept, most studies have just examined age and gender effects. Studies that have examined age effects have primarily examined differences between older and younger adolescents.

The limitations highlighted in these literature reviews have informed the research questions posed by this research.

3.7 Background to Research Questions

As stated in Section 1.2, the aim of this research is to examine adolescents', emerging adults' and adults' risk perception of a wide range of potential risks on SNSs. As there was no existing validated measurement tool available to assess risk perceptions on SNSs, a framework had to be developed identifying the factors that can contribute to risk perception. The following section provides some background about the risk factors that are examined in this study before describing the research questions posed by this research.

The two most influential areas of risk perception research have been the psychometric paradigm and Cultural Theory. Both of these paradigms have strengths and weaknesses. Recent risk perception research has attempted to bridge the paradigmatic gap and this has led leading exponents of the psychometric approach to begin to take into account how other factors influence risk perception. These include: biological; psychological; social; political and cultural factors such as age, gender, race, emotions, control, and trust. To further this aim, this research examines risk characteristics highlighted by the psychometric paradigm but also examines biological, psychological and social factors that have been shown to influence risk perception. Other contextual variables such as Internet experience, intensity of SNS use and amount of information revealed are also considered. This section discusses the choice of negative events and risk characteristics examined in this study, followed by a discussion of the further risk factors and contextual variables that have been considered in the research.

Negative Events

A criticism of adolescent risk perception studies and studies of online risk is that most studies have examined a limited number of risks which have usually been determined by the researcher or adult society (Moore and Gullone, 1996, Millstein and Halpern-Felsher, 2002a, Livingstone and Haddon, 2008). For SNS research, this has meant that research has tended to focus on the more threatening risks such as cyberbullying, encountering pornography, paedophiles, stranger contact etc. and there is little available research on other risk areas.

To address this limitation and allow current users to highlight areas of concern to them, the choice of which negative events on SNSs to examine is based on a review of the literature but also on three focus group interviews with emerging adults; see Section 4.3.4 for a more

detailed discussion. Keeping in mind the concerns of current users, twelve negative events were selected according to several criteria including prevalence, seriousness and in order to represent a wide ranging set of negative events. The twelve negative events examined in this study are:

- Threatening Risks:
    1. Being bullied or harassed;
    2. Being stalked;
    3. Meeting in person a stranger that was initially met online;
    4. Accidentally stumbling across disturbing content.
- Personal Information Risks:
    5. Personal information being misused by strangers;
    6. Personal information being sold to advertisers.
- Technology Risks:
    7. Spam;
    8. Viruses.
- Excessive use of SNSs:
    9. Spending too much time on SNSs;
    10. Replacing the need for meeting up with existing friends.
- Reputational Risks:
    11. Being Hurt by Information Posted;
    12. Embarrassing Information or Photos Seen by Others.

Risk Characteristics

The earliest studies using the psychometric paradigm identified nine risk characteristics that were thought to be important for the way people perceive risk (Fischhoff *et al.*, 1979, Slovic *et al.*, 1979, 1980). Over time this list of risk characteristics has extended. As can be seen in Appendix D, a review of previous studies of risk perception using the psychometric paradigm (with an emphasis on ICT studies and adolescent studies) identifies over 45 different risk characteristics. The risk characteristics examined in this study are chosen based on their relevance to the field of study and their frequency of use in previous studies. Many of the risk characteristics identified by previous research are not of direct relevance to the type of negative events that can be encountered on SNSs, for example the psychometric paradigm identifies two main risk factors dread and unknown. The latter being more relevant for IS/ICT risks. To minimise the amount of time taken to complete

the survey, it is necessary to minimise the number of risk characteristics examined. Thus six risk characteristics are examined in this study: personal risk, awareness/knowledge of risk, severity of risk, controllability of risk, likelihood of risk and risk to others. According to the "*risk as feelings*" hypothesis, risk perception can be dependent on intuitive and experiential thinking, guided often by emotional and affective processes (Finucane *et al.*, 1999, Slovic, 2000b, Lowenstein *et al.*, 2001). There is evidence that affect is also relevant for adolescents (Arnett *et al.*, 1997, Hussong *et al.*, 2001, Pardini *et al.*, 2004, Sigfusdottir *et al.*, 2004, Curry and Youngblade, 2006), so a further risk characteristic based on emotion is examined: concern about risk.

Age

As the predominant users of SNSs were until recently younger people in the 14-24 year age group, research to date has mostly been carried out on these age groups. Studies have examined single age groups such as children/adolescents or emerging adults, and have made comparisons within these homogenous groups. A particular emphasis has been placed on how younger adolescents and older adolescents differ with regard to online risk. As far as it is known, no studies have examined the risks on SNSs across a number of age groups. However, risk perception studies have examined age effects and in particular how adolescent risk perception differs to that of adults. This research indicates that risk perception decreases with age (Gullone and Moore, 2000, Gullone *et al.*, 2000, Millstein and Halpern-Felsher, 2002a). Some caution has to be exercised in generalising these findings, as some studies have used young adults or parents as representative of adults in general. This study provides an understanding of how SNS risks are perceived by each age group and whether the risk landscape changes across age groups. As suggested by previous risk perception research, it is expected that the risk perception of negative events on SNSs will decrease with age. As emerging adults and adults have developed better coping skills and life skills, it is conjectured that emerging adults and adults would be less concerned about the threatening risks on SNSs such as cyberbullying or meeting a stranger. However, it is expected that they would be more concerned about other risks, such as the risks to their personal information.

Gender

Research studies have found no gender differences in SNS participation rates, but gender differences have been found in the use of SNSs. Studies have found that females are more likely to use SNSs to communicate with their peers and males are more likely to use SNSs

to promote themselves and make new friends (EUROBAROMETER, 2007a, Lenhart and Madden, 2007, Barker, 2009). , Studies have found that males are more likely than females to provide direct contact information (Gross and Acquisti, 2005, Tufekci, 2008, Fogel and Nehmad, 2009), possibly signalling their interest in making new friends. With regard to experience of negative events on SNSs, the findings with respect to gender are sometimes contradictory, for example some studies have shown that females are more likely to be the victims of cyberbullying (Smith *et al.*, 2006, Li, 2007b, Dehue *et al.*, 2008, O'Moore and Minton, 2010), some that males are more likely to be the victims (Erdur-Baker, 2010) and others have found no gender differences (Li, 2006, 2007a, Livingstone *et al.*, 2011a).

A number of studies (of both adults and adolescents) have shown that men tend to be less risk adverse than women and it is a common finding that males perceive less risk than females (Slovic, 1997). It seems unlikely that males will be greater risk takers in all areas and indeed studies indicate that this is not the case (Byrnes, 2003) and the context of the negative event is important. As previous research suggests that young females tend to more upset by the risks they experience on SNSs (Livingstone *et al.*, 2011a) it is expected that risk perceptions will be higher for females as compared to males.

Prior Experience

As suggested by Eiser (2004) perceptions of risk are based on, and learnt from, experience, so clearly prior experience of a negative event should be an important determinant of risk perception. However, to date few studies have examined the relationship between experience of a risk and general risk perceptions and these studies provide few coherent conclusions (Breakwell, 2007). Prior experience is not relevant or even measurable for studies that examine extreme hazards such as a fatal airplane crash etc., but for those studies that have examined ICT/IS risks, it is both possible and important to examine the impact of prior experience. An examination of risk perception studies in the IS/ICT area shows that in the studies where prior experience has been measured (Sjöberg and Fromm, 2001, Campbell *et al.*, 2007) no conclusions have been reached with regard to the relationship of prior experience and risk perception. Other studies examining IS/ICT risks (Coles and Hodgkinson, 2008, Gabriel and Nyshadham, 2008) have not even measured prior experience. It is expected that prior experience will be a significant predictor of the likelihood of personal risk.

Internet Experience

Previous research examining IS/ICT risk suggests, although it has not been empirically tested, that those with high Internet skill levels can be overconfident, feel in control of the technology and this can prevent them from seeing the risks involved with technology (Collins and Mansell, 2004, Jackson *et al.*, 2004a). It is expected to see a similar pattern with regard to SNS risks.

Disposition to Trust

From the risk perception literature, no consensus has emerged regarding the relationship between trust and risk perception. There are two opposing schools of thought: the first contends that trust is an important determinant of perceived risk (Flynn *et al.*, 1992) whereas others believe trust has little effect (Sjöberg, 2000, 2001). In these studies, trust in specific objects or entities (social trust) is measured rather than trust as a personality trait. In contrast, a consistent finding in the online shopping literature is that trust reduces perceived risk and this is turn influences intentions to purchase online (Grazioli and Jarvenpaa, 2000, Jarvenpaa *et al.*, 2000, Pavlou, 2003). Online shopping studies have considered both social trust and trust as a personality trait. However, many of these studies have treated perceived risk as a one-dimensional construct and only one study has employed the psychometric paradigm (Gabriel and Nyshadham, 2008). With regard to SNSs, the literature on trust is patchy and has produced few coherent findings. Trust in SNSs is an area that has not yet been adequately addressed in the research literature. Trust is a complex phenomenon, it is difficult to define and even within the IS domain there are different conceptualisations of the construct (Grabner-Kräuter and Kaluscha, 2003, Connolly and Bannister, 2007). The trust constructs identified in the literature include both institutional phenomena (system trust) and personal and interpersonal forms of trust (dispositional trust, trusting beliefs, trusting intentions and trust-related behaviours) (Grabner-Kräuter and Kaluscha, 2003). As the main aim of this thesis is to explore risk perception on SNSs and not trust, a full examination of trust and its antecedents is beyond the scope of this thesis. However it is expected that trust plays an important role in communication on SNSs, especially as communication on SNSs tends to involve postings to large groups of friends (including strong and weak ties). A choice has been made to look at an interpersonal form of trust, dispositional trust. Disposition to trust is a general inclination to display faith and a general willingness based on extended socialization to depend on others (McKnight *et al.*, 1998). Previous research into trust in online shopping indicates that individuals with a higher propensity to trust place more trust in e-commerce

systems (Gefen, 2000, McKnight *et al.*, 2002) and they are less likely to see the potential for risk (Young Hoon, 2005, Harridge-March, 2006).

Online Privacy Concern

Numerous researchers in IS have examined privacy issues and in particular understanding what motivates Internet users to disclose or not disclose personal information (e.g. Culnan and Armstrong, 1999, Cranor *et al.*, 2000, Phelps *et al.*, 2000, Sheehan and Hoy, 2000, Miyazaki and Fernandez, 2001). Findings from a number of studies suggest that Internet users express a high level of concern about their online privacy (Cranor *et al.*, 2000, Phelps *et al.*, 2000, Han and Maclaurin, 2002, Earp and Baumer, 2003), but a paradox seems to exist between user's intentions and their actual behaviour (Spiekermann *et al.*, 2001, Syverson, 2003, Acquisti, 2004, Acquisti and Grossklags, 2005, Chellappa and Sin, 2005, Norberg *et al.*, 2007) in particular with regard to the information revealed on SNSs (Acquisti and Gross, 2006, Dwyer *et al.*, 2007, Livingstone, 2008, Tufekci, 2008, Debatin *et al.*, 2009, Fogel and Nehmad, 2009, Young and Quan-Haase, 2009). It is expected that those that express higher levels of online privacy concern would perceive themselves to be at higher risk especially for the personal information risks.

Other contextual variables

A number of contextual variables have been included to assess their effect on risk perception. These include Internet skill level, intensity of SNS use and quantity of personal information revealed. It is expected that intensive SNS users would see themselves as more likely to experience the excessive use risks on SNSs. It is expected that those that reveal more personal information on SNSs should perceive themselves to be at higher risk especially for the personal information risks.

3.8 Research Questions

Risk Perception

As stated previously the main aim of this research is to explore users' perception of the risks associated with SNSs across a number of age groups. Two research questions have been proposed to explore in further detail users risk perception on SNSs.

1 To what extent do users perceive themselves at risk of a wide range of negative events on SNSs? Does the nature and composition of these risk perceptions vary by age?

   1a. To what extent do users believe they are personally likely to encounter negative events on SNSs?
   1b. How do users perceive the consequences of these negative events?
   1c. To what extent are users concerned about these negative events?
   1e. How knowledgeable/aware are users of the negative events that can occur on SNSs?
   1f. To what extent do users perceive they have control over the negative events that can occur on SNSs?
   1g. Are females more likely than males to perceive themselves at risk on SNSs?

A model of the factors that can contribute to risk perception has been derived from the literature, see Figure 3.6. This model is used to assess the contribution of a number of factors to a user perceiving themselves to be at high risk for five negative events on SNSs.

2 What are the factors that contribute to a user perceiving themselves to be at a higher likelihood of experiencing negative events on SNSs?

   2a. What effect do the risk characteristics of knowledge, concern and control have on the likelihood of high personal risk perception?
   2b. What effect do demographic factors such as age and gender have on high personal risk perception?
   2c. How does prior experience affect the likelihood of high personal risk perception?

2e. What effect do psychological factors such as disposition to trust and online privacy concern have on the likelihood of high personal risk perception?

2f. How do contextual factors such as Internet experience, intensity of SNS use and personal information revealed affect the likelihood of high personal risk perception?

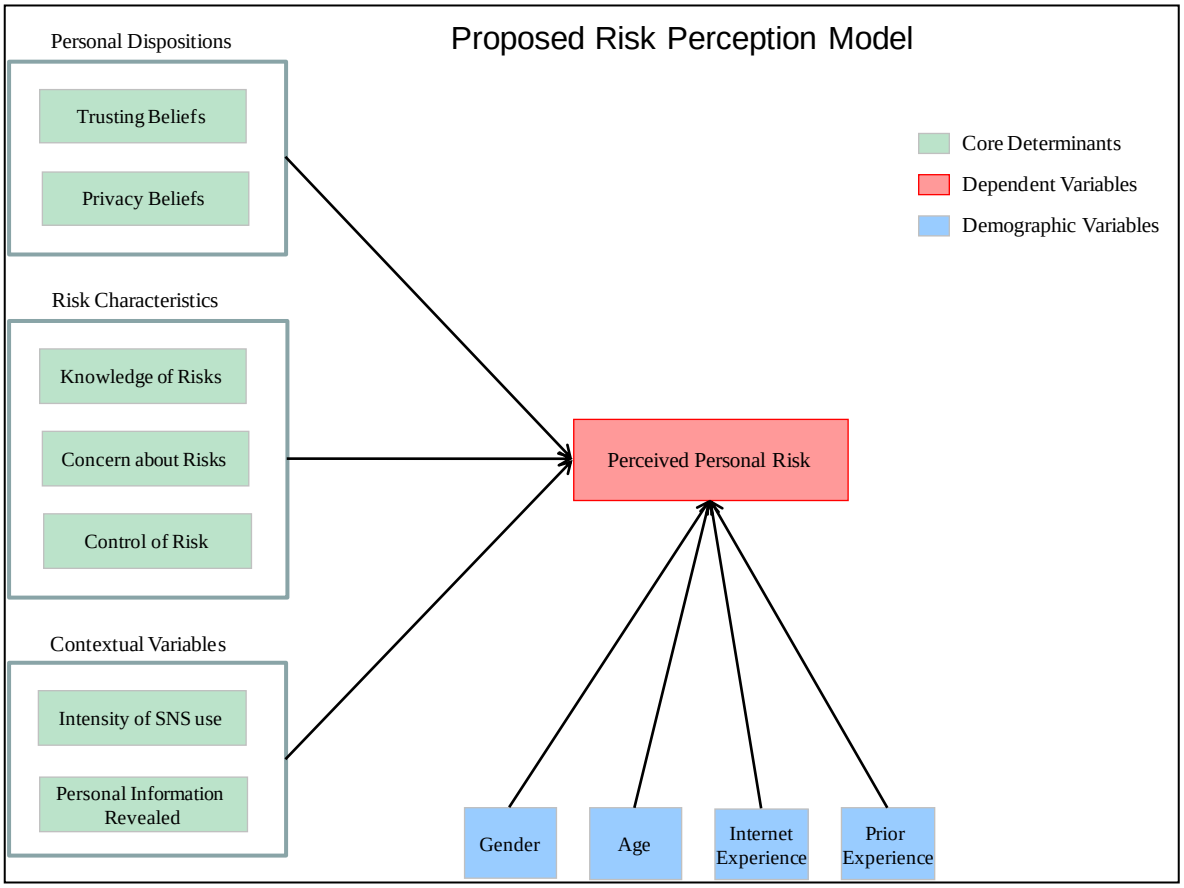


Figure 3.6 Proposed Risk Perception Model

Optimistic Bias

Previous research has shown that individuals tend to believe that they are less likely to encounter negative events and more likely to encounter positive events than the average person (Weinstein, 1980). This phenomenon is known as "*unrealistic optimism*" or "*optimistic bias*" as discussed in Section 2.4.4. Previous research indicates that optimistic bias is evident for IT events (Campbell *et al.*, 2007) and many studies of adolescent risk perceptions have found support for this concept (Hansen and Malotte, 1986, Benthin *et al.*, 1993, Cohn *et al.*, 1995). Some studies have examined whether optimistic bias differs between adults and adolescents and results indicate that adolescents show higher levels of optimistic bias (Cohn *et al.*, 1995, Arnett, 2000b). Studies that have examined online risks have also found evidence for a similar phenomenon called the "*third person effect*"

(Debatin *et al.*, 2009, Zhang and Daugherty, 2009, Livingstone *et al.*, 2011a). Davison's (1983) third-person effect theory proposes that individuals tend to expect mass media to have a greater effect on others than on themselves. This study has focussed on optimistic bias with regard to negative rather than positive events on SNSs as an optimistic bias for negative events has implications for risk perception and risky behaviour.

3 To what extent do users perceive that others are more likely than them to experience negative events on SNSs?

3a. How does optimistic bias differ between the negative events on SNSs?

3b. How does optimistic bias differ by age?

Behaviour on SNSs

Previous research has highlighted a number of behaviours that can potentially increase a user's vulnerability to negative events on SNSs. Early studies examining user's privacy settings on SNSs found that the majority of users were not setting their profiles to be restricted or private (Gross and Acquisti, 2005, Anchor, 2007, Dwyer, 2007, Hinduja and Patchin, 2008b, OFCOM, 2008), but there is evidence that this trend is changing and in particular with younger users (boyd and Hargittai, 2010, Livingstone *et al.*, 2010b, Madden and Smith, 2010, O'Neill *et al.*, 2011). Studies have found that women/girls have greater online safety concerns and are more likely than men/boys to alter their privacy settings (Lewis *et al.*, 2008, Fogel and Nehmad, 2009, Phippen *et al.*, 2009, Livingstone *et al.*, 2010b, O'Neill *et al.*, 2011). However studies have found significant dichotomies between specific privacy concerns and the information that was actually revealed on SNSs (Acquisti and Gross, 2006, Dwyer *et al.*, 2007, Livingstone, 2008, Tufekci, 2008, Debatin *et al.*, 2009, Fogel and Nehmad, 2009, Young and Quan-Haase, 2009), reflecting a "*privacy paradox*" that is evident in other Internet applications.

4 To what extent are SNSs users engaging in behaviours that could increase their vulnerability to risk?

4a. What are the privacy protection strategies that users implement on SNSs and how do these strategies differ by age and gender?

4b. To what extent does a privacy paradox exist between privacy settings, expressed privacy concern and personal information revealed on SNSs?

Peer Effect

It is well known that the effect of peers can be substantial in adolescence and it is acknowledged as a major variable in adolescent risk-taking (Jessor and Jessor, 1977, Benthin *et al.*, 1993, Gerrard *et al.*, 1996a, Miller *et al.*, 2000, Gardner and Steinberg, 2005). Studies have shown that peers can exert positive or negative effects. As communication with peer group members is the most important motivation for SNS use, it is anticipated that peer group influence will be strong on SNSs. A possible negative effect of peer influence, as suggested by Gross and Acquisti (2005), is that when peers are sharing certain types of information on SNSs, other users may feel obligated to do so as well. Another possible consequence of high levels of peer influence is that users spend more time on SNSs and share more personal information.

5 How and to what extent do peers influence the personal information revealed and intensity of SNS use?

4 Methodology

4.1 Introduction

This chapter presents the research philosophy and research approach of the thesis. All research (whether quantitative or qualitative or both) is based on some set of underlying assumptions about what constitutes "*valid*" research and which research methods are appropriate. These assumptions underpin the research strategy and in turn the research methods chosen (Saunders *et al.*, 2009).

Information Systems (IS) is a relatively new discipline which tends to draw upon theoretical frameworks from other more established disciplines such as computer science, computer engineering, sociology, anthropology, psychology, business and management studies. IS research is seen as a social rather than a technical science. As stated by Lee (2001, pIII), IS "*examines more than just the technological system, or just the social system, or even the two side by side; in addition it investigates the phenomena that emerge when the two interact"*. IS research is thus diverse in nature. Some researchers have argued that this diversity has led to a lack of identity for the IS discipline (Benbasat and Weber, 1996, Benbasat and Zmud, 2003) whereas others believe there is a strength in this diversity (Banville and Landry, 1989, Robey, 1996, Galliers, 2003, Elliot and Avison, 2005). From a research student perspective, the breadth of the IS discipline offers many advantages in allowing a large choice in the topic of study. IS studies are not confined to just studying technology but allow an outward focus to examine how a technology and a social system interact. This means that IS research is generally interdisciplinary and the IS researcher has to master not only research in IS, but also in other reference disciplines, some of which they may not be familiar with. The research question addressed in this thesis is typical of research in the IS discipline. In addition to IT and IS it also involves a knowledge of the risk perception reference discipline.

Figure 4.1 shows the structure of this chapter. The chapter begins by providing some background to the IS discipline and IS research. This is followed by a discussion of the research philosophy and approach of the thesis. The research methodology adopted in this research is explained in detail, including a discussion of design, administration and analysis issues. The chapter concludes with an examination of how the credibility of the research methods in this study is evaluated.

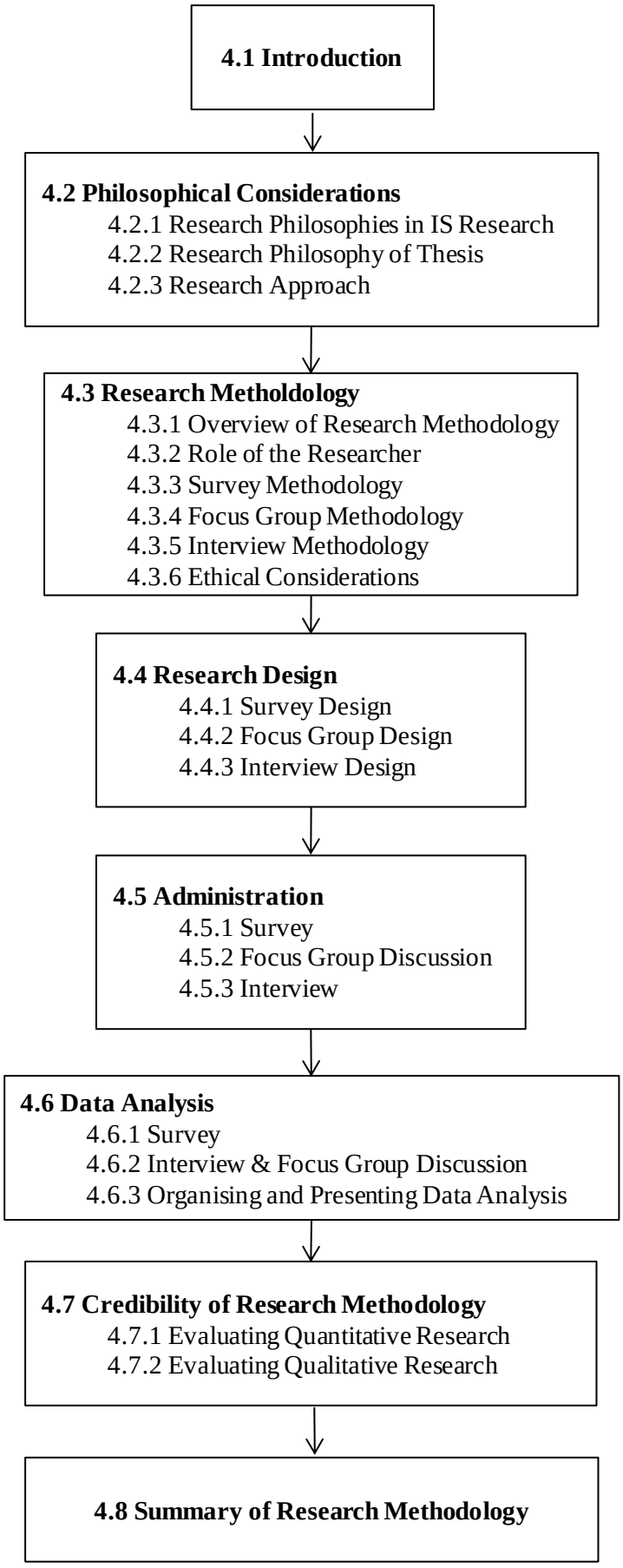


Figure 4.1 Structure of Chapter 4.

4.2 Philosophical Considerations

In a research context, philosophical assumptions can be characterised as a group of beliefs with associated modes of inquiry, these assumptions underpin the choice of research strategy and methods used in a study. These philosophical assumptions have been called "*worldviews*" or "*paradigms*" (a term initially coined by Thomas Kuhn (1970)). Morgan (2007, p49) defines paradigms "*as systems of beliefs and practices that influence how researchers select both the questions they study and methods they use to study them*".

Before presenting the research philosophy of this thesis the dominant research paradigms in IS research are introduced briefly as these inform the choice of research philosophy and research strategy employed in this thesis.

4.2.1 Research Philosophies in IS Research

In IS research there are three predominant research paradigms, positivism, interpretivism and critical research, but numerous other research paradigms/philosophies exist in the social science and information systems area, such as: critical rationalism, hermeneutics, ethnomethodology, social realism and pragmatism. A number of different typologies of research paradigms exist in the social science research literature, such as those of Burrell and Morgan (1979) and Guba and Lincoln (1994, 2005). In IS research the typology suggested by Orlikowski and Baroudi (1991), based on Chua (1986), has been particularly influential. This typology examined three distinct epistemological categories: positivist, interpretive and critical. A further discussion of these typologies can be found in Appendix E.

Although not mentioned in any of these typologies, the pragmatic paradigm is gaining some relevance. This paradigm is presented in a number of popular research method textbooks (Creswell and Plano Clark, 2007, Creswell, 2009, Saunders *et al.*, 2009, Teddlie and Tashakkori, 2009) and has been linked to mixed method research.

Positivism & Postpostivism: Positivists believe that an objective physical and social world exists which can be measured through objective methods. Positivism is also known as the "*natural science model of social science research"* (Lee *et al.*, 1997, p3). Postpostivism is a revised form of positivism that addresses some of the criticisms of

positivism, but maintains an emphasis on quantitative methods. One criticism of positivism is the assertion that research can be carried out in an objective and value-free way. Postpositivists acknowledge that their value systems play an important role in how they conduct their research and interpret their data.

Interpretivism: Interpretivists believe that the methods of natural science are inadequate for social science. They believe that reality is socially constructed and given meaning by people. The researcher cannot objectively observe/measure meanings but has to gain a relativistic, shared understanding of phenomenon.

Critical approaches: Critical research is a variant of interpretivism. The ideological stance and assumption is that the purpose of research is emancipation. The role of the critical researcher is to go beyond mere studying and theorising and to actively affect change in the phenomenon being studied.

Pragmatic paradigm: The aim of pragmatism is to find a middle ground between the philosophical dogmatism of positivism and interpretivism. Pragmatists advocate the use of mixed methods in research and acknowledge that the values of the researcher play a role in the interpretation of the results.

Easterby-Smith *et al.* (2002) produced a table to contrast positivism and interpretivism. The framework of their table has been used as a template for Table 4.1 which compares these four research philosophies. A more detailed description of each of these paradigms can be found in Appendix F. It should be noted that the descriptions of paradigms presented to date in this literature review illustrate the "*pure*" versions of each research philosophy, but in practice these distinctions are not always so evident. In practical terms, the lines of demarcation are not so clear-cut as for example some positivist researchers will use some interpretive aspects in their research.

	Positivism	Interpretivism	Critical Research	Pragmatism
Ontology	Reality is external and objective Single reality Researcher and reality are separate	Reality is socially constructed Multiple social realities Researcher and reality are inseparable	Reality is historically and socially constructed Multiple social realities Researcher and reality are inseparable and researcher can actively affect change in the phenomena being studied	View chosen to best enable answering of research question
Epistemology	Objective reality	Subjective reality Reality co-constructed	Subjective reality Reality co-constructed	Both objective and subjective points of view, depending on research question.
Human interests	Are irrelevant - determinism	Can influence and change environment – voluntarism	Can influence and change environment – voluntarism but are constrained	Depends on approach
Role of theory/logic	Hypothesis and deduction	Inductive logic or reasoning	Inductive logic or reasoning and critique	Can use both deductive and inductive logic
Concepts	Focus on facts	Focus on meanings	Focus on meanings	Focus on facts and meanings
Units of analysis	Should be reduced to simplest terms	Should include social context	Should include social and historical context	Should include social context
Generalisation	Nomothetic statements (time and context free generalisations)	Ideographic statements (time and context bound working hypotheses)	Ideographic statements emphasised; results linked to issues of social inequality and justice.	Ideographic statements emphasised
Sampling	Large random samples (probability sampling)	Small number of cases chosen for specific reasons (purposive sampling)	Small number of cases chosen for specific reasons and examined over time	Can use both probability and purposive sampling
Methods	Surveys, controlled experiments (primarily quantitative)	Participant observation, ethnography, interviews, hermeneutics (primarily qualitative)	Critical ethnography, longitudinal studies, long term historical studies. (primarily qualitative)	Can use both quantitative and qualitative methods

Table 4.1 Contrasting Implications of Positivism, Interpretivism, Critical Research and Pragmatism.

There has been much debate in the academic literature regarding these paradigms and this has become known as the "*paradigm war*" or "*paradigm debate*". This debate has primarily been between interpretivists and positivists with each defending their approach, but also includes whether it is even appropriate to mix different paradigms. Some believe that it is inappropriate to mix quantitative and qualitative methods due to the fundamental differences in the paradigms underlying those methods (Burrell and Morgan, 1979, Smith, 1983, Guba, 1990). This follows Thomas Kuhn's (1970) argument that competing paradigms were "*incommensurable paradigms*" (also known as the "*incompatibility thesis*"). It is argued that using multiple paradigms produces incomplete and vague information which is of limited use (Silverman, 1969, Pfeffer, 1993). However, increasingly researchers are advocating a mixed method approach to research combining the techniques and viewpoints of positivists and non-positivists to *triangulate* on phenomena. Many researchers have argued that a methodological pluralist approach is suitable for IS research (Orlikowski and Baroudi, 1991, Galliers, 1992, Landry and Banville, 1992, Robey, 1996, Goles and Hirschheim, 2000, Mingers, 2001, Chen and Hirschheim, 2004). Some argue that the diverse nature of IS research is particularly suited to a pluralist approach (Landry and Banville, 1992, Goles and Hirschheim, 2000, Mingers, 2001) and that research results will be enriched if different research methods (especially from different paradigms) are routinely combined together (Goles and Hirschheim, 2000, Mingers, 2001). A number of authors contend that pluralism should be driven by the research question rather than the dominant paradigms (Galliers, 1992, Robey, 1996, Goles and Hirschheim, 2000).

Although many researchers are now advocating the use of mixed method and pluralist research in IS, studies show that the positivist paradigm is still the most dominant approach in US journals (Chen and Hirschheim, 2004, Richardson and Robinson, 2007, Avison *et al.*, 2008). In European journals, the qualitative approach is slightly ahead of the quantitative approach. In both areas the representation of mixed research is very low. Researchers have suggested a number of reasons for this. One suggestion proposed by Mingers (2001) is that many researchers believe in paradigm incommensurability and thus only follow one paradigm. Another suggestion is that researchers tend to follow paradigms based on their academic culture in a "*parochial*" manner (Galliers and Meadows, 2003). Chen and Hirschheim (2004) state that the tenure and promotion "*publish or perish*" position in academic institutions could account for the domination of positivist research, as positivist research is more easily accepted due to its well established research tradition.

There is also a belief that carrying out research using the positivist paradigm is less time consuming than using the interpretive approach (Walsham, 1995). Another viable explanation is that mixed research may be published as two separate papers rather than one, in order to maximise the publications from a single piece of research (Avison *et al.*, 2008). The editorial stance of journals can also have an impact on what is published.

4.2.2 Research Philosophy of this Thesis

The ontological stance of this dissertation is predominantly postpositivist, but also combines some interpretivist characteristics. The primary focus of the research is to assess an individual's perception of risk associated with the use of SNSs. Risk perception can be defined as "*people's beliefs, attitudes, judgements and feelings as well as the wider cultural and social dispositions they adopt towards hazards and their benefits*"(Pidgeon *et al.*, 1992, p89). The dominant paradigms in risk perception research, the psychometric and cultural paradigms are both predominantly based on positivist philosophies and have used survey and quantitative techniques to assess individuals risk perceptions, but increasingly researchers are acknowledging that risk perceptions also involve individual beliefs and feelings. These aspects of risk perception are not easy to quantify objectively, but rather are socially constructed and using interpretive research will provide additional insights in this area. Many of the risk factors identified with using SNSs are easily measured variables such as age, gender, amount of time spent on sites and constructs such as computer experience etc., but also include many factors that are not so easily measured such as attitudes to SNSs and effects of online usage. Interpretive methods are used to gain an in-depth understanding of these factors.

The epistemological position of this research combines characteristics of positivism and interpretivism. The research follows a mixed methods sequential explanatory research design. This research design consists of two distinct phases: quantitative followed by qualitative (Creswell and Plano Clark, 2007). In the first phase of this design, a survey is used to collect empirical data on user's SNS usage and their perceptions of the risks on these sites. The data from the survey is analysed. This quantitative analysis provides an initial examination and overview of the risk perceptions and risk factors associated with SNS usage. The qualitative data are collected and analysed second in the sequence and are used to gain a deeper understanding of the risk perceptions and risk factors highlighted in the first phase. The qualitative data are collected using in-depth interviews and focus

groups. The rationale for this approach is that the quantitative data and their subsequent analysis provide a general understanding of the research problem. The qualitative data and their analysis refine and explain those statistical results by exploring participants' views in more depth (Greene and Caracelli, 2003, Tashakkori and Teddlie, 2003). A mixed method sequential exploratory design is used for developing some aspects of the survey. As with the explanatory design, the results of the first method, focus groups (qualitative) inform the second method, survey (quantitative). This design is used for identifying the negative events associated with SNS usage.

This research adopts a mixed methods design for a number of reasons:

1. In IS research, positivism has been subject to increasing criticism as some researchers feel that it isn't an appropriate epistemology for IS research (Hirschheim, 1992, Walsham, 1995, Remenyi *et al.*, 1998). A number of researchers contend that using just a positivist research perspective for studying IS phenomena is restrictive and they suggest using a plurality of research perspectives (Orlikowski and Baroudi, 1991, Galliers, 1992, Landry and Banville, 1992, Robey, 1996, Goles and Hirschheim, 2000, Mingers, 2001, Mingers, 2003, Chen and Hirschheim, 2004, Avison *et al.*, 2008).
2. The rationale for mixing both quantitative and qualitative data within the one study is based on the reasoning that neither methods are sufficient on their own to fully explain the details of a situation. When they are used in combination, quantitative and qualitative methods complement each other and allow for a more robust analysis (Greene and Caracelli, 2003, Tashakkori and Teddlie, 2003).
3. It is important that mixed methods research is driven by the research question rather than the dominant paradigms (Galliers, 1992, Robey, 1996, Goles and Hirschheim, 2000, Creswell and Plano Clark, 2007). Although risk perception research has been dominated by positivist philosophies, it is a concept that also involves individual beliefs and feelings, so it is clear that interpretive research could provide additional insights in this area.
4. A number of important factual and easily measurable issues need to be determined as these can effect an individual's risk perceptions to SNS usage. These can include for example gender, age, level of usage etc. These can easily be determined using positivist research methods.

4.2.3 Research Approach

This thesis uses a combination of deductive and inductive logic as proposed by the inductive-deductive research cycle (see Figure F.1, Appendix F). Figure 4.2 shows that the literature review presents a number of hypotheses or conjectures with respect to risk perceptions and social networking, these conjectures are tested with quantitative methods using deductive reasoning. This is followed by a qualitative analysis. Following both of these analyses, the findings and implications are derived using inductive reasoning. Inductive reasoning is also used in deriving, from focus groups, the list of negative events that are of concern to users of SNSs. This informs the survey instrument.

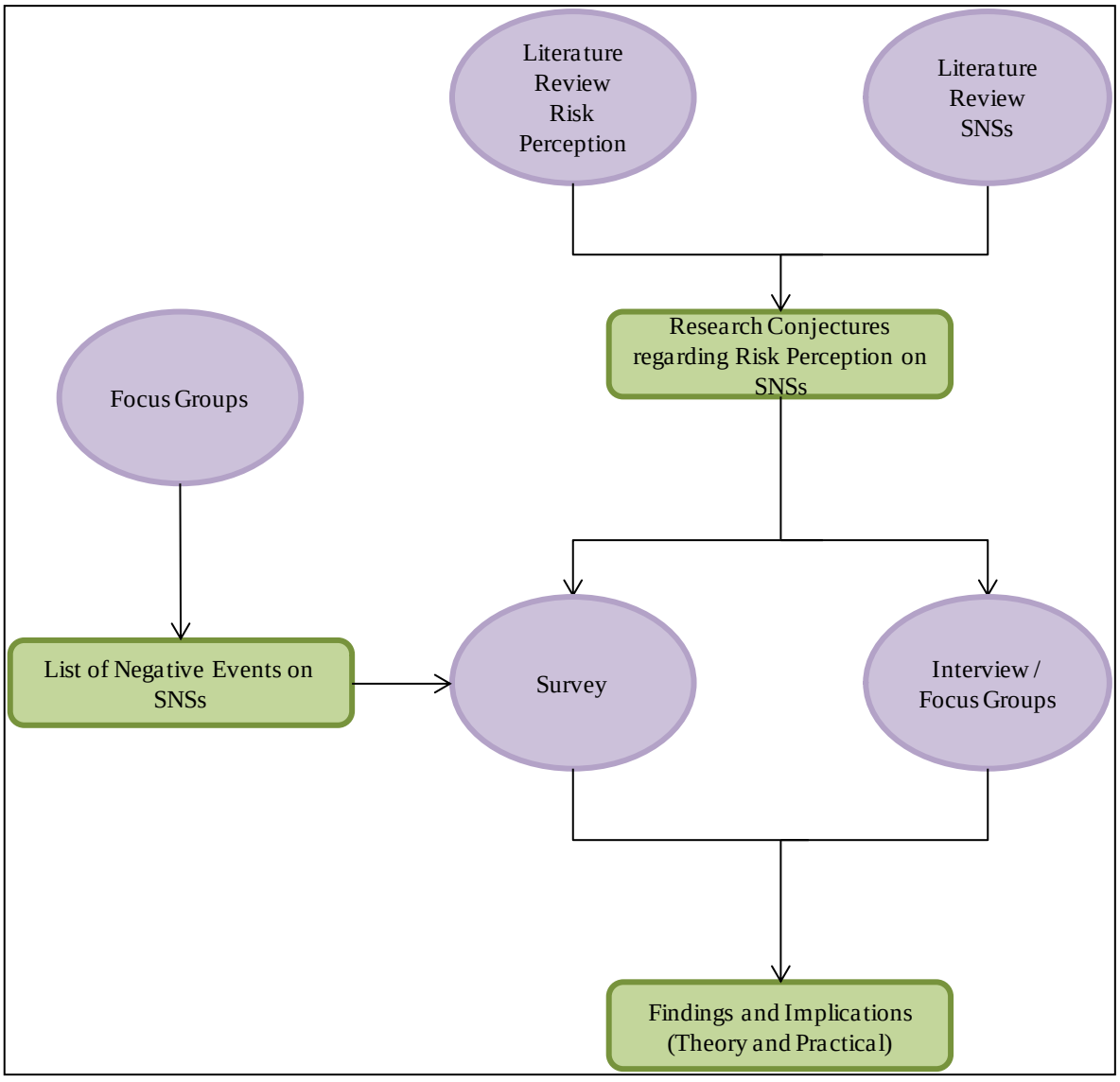


Figure 4.2 Research Approach

4.3 Research Methodology

4.3.1 Overview of Research Methodology

A mixed method research design is chosen for this research as a mixture of qualitative and quantitative methods are needed to fully address the research question. The rationale for mixing both quantitative and qualitative data within the one study is based on the reasoning that neither quantitative nor qualitative methods are sufficient on their own to fully explain the details of a situation. When they are used in combination, quantitative and qualitative methods complement each other and allow for a more robust analysis (Greene and Caracelli, 2003, Tashakkori and Teddlie, 2003, Creswell and Plano Clark, 2007). Mixed method, pluralist research has been given many names, for example multiple operationalism (Campbell and Fiske, 1959), triangulation (Denzin, 1970), blended research (Thomas, 2003a), integrative research (Johnson and Onwuegbuzie, 2004), multimethod research (Mingers, 2003, Morse, 2003) and mixed research (Johnson and Christensen, 2008). However, mixed method research has become the most popular term used to describe this movement (Tashakkori and Teddlie, 2003, Creswell and Plano Clark, 2007, Creswell, 2009, Teddlie and Tashakkori, 2009) and is the term used in this thesis.

Johnson *et al.* (2007, p123), after examining numerous definitions of mixed method research, propose the following definition:

> *"Mixed methods research is the type of research in which a researcher or team of researchers combines elements of qualitative and quantitative research approaches (e.g., use of qualitative and quantitative viewpoints, data collection, analysis, inference techniques) for the broad purposes of breadth and depth of understanding and corroboration."*

Mixed method researchers suggest a continuum, as shown in Figure 4.3, of philosophical considerations as a better representation of how researchers work rather than the four distinct paradigms that are represented in Table 4.1. Interpretivism and critical research (predominantly qualitative research) would be towards the right of the table, positivism (predominantly quantitative research) towards the left and pragmatism would represent the middle points of view.

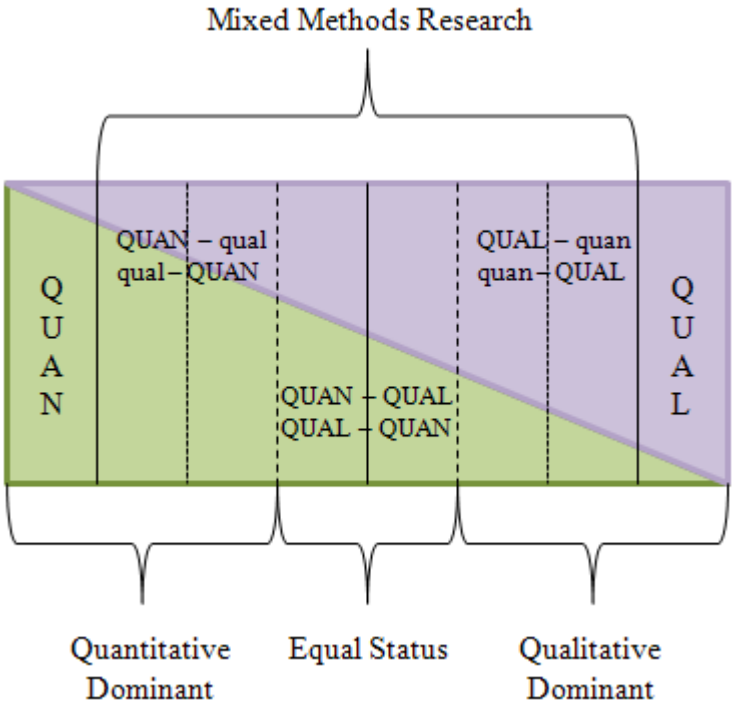


Figure 4.3 Continuum of QUAL and QUAN Research
(Johnson *et al.*, 2007, Teddlie and Tashakkori, 2009).

The area around the centre of the continuum, *equal status*, represents mixed methods researchers that believe that both quantitative and qualitative approaches add insights to the research question. Both approaches are given equal weighting in the research project. *Qualitative dominant*, symbolised as QUAL + quan or quan + QUAL, researchers believe that it is important to include quantitative data and approaches into otherwise qualitative research projects. The research philosophy is predominantly interpretive. A *quantitative dominant* (QUAN + qual or qual + QUAN) researcher believes it is important to include qualitative data into a predominantly quantitative research project. These researchers would hold a post-positivist view point. It is the latter type of mixed method research that is adopted in this thesis.

In considering how to mix methods, a number of researchers have presented typologies of mixed method designs (Greene *et al.*, 1989, Morse, 2003, Tashakkori and Teddlie, 2003, Johnson and Onwuegbuzie, 2004, Creswell and Plano Clark, 2007). Tashakkori and Teddlie (2003) warn that although these typologies are useful for researchers, they are by no means exhaustive and new designs are evolving. A choice was made to use the typology formulated by Creswell and Plano Clark (2007) to help choose the most suitable mixed method design for this study. The Creswell and Plano Clark typology (2007) includes four major types of mixed method designs (with variants in each): triangulation;

embedded; explanatory and exploratory. Further details about each of these design types can be found in Appendix G.

It became clear that a single research design would not be adequate to fully address the research question so a choice was made to use a mixed method design that has more stages. A three strand sequenced mixed method research design was chosen (qual → QUAN → qual) using a combination of both the exploratory and explanatory research designs. This research design is shown in Figure 4.4.

The primary research design chosen for this thesis is the sequential explanatory design. This is a two-phase mixed method design. The purpose of this design is that qualitative data helps explain or builds upon initial quantitative results (Creswell *et al.*, 2003). In this study the quantitative first phase of the design is a survey that was administered to adolescents (ages 12-17), emerging adults (ages 18-25) and a working adult cohort. The survey is used to measure user's risks perceptions with respect to SNS's. The second, qualitative phase expands on the results found in the survey and looks for explanations as to why certain risk perceptions existed. The second phase consists of qualitative semi-structured interviews with the emerging adult cohort and qualitative focus groups interviews with the adolescent group. In this design the primary emphasis is on the quantitative aspects (i.e. QUAN emphasised). There is a number of benefits in using this explanatory design:

- it is considered the most straightforward of the mixed method designs (Creswell and Plano Clark, 2007);
- the design is split into two phases that are carried out sequentially. This means that a single researcher can carry out the design;
- the design appeals to the researcher as it has a strong quantitative emphasis.

The challenges in using the design are that:

- it takes a long time to implement the two phases;
- it is necessary to learn about multiple methods and approaches and understand how to mix them appropriately.

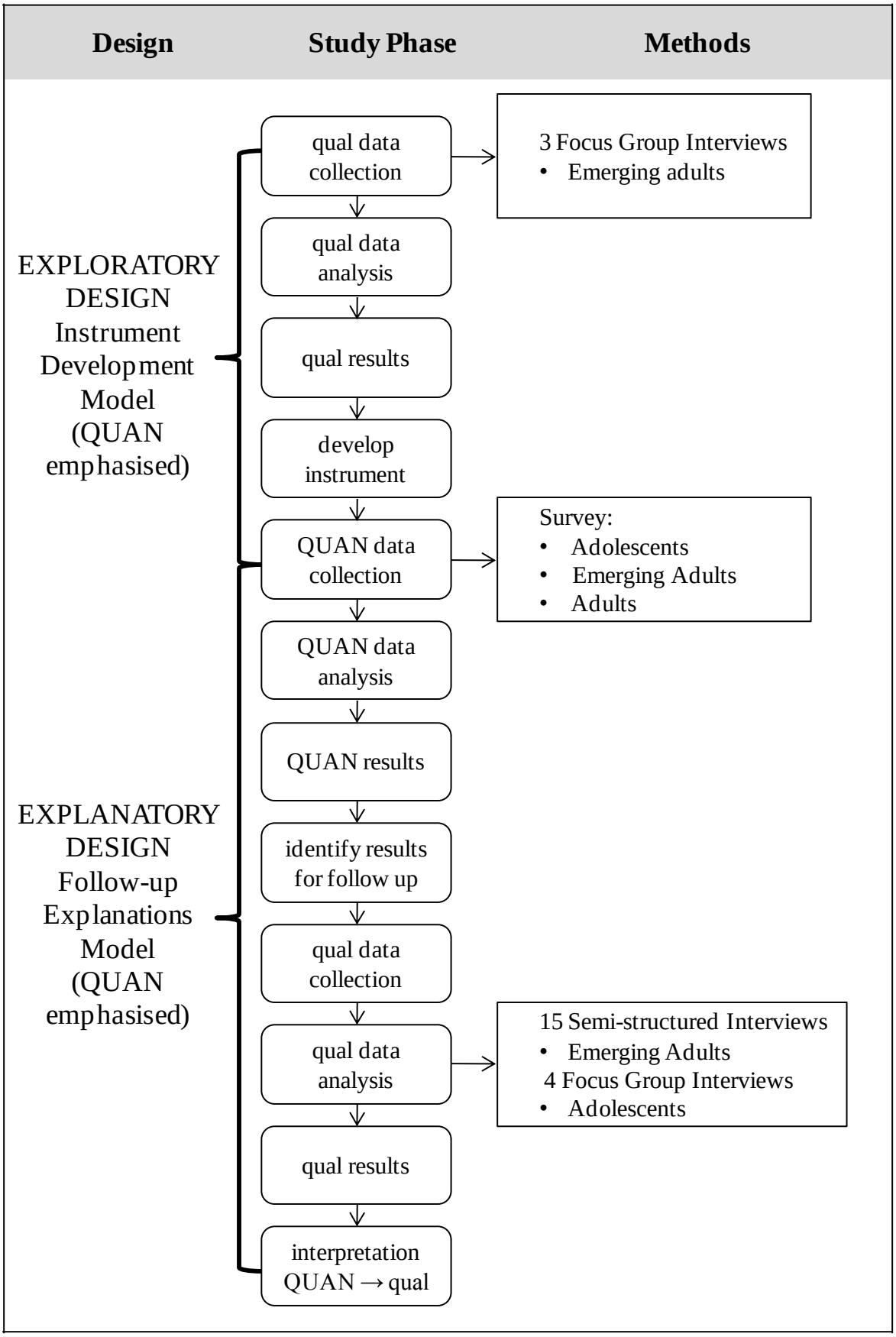


Figure 4.4 Overview of Research Design

The sequential exploratory mixed method design is also used in the study. In this design the results of the first method (qualitative) are used to help inform the second method (quantitative) (Greene *et al.*, 1989). This design is particularly useful to identify important variables to study quantitatively (Creswell and Plano Clark, 2007). The literature identifies a number of risks associated with SNSs, as discussed in Section 3.5. It is not possible to address all these risks in the survey, so it is necessary to choose a shortlist of risks that are relevant to current users of SNSs. The design starts with focus group interviews with emerging adults to explore their views on the risks associated with SNSs and develop a list of the risks most pertinent to their age group. These qualitative findings are then used as a guide for the development of the risk items to be included in the subsequent survey. Again the emphasis in this design is on the quantitative data. The benefits and challenges of this design are similar to those of the explanatory design. A further consideration is that the researcher needs to decide which data to use from the qualitative phase in building the quantitative survey.

As the intention of the explanatory design is to use the qualitative data (focus group interviews and semi-structured interviews) to provide more detail about the quantitative results (survey), it was decided that the same individuals could be included in both data collections. This consideration was not deemed important for the exploratory design and the survey was administered to a different and larger population.

After a discussion of the researcher's role, the following sections describe the differing research strategies that were employed in this study.

4.3.2 Role of the Researcher

It is important with any research but particularly with qualitative research to explicitly identify the personal values, assumptions and biases of the researcher at the outset of the study. The researcher's involvement with data collection in the qualitative and quantitative phases of this study is different. In the quantitative phase, the researcher has administered the survey and collected the data using standardized procedures for survey design and incorporating the relevant reliability and validity checks of the instrument. The data analysis has been performed using rigorous statistical analysis techniques. In the qualitative phase, the researcher assumes a more participatory role as an interviewer or as a focus group facilitator.

The researcher knows some of the participants in the qualitative study as a course lecturer. The researcher has worked in the IT industry for a number of years as a systems administrator and IT consultant and has experience of the IS/ICT risk landscape, the researcher has also previously published in the area of Internet privacy, identity theft and spamming (Keaney and Remenyi, 2004, Keaney, 2009). All of these experiences introduce a possibility for subjective interpretations of the phenomenon being studied and create a potential for bias. To minimise this bias extensive verification procedures, including triangulation of data sources have been used to establish the accuracy of the findings and to control for some of these bias issues. Further details of how the credibility of both the quantitative and qualitative methods are evaluated is presented in Section 4.7.

4.3.3 Survey Methodology

As defined by de Leeuw *et al.* (2008, p2) a survey is a *"research strategy in which quantitative information is systematically collected from a relatively large sample taken from a population".* The survey method is employed in this study to explore the SNS usage and risk perceptions of three different age cohorts: working adults, emerging adults (college students) and adolescents (school students). Figure 4.5 illustrates the variables that are measured by the survey instrument.

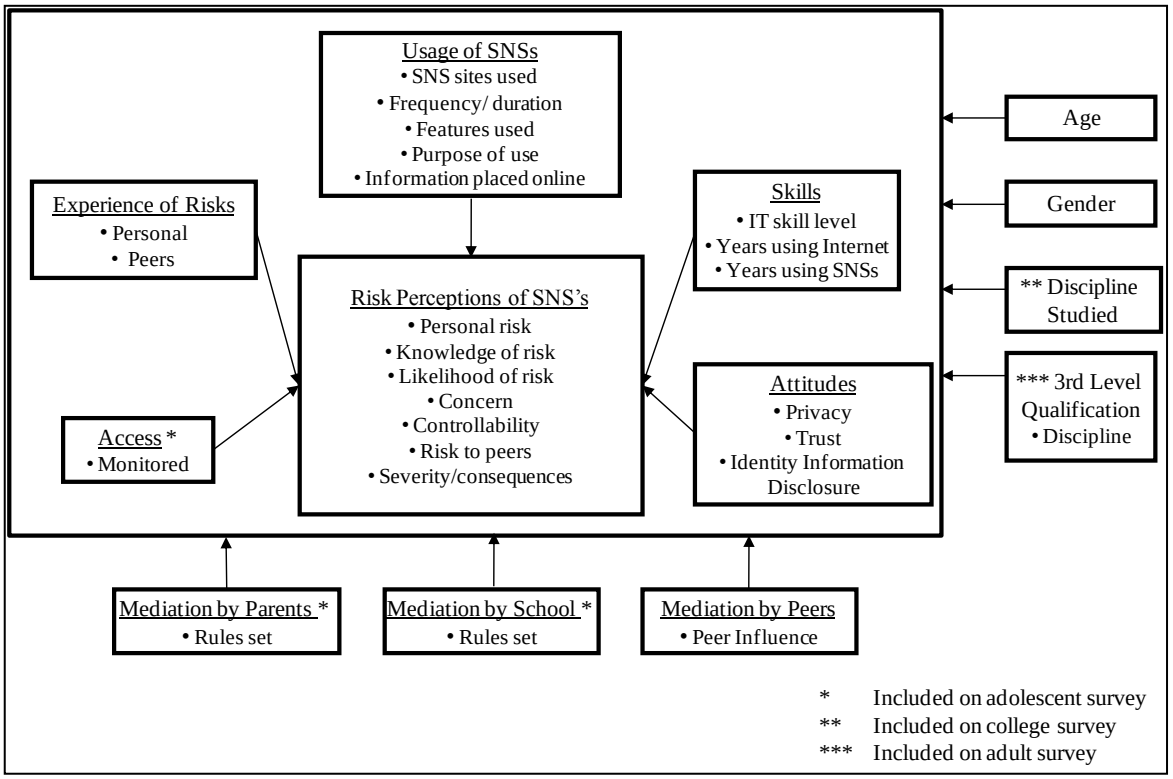


Figure 4.5 Variables Measured by Survey Instrument

Surveys are an effective research strategy for this study as they allow the collection of a large amount of data from a sizeable population in an economical way and data collection can be standardised which allows for easy comparison across groups. A limitation of the survey strategy is that the data collected is unlikely to be as wide-ranging as those collected by other research strategies. Surveys require simple questions and measures and do not allow for particular responses to be explored in further detail. This can sometimes result in a superficial understanding of the phenomena under investigation. This limitation is offset in this study by the use of semi-structured interviews and focus group interviews. Although surveys are viewed as a relatively quick method of collecting data from a large number of respondents, the time required can be underestimated. The time required in planning the research to ensure methodological rigor, piloting the survey and administrating a large scale survey is appreciable.

Many of the recommendations of "*The Tailored Design Method*" (Dillman *et al.*, 2009) are followed in this study. This is a scientific approach to conducting sample surveys that uses motivational features (based on social exchange theory) to encourage high quantity and quality of responses to surveys. Other texts consulted during the design and administration of the survey include: Survey Methodology (Groves *et al.*, 2004), International Handbook of Survey Methodology (de Leeuw *et al.*, 2008) and Designing Effective Web Surveys (Couper, 2008).

Section 4.5.1 examines the steps taken in designing the survey, including the methods used to pretest the questionnaire. Section 4.6.1 addresses survey administration and Section 4.7.1 describes the data analysis phase. Assessing the validity and reliability of the survey instrument is described in Section 4.8.1.

4.3.4 Focus Group Methodology

The section introduces the focus group methodology and justifies its suitability as a research method for this study.

Focus groups are a qualitative data gathering technique. Morgan (1996, p130) defines focus groups "*as a research technique that collects data through group interaction on a topic determined by the researcher*". Krueger and Casey (2000, p5) contend that focus groups should be held in "*a permissive, non-threatening environment*". The method used

with focus groups is to collect data across several focus groups and the researcher then compares and contrasts the data. Focus groups thus differ from other group interactions as the goal is not to come to some conclusion at the end of each discussion. Focus groups have been utilised in two ways in this research. In the first instance, focus groups are used as the qualitative part of the mixed method sequential exploratory design to help develop the content of the survey. As stated in Section 2.6.3., research has shown that adolescent/emerging adult and adult opinion often differ in what is perceived as risky behaviour (Furby and Beyth-Marom, 1992). As the reviewed research literature and popular press articles about the risks with SNSs are written from an adult viewpoint, it is important to seek current users' perceptions and views of the risks inherent in SNSs, before a survey instrument is developed. Eliciting views in this way presents a more natural environment than that of an individual interview because participants are influenced and influencing others, just as they do in real life (Krueger and Casey, 2000) and this interaction offers valuable data on the extent of consensus and diversity among the participants. These focus groups are useful as they show how participants talk about the risks on SNSs and allow the survey to be designed using relevant language for adolescents and emerging adults. Another advantage is that it is an efficient way to interview more participants in a shorter amount of time than is possible with a one to one interview.

The second way focus groups are utilised in this study is as the qualitative part of the mixed methods sequential explanatory research. Focus groups are used with the adolescent cohort of this study as a follow up to help interpret the survey results and to add depth to the responses obtained in the survey. The chosen methodology for the College cohort is semi-structured interviews, but for the adolescent cohort, focus group interviews are deemed a more suitable methodology. As access to schools is limited, focus group interviews are less time consuming than conducting individual interviews. Focus groups are less threatening for adolescents than one on one interviews.

Focus groups are run by a moderator. The moderator should be as neutral as possible. One of the weaknesses of focus groups relates to the role of the moderator. Research has shown that the moderator can interrupt the natural flow of discussion and often the moderator determines the agenda and form of the discussion (Agar and MacDonald, 1995). This argument of interviewer or researcher effect is not only limited to focus groups but can be applied to most research methods. Increasingly focus groups are being used successfully with adolescents and children (Gibson, 2007, Stewart *et al.*, 2007), but the

role of the moderator is especially important in ensuring the group members are comfortable and relaxed (Vaughn *et al.,* 1996). The choice of moderator, the age range of group members, the questioning route and maintaining involvement with the discussion are all important considerations for adolescent focus groups. These considerations are described in further detail in Sections 4.4.2 and 4.5.2.

4.3.5 Interview Methodology

The section discusses the interview methodology and explains the use of this research method in this study.

Qualitative interviews are an important and commonly used data gathering tool in qualitative research. The research interview has been defined by Cannell and Kahn (1968) as cited by Cohen *et al.* (2007, p351) as:

> *"a two-person conversation initiated by the interviewer for the specific purpose of obtaining research-relevant information, and focused by him on content specified by research objectives of systematic description, prediction or explanation."*

Semi-structured interviews are used in this study as the qualitative part of the mixed methods sequential explanatory research design. Semi-structured interviews are used with the emerging adult cohort of this study to help interpret the survey results and to add depth to the responses obtained in the survey. Semi-structured interviews were chosen over unstructured interviews, as with a structured approach, comparisons can be made across all respondents.

As with qualitative methods in general, the qualitative interview is prone to subjectivity and bias on the part of the interviewer. A further consideration is that qualitative interviews cannot be thought of as "*normal*" everyday conversations, as the interviewer defines and controls the interview (Kvale and Brinkmann, 2009). The questions are posed by the interviewer, the interviewer can express ignorance (but not the interviewee) and the responses must be as explicit and detailed as possible (Cohen *et al.,* 2007). Qualitative interviews are a constructed rather than a naturally occurring conversation and as stated by Myers and Newman (2007) the qualitative interview is an artificial situation. Unlike quantitative research, there is no formula for conducting qualitative research, but a number

of models exist that can help guide the novice researcher (Rubin and Rubin, 2005, Myers and Newman, 2007, Kvale and Brinkmann, 2009). Insights and advice from other researchers were also included (Fontana and Frey, 1994, Patton, 2002, Rubin and Rubin, 2005, Oates, 2006, Cohen *et al.*, 2007, Myers and Newman, 2007, Saunders *et al.*, 2007).

4.3.6 Ethical Considerations

In research of this nature, there are two fundamental ethical questions: what is the ethically correct way to collect, process and report research data; and how should researchers behave with respect to their research subjects? The conduct of this research was guided by the ethical guidelines set down by Trinity College Dublin, the School of Computer Science and Statistics, and to cater for research with adolescents, the guidelines set down by the Children's Research Centre, Trinity College Dublin. The core ethical principles of this research are:

- to have a commitment to the well-being of those participating in the study (beneficence);
- to have a commitment to doing no harm (non-maleficence); and
- to have a commitment to the rights of those involved including the right of individuals to take responsibility for themselves (autonomy).

These principles follow a deontological as opposed to teleological view and advocate the application of *primum non nocere*, first of all do no harm. Appendix H describes the ethical considerations raised by this study and how they were addressed.

It can be difficult with some mixed method research to gain ethical approval. As a sequential mixed method research design was used in this study, it was possible to split the ethical approval requests into separate submissions for the quantitative and qualitative aspects of this study. Requests for ethical approval were submitted to and passed by the Ethics Research Committee, School of Computer Science and Statistics, Trinity College Dublin. Section H.3 shows the ethical approval application for the first phase survey of school children.

4.4 Research Design

4.4.1 Survey Design

This section describes the steps taken in designing the survey. The steps described include: the choice of sampling frame and how the sample was designed and selected, the mode of data collection used, how the questionnaire was designed and the constructs measured. The methods used to pretest the questionnaires are also described.

Target Population, Sampling Frames and Sample Selection

An aim of this study was to examine if risk perceptions to SNSs varied over different age groups. Three target populations were identified, adolescents (12-17 years old), emerging adults (18-24 years old) and older adults (25+). For convenience to the researcher, the target populations were restricted to a single geographical location, Dublin Ireland. School students were selected as the population most suitable for accessing the adolescent cohort. The target population consisted of all public and private post-primary school students in the Dublin area. Undergraduate college students were considered an ideal population for studying emerging-adult SNS users, given their high Internet connectivity levels. A large university in Dublin, Trinity College was selected. Without suitable resources, gaining access to a representative population of older adults is extremely difficult. Using working adults in various organisations as the target population was deemed a suitable compromise. Although working adults are not fully representative of the adult population, carrying out the study with working adults would allow the researcher explore whether differences in older age groups are indicated.

A multi-stage sampling approach was used to sample the school student population. The first-stage sampling frame for the school students was a list of post-primary schools in the Dublin area, downloaded from the Irish Department of Education website. The second stage sampling frame was the classes within the schools selected. Due to resource constraints, it was only possible to survey a maximum of 8 schools. These 8 Schools were randomly selected using stratified sampling to be representative of the different types of schools in the Dublin area, i.e. three girls only schools (one private funded, two public funded), three boys only schools (one private funded, two public funded) and two co-educational schools (one private funded, one public funded). Many difficulties emerged in attaining access to these schools and it became clear that access to schools was most

successful when contacts were known in the schools. The sampling strategy had to be modified to a non-probability convenience sample of schools. The second stage of sampling consisted of randomly selecting a class within each year (from 1st year to 5th year). All students in the selected classes were eligible to participate. The proposed sample size for the adolescent study was set at 1000, 125 (i.e. 5 classes) students from 8 schools.

As it was possible to administer a web-based questionnaire to the full population of college students via a College maintained e-mail list, it was not necessary to select a sample. Some researchers (as discussed below) have expressed concern that carrying out a web-based questionnaire studying Internet use could be biased. Web-based questionnaires generally have a lower response rate. To address these concerns, a group-administered questionnaire was also carried out. A list was prepared of large undergraduate classes run in two disparate faculties (Faculty of Arts, Humanities and Social Sciences and Faculty of Engineering Mathematics and Science). A selection of 7 classes was chosen from the full list, the classes were stratified by faculty and year of study. All students in the selected classes were eligible to participate. The sample size for the group-administered College survey was 1,245.

For the working adult cohort, using a convenience sample, a list of larger Dublin based companies was compiled. Gaining access to companies proved extremely difficult and only one company agreed to take part in the study. As it was possible to administer a web-based questionnaire to the full staff population of this company via a staff e-mail list, it was not necessary to select a sample.

Mode of Collection

Questionnaires were administered to 3 separate cohorts. Table 4.2 shows the methods of data collection used for each cohort:

Cohort	Mode of Collection	Use of Researcher
College Students	1. Group-administered questionnaire 2. Web-based questionnaire	1. Researcher administered – same researcher for each group 2. None
Working adults	Web-based questionnaire	None
Adolescents	Group-administered questionnaire	Researcher administered – same researcher for each group

Table 4.2 Methods of Data Collection used in Study

Web-based questionnaires offer the advantage of improved and efficient data collection and compared to other modes of data collection are relatively inexpensive. Early research into the use of web-based questionnaires expressed some concerns with the methodology. It was argued that Internet samples were not diverse and did not give a full population coverage (Krantz and Dalal, 2000); Internet samples were maladjusted, socially isolated or depressed (Kraut *et al.*, 1998); data obtained from Web sites were affected by the presentation format of the site; web-based questionnaire findings could be adversely affected by the anonymity afforded by the web (Buchanan, 2000) and that the findings of web-based questionnaires were inconsistent with findings from traditional methods (Krantz and Dalal, 2000). More recent research has found that most of these concerns are unfounded (Gosling *et al.*, 2004) and the use of web-based questionnaires has become accepted in academic research. However there are still some concerns with web-based questionnaires. It is still difficult to attain fully representative samples on the Internet and respondents have to be computer literate. In this study, this was not of concern as full lists were available of the cohorts being studied and the respondents were computer literate and had access to computer facilities. There are also some validity issues particular to web-based questionnaires, such as repeat responders. How this and other validity issues were addressed is discussed in Section 4.7.1.

Group-administered questionnaires are considered a suitable choice for large groups that can easily be brought together, as in students attending a lecture or school students in a school classroom. Each member completes their own questionnaire and returns it to the researcher on completion. One advantage of group-administered questionnaires is that response rates are usually higher than mail or web-based questionnaires. As the researcher is present, respondents can ask for clarification about questions they do not understand. Using group-administered questionnaires also raises some validity issues, such as respondents feeling coerced to participate in the study, see Section 4.7.1 for a discussion of these validity issues.

Hargittai and Hsieh (2010) express a concern that relying on a web-based questionnaire when studying Internet users could potentially create a bias towards people who spend more time online. To account for this bias the questionnaires for the college student cohort were administered online and also in a paper group-administered questionnaire. This allowed for a comparison between the two modes of collection. A full comparative analysis shows that the respondents that completed the web-based questionnaire did indeed

spend more time online but their responses to the other questions were not statistically significantly different.

The adolescent cohort was accessed via schools. Using web-based questionnaires with this cohort proved to be impractical due to parental consent issues and the availability of suitable computer facilities in schools. Group-administered questionnaires were also used for the adolescent student cohort. A web based questionnaire was deemed the best option for the work based adult cohort as a full staff e-mail lists were available.

Design of Questionnaire

As recommended by Dillman *et al.* (2009) a holistic approach was taken to the design of the questionnaire, which meant considering which question structure best measures the concept of interest, how questions are composed of multiple parts and how both the words and visual presentation of questions are important. In the questionnaire most questions used a closed-ended question format with a list of answer choices from which the respondent selected an answer. Some open-ended questions were used to elicit more detailed information from respondents, for example if a respondent had never used a SNSs, asking them to explain why. The paper questionnaire was presented as an A4 booklet. The following section provides an overview of the considerations made in designing the questionnaire. Further details can be found in Appendix I, the final versions of the school student questionnaire are shown in Section I.2.

Visual presentation of questionnaire

Researchers, for example Tourangeau *et al*. (2004) and Christian *et al.* (2007), have examined how the visual design and layout of survey questions can influence how people respond to paper and Internet questionnaires. A number of guidelines, such as using a consistent format throughout the questionnaire, were followed to help respondents to quickly understand the layout and organisation of the questionnaire. These guidelines are shown in Appendix I.

Ordering the questions

As stated by Schwartz (1996), questionnaires should be organised much like a conversation. A number of considerations were implemented in the questionnaire to ensure a logical ordering of questions, see Appendix I.

Constructing the questions

There is a body of research that addresses how the design of open-ended and closed-ended questions can affect responses. The recommendations followed are shown in Appendix I.

Additional considerations for Internet Survey

As the paper based and Internet survey results were going to be compared, the Internet questionnaire was designed to match the paper based questionnaire as closely as possible. The survey was designed and administered using Survey Monkey (http://www.surveymonkey.com). Although Survey Monkey provides limited flexibility for designing web surveys, the application was more than adequate to replicate the paper based survey. As the survey was quite long and in keeping with recommendations for Internet surveys, multiple questions were presented on each WWW page and respondents navigated between multiple pages. A progress bar was also included. As with the paper questionnaire a consistent format was used across each screen of the questionnaire. The Internet survey was tested using a variety of platforms, connection speeds, browsers and the database was tested to ensure that items were collected and coded correctly.

Measures

Figure 4.5 shows the variables measured by the survey method. Where available, pre-existing measures and scales were used in the questionnaire. Using pre-existing scales has the advantage that the scale has been psychometrically tested. The measures used in the final questionnaire are presented in this section. A description of how the measures were adapted and changed based on pretesting and piloting is shown in Appendix J.

Risk Perceptions of SNSs:

Risk factors examined: As stated in Section 3.7, a review of previous studies using the psychometric paradigm of risk perception (with an emphasis on ICT studies and adolescent studies) identified that these studies measured over 45 different risk factors. The final questionnaire examined 7 of these risk factors. Each rating used a 7 point bi-polar scale. Piloting of the questionnaire showed that that the questionnaire took too long to complete when all 7 factors were examined in a single questionnaire. Using a method similar to one applied by Slovic *et al*. (2007b), the questionnaire was split into two questionnaires with respondents randomly assigned to each questionnaire. As it is an important characteristic, the personal risk factor was included in both questionnaires and the remaining risk factors were split as shown in Table 4.3.

Questionnaire Version 1	Questionnaire Version 2
Personal Risk	Personal Risk
Severity/Consequences	Controllability
Risk to peers	Concern
Likelihood of Risk	Knowledge of Risk

Table 4.3 Risk Factors by Questionnaire.

A choice was made to split the questionnaires by risk factor rather than by risk item as it was deemed more useful to examine and rank the responses by risk item rather than by risk factor. An attempt was made to split the risk factors into groupings found in previous studies, for example control and knowledge factored together in studies by Fischhoff *et al*. (1978), Huang (2007) and Gabriel and Nyshadham (2008). This proved difficult as studies present quite different factor groupings and as stated by Slovic (2000b) these factor groupings can be context dependent. Where possible, items were grouped together into homogenous groups.

Risks examined: The choice of risks examined in the questionnaire was derived from the literature and three focus group interviews. Over 20 potential risks with using SNSs were identified. This was shortened to an initial list of 10 risk areas. The risks areas were selected according to several criteria including user concern, prevalence, severity and to show a wide ranging set of risks. At pretesting, two further risk areas were identified and included on the final list; these risks were viruses and spam.

The initial questions about risk characteristics were designed using the wording and scales proposed by Benthin *et al.* (1993) as they had successfully administered their questionnaire to an adolescent sample. All the risk scales were rated in the same direction from 1, not risky to 7 very risky. (See Q24 to Q27 School Questionnaire version 1 & 2, Appendix I)

Experience of Risks:

Respondents were asked to indicate if they had themselves or knew of others that had experienced any of these risks. This was asked as two separate questions (personal experience, knew of others' experience) with a dichotomous yes/no answer. (Q28 & Q29 School Questionnaire).

Access [School Student Questionnaire ONLY]:

Based on a question used in the UK Kids Go Online Survey (Livingstone and Helsper, 2007), school students were asked whether they had supervised access to the Internet. The options were whether they used the Internet: by themselves or with friends, siblings or parents. (Q1, School Questionnaire).

Usage of SNSs:

SNS Sites Used: The questionnaire used a simplified version of a question assessing SNS usage proposed by Hargittai (2007). Respondents were presented with the three most popular SNS sites in Ireland at the time of the study (Bebo, Facebook and MySpace) and were asked if they had ever used these sites, or if they currently used these sites more/less than once a week. They were also given the opportunity to include any other sites they used/use. (Q11, School Questionnaire).

Frequency/Duration of SNS Usage: Many studies that estimate SNS usage use frequency or duration indices to measure intensity of Internet usage (Acquisti and Gross, 2006, EUROBAROMETER, 2007a, Lenhart and Madden, 2007, Anchor, 2008b, OFCOM, 2008, Fogel and Nehmad, 2009, Young and Quan-Haase, 2009, Livingstone *et al.*, 2010b). An alternative scale "*the facebook intensity scale*", developed by Ellison *et al*. (2007) was modified for use in this study. As Facebook is not the only SNS being examined in this study, all references to Facebook were changed to social networking site. The scale contains two-self reported measures of an individual's engagement in SNS activities: the number of SNS "*friends*" an individual has and the amount of time an individual spends on SNS on a typical day. The measure also includes a series of bipolar Likert-scale (1 = strongly disagree to 5 = strongly agree) attitudinal questions designed to measure the extent to which the participant was emotionally connected to SNSs. Examples of items on this scale are "Using a social networking site is part of my everyday activity" and "I feel I am part of the social networking site community" (See Q14, Q15, Q20 (part 1-6), School Questionnaire).

A measure of how often individuals accessed SNSs was also included in the questionnaire. (See Q13, School Questionnaire).

SNS Features Used: Respondents were presented with a list of 6 features of SNS and asked to indicate whether they had ever used these features (using a dichotomous yes/no response). (Q15, School Questionnaire).

Purpose of Use: Respondents were presented with a list of uses of SNS, such as keeping in contact with old friends, sharing information etc. and asked to indicate (using a dichotomous yes/no response) whether they found these features useful or not. An open-ended question allowed respondents to add other useful features. (Q21, School Questionnaire).

Information Placed on SNS: Respondents were asked to select from a list, the type of personal information that they had ever placed on a SNS (using a dichotomous yes/no response), for example name, email address, phone numbers etc. The college students and working adult cohort were given a list of 15 items; two of these items, sexual orientation and relationship status were removed for the school student's questionnaire. An open-ended question was included that asked if respondents had removed any personal information and if so why? (See Q16, Q17 School Questionnaire).

Skills:

IT skill level: Assessing the IT skill level of respondents was based on self-reported measure similar to one used in the UK Kids Go Online Survey (Livingstone and Helsper, 2007). Livingstone and Helsper asked respondents to self-rate how good they were at using the Internet, the categories used were beginner, average, experienced and expert. These categories were re-worded as follows to make them more meaningful for respondents:

- ☐$_1$ I am just finding my feet
- ☐$_2$ I am up and running but there are still things I cannot do
- ☐$_3$ I can do pretty much everything I want to do
- ☐$_4$ I am hot and friends often come to me for computer advice

(Q3, School Questionnaire).

Years using Internet and SNSs: Respondents experience online was also measured by how many years they had been using the Internet and SNSs (Q2 & Q10 School Questionnaire).

Attitudes:

Privacy: IS researchers have often used the construct of privacy concern as the proxy to define and measure the concept of privacy. A number of scales have been developed to measure privacy concern, such as the Westin privacy segmentation scale (Harris_&_Associates and Westin, 1998), the Concern for Information Privacy Scale (CFIP) (Smith *et al.*, 1996), the Internet Users Information Privacy Concerns scale (IUIPC) (Malhotra *et al.*, 2004) and the Internet Privacy Concern Scale (Dinev and Hart, 2004). Some of these scales have been adapted for studies addressing privacy concerns with SNSs (Acquisti and Gross, 2006, Fogel and Nehmad, 2009). The Acquisti and Gross (2006) scale was adapted for use in this study. The scale contained five items measuring privacy concerns on a 7 point bipolar Likert scale. For example, an item in this scale is, ‘‘I am concerned about what social networking sites can know about me”. (See Q30 (part 5-9), School Questionnaire).

As a further indication of respondents attitudes to privacy, a question was included that asked if respondents had ever restricted their privacy settings on a SNSs and if so why? (Q22 & Q23, School Questionnaire).

Trust: A number of studies has investigated trust with respect to SNSs (Acquisti and Gross, 2006, Dwyer *et al.*, 2007, Fogel and Nehmad, 2009). The scales used by Dwyer *et al.* (2007) reported poor reliability scores so were not considered suitable for inclusion in the study. Although Fogel and Nehmad (2009) reported adequate reliability measures for their scale, it proved too awkward to use in this study as a separate four item scale was needed for each SNS. The trust scale devised by Acquisti and Gross (2006) was used in the pilot study. The Cronbach alpha reliability score for this scale in the pilot study was extremely poor (0.390) so an alternative measure was used for the final questionnaire. Gefen’s (2000) disposition to trust scale was used to assess how trusting respondents were in general rather than measuring their trust in a particular technology. This scale measures four trust items such as “I generally trust other people” and is measured on a 7 point bipolar (1 = strongly disagree; 7= strongly agree) Likert scale. A further single item measure was included to measure trust in SNS companies (See Q30 (part 1-4), School Questionnaire).

Identity Information Disclosure: Identity information disclosure was measured using a subscale that measures respondent's views on the access by others to the identity information they have disclosed. This subscale was devised for SNSs by Stutzman (2006). Items are measured on a 5 point bipolar Likert scale (1 = strongly disagree; 5 = strongly agree). A sample item from the subscale includes, ''I am OK with friends accessing my social network communities profile". All references to "social network communities" were changed to "social networking sites". (Q20 (part 7-10), School Questionnaire).

Mediation by Parents [School Student Questionnaire ONLY]:

School students were asked if their parents set rules for using the Internet or SNSs. (See Q4 & Q18, School Questionnaire).

Mediation by Schools [School Student Questionnaire ONLY]:

School students were asked if their school set rules for using the Internet or SNSs. (See Q5 & Q19, School Questionnaire).

Mediation by Peers:

A number of different scales have been used in the IS literature to measure peer and social influence, for example (Davis, 1989a, Ajzen, 1991, Moore and Benbasat, 1991, Thompson *et al.*, 1991, Taylor and Todd, 1995a, Taylor and Todd, 1995b). The Taylor and Todd (1995b) scale was used in this study to measure peer influence, in their initial study the scale had a reliability coefficient of 0.92. The scale was modified to reference SNSs. The scale contains two items "My friends think that I should use social networking sites" and "Generally speaking, I want to do what my friends think I should do". Respondents were asked to rate their level of agreement on a 7 point bipolar Likert scale (1 = strongly disagree and 7 = strongly agree). A further single measurement was included based on the Thomson *et al.* (1991) scale, this item was "I use social networking sites because many of my friends use them", this was also measured on a 7 point bipolar Likert scale. (See Q30 (part 10-12), School Questionnaire).

Demographic Data:

The minimum amount of demographic data was collected in the questionnaires. All respondents were asked for their age and gender, the college students were also asked

for the discipline they studied and the working adult cohort were asked if they had a third level qualification and if so the discipline.

Questionnaire Effect:

A further question was included on the questionnaire which examined if completing the questionnaire had changed respondents opinions about the risks associated with SNSs. This was a modified version of a question used by Furnell *et al*. (2007) in their study assessing security perceptions of Internet users. The question asked users whether completing the questionnaire had changed their opinions about the risks on SNSs. The options presented to the respondents were:

It has made me more worried about the risks	☐$_1$ Yes	☐$_2$ No
It has made me more confident about my own knowledge	☐$_1$ Yes	☐$_2$ No
It has increased my awareness of the risks	☐$_1$ Yes	☐$_2$ No
It has made me realise that I am not aware of some of the risks	☐$_1$ Yes	☐$_2$ No
It has made me realise that I don't protect myself as much as I could	☐$_1$ Yes	☐$_2$ No
I was already aware of these risks	☐$_1$ Yes	☐$_2$ No

(See Q34, School Questionnaire).

Pretesting Questionnaire

A number of different methods, expert reviews, cognitive interviews and pilot testing were used in this study to ensure the content, cognitive and usability standards of the survey.

Expert reviews:

The draft survey questions were first evaluated by a number of subject matter experts and questionnaire design experts. These experts were consulted independently. The questionnaire design experts assessed whether the questions met the content, cognitive and usability standards, by reviewing the wording of the questions, the structure of the questions, the response alternatives and the order of the questions. The subject matter experts reviewed the questions to assess whether their content was appropriate for measuring the intended concepts. The subject matter experts included college lecturers, college students, working adults, school teachers and parents of adolescents. These expert reviews led to many changes to the draft questionnaire with regard to layout, wording and structuring of questions.

Cognitive interviews:

After the expert reviews, the questionnaire was redrafted and cognitive interviews were carried out with a number of younger adolescents (11-12 year olds). Cognitive interviews are used as a way to determine whether respondents understand questions in the way the researcher intended. The cognitive interviews were carried out as individual interviews where the adolescent was asked to think out loud as they went through the draft questionnaire. These cognitive interviews highlighted a number of questions where the adolescents had difficulty understanding their meaning. Based on recommendations from the cognitive interviews, the wording of these questions was simplified. Cognitive interviews were not carried out with the college or adult cohorts due to time and resource constraints and as it was felt that these cohorts were educated literate adults that should not have any difficulty in understanding the questions posed in the questionnaire.

Pilot study:

After the expert review and cognitive interviews, pilot studies were carried out with a college student cohort (n = 47) and a school student (n=37) cohort. This evaluated interconnections among questions, the questionnaire and the implementation process. After completing the questionnaire, all respondents were asked for comments on the questionnaire, such as how long it took to complete and how difficult it was to complete. A copy of the comment sheet respondents were asked to fill in is shown in Appendix K. The questionnaire data was analysed to assess how questions were answered and if particular response categories were not used. This analysis also gave an indication of whether individual questions and scales were working as intended. Further changes were made to the questionnaire based on the findings from these pilot studies.

It is recognised that each of these pretesting methods has limitations. Expert reviews are only as good as the experts selected. Cognitive interviews are time consuming and thus the sample interviewed was small and cannot be thought of as a random sample of the larger population being studied. The pilot studies were restricted in how much the researcher could probe and understand the problems that respondents face. However the different techniques do complement each other and provide information related to different issues. In this study the techniques were combined to take advantage of the strengths of each method.

4.4.2 Focus Group Design

This section describes the decisions made in designing the focus groups.

Group Structure

As discussed in Section 4.3.3., focus groups were utilised in two ways in this research, firstly to help develop the content of the survey and secondly with the adolescent cohort of this study as a follow up to help interpret the survey results. In both cases a structured questioning and moderator involvement strategy was adopted. This strategy allowed for direct comparisons of discussions from group to group. The use of a structured questioning route and a higher level of moderator involvement ensured that the discussion concentrated on the topic of interest to the research.

Designing the Questioning Route

The questions for both focus groups were designed, as suggested by Krueger and Casey (2000), to be conversational (using simple language and words the participants would use), to be clear and concise and open ended to encourage discussion amongst participants. To ensure that the questions naturally flow from one question to another and move from general questions to more specific questions (which are of more importance to the study), as recommended by Krueger and Casey (2000), a questioning route with five categories of questions: opening; introductory; transition; key and ending was designed. Details of this questioning route are shown in Appendix L, Table L.1.

The questioning route designed for the adolescent focus group is shown in Appendix L, Table L2. Care was taken to word the questions in a way that was suitable for adolescents. Activities were incorporated into the design to ensure that the adolescents remained engaged. As recommended by Kreuger and Casey (2000) fewer questions were asked and more time was spent at the start of the focus group getting the participants comfortable and talking.

Care was exercised in the focus groups to avoid adhering rigidly to fixed questions, variations were allowed in the questioning route to accommodate the unique aspects of each group.

Sampling

The next step in the focus group design process was to decide on the types of respondents that would be able to provide the information required in the study. As stated by Patton (2002) this can be thought of as identifying the "*information-rich*" cases for study in depth. He states that "*information-rich cases are those from which one can learn a great deal about issues of central importance to the purpose of the research*" (Patton, 2002, p46). At the time of the study, the predominant age groups that used the more popular SNSs in Ireland, such as Bebo and Facebook, were 14-17 year olds and 18-24 year olds. For the developing the survey focus group, it was felt that sophister undergraduate students would be a suitable cohort as they would have had adequate experience with SNSs. These focus groups were not segmented by gender as it was felt that students of this age would not have difficulties in expressing their opinions in front of the opposite sex. The samples were recruited using convenience sampling due to ease of access and cost implications for the researcher. The undergraduate students were third and fourth year students taking a degree course in Trinity College Dublin. Full class lists were e-mailed to request participation in the study. The focus groups were held at the university. As this part of study was exploratory and would be followed by a more rigorous study, it was felt that these groups were a good source of information and could provide useful input to the next stage of the research design.

For the adolescent focus groups, it is recommended that the participants be no more than 2 years apart in age (Vaughn *et al.*, 1996, Krueger and Casey, 2000), as levels of comprehension and abstraction differ substantially at different ages (Kennedy *et al.*, 2001). It was decided to segment the school students into two age groups, 2nd year students (13-14) and transition year students (15-16). Some researchers suggest segmenting focus groups with adolescents by gender, particularly as boys are more active (Krueger and Casey, 2000). Thus the focus groups were run in one girls school and one boys school in the Dublin area. These students had already completed the survey and had expressed an interest in being involved in the focus groups. The focus groups were selected from within class groups. Assistance was sought from teachers in selecting the most suitable students for the focus group. An additional benefit of selecting focus groups from within a existing class is that the students knew each other and should be comfortable with each other and thus little time had to be invested in developing a new group dynamic (Davies, 1999).

Group Size

For the developing the survey focus group, breadth of understanding of the risks involved in SNS was considered important, so a group size of 6-7 was chosen. As the target group were articulate undergraduate students, it was felt that a larger group would be too difficult to control. For the interpreting the adolescent survey focus group, the aim of this focus group was to gain an in-depth understanding and explanation of particular issues raised by the survey, so a smaller focus group size of 5 was deemed appropriate. In both instances a choice was made to over-recruit by 20% to cater for no-shows.

Number of Groups

For the developing the survey focus group, initially, three focus groups were run sequentially, using a single category design. As saturation had been achieved no further focus groups were carried out. Saturation describes the point at which no new ideas or information is being generated.

A multiple-category design was used for the adolescent focus group. Two focus groups were carried out with the two different audiences (younger adolescents and older adolescents). These focus groups were carried out sequentially. This design allowed comparisons to be made in two ways – from one group to another within a category (younger adolescents) and from one category to another category (e.g. comparing what younger adolescents said to what older adolescents said).

4.4.3 Interview Design

This section describes the decisions made in designing the qualitative interviews.

Designing the Interview

An interview guide was prepared to help structure the interviews. A key consideration was to develop a guide that would enable the interviewer to guide the general direction and flow of the interview, while letting the interviewee freely express their opinions. Apart from the background questions assessing an interviewee's use of SNSs, a choice was made to allow unstructured responses which allow interviewees to answer in whatever way they choose.

A number of considerations were made regarding the sequence and framing of the interview questions. To help put interviewees at their ease, the easier '*what*' and less threatening questions were placed earlier in the interview guide (Patton, 2002). In framing the questions for the interview guide, *prompts* and *probes* were also used (Cohen *et al.*, 2007). Prompts allow the interviewer to clarify topics or answers, probes enable the interviewer to ask interviewees to extend and elaborate on their responses. The interview guide was not over prepared in order to encourage flexibility and improvisation (Myers and Newman, 2007). The interview guide, including probes, is shown in Appendix M, Table M.1.

Sampling

The next step in the interview design process was to decide on the types of respondents that would be able to provide the information required in the study. As the semi-structured interviews were being carried out to help explain findings from the survey, it was decided that the same individuals should be included in both data collections. E-mails were sent to the sampling frame used for the survey, explaining what was involved for the student and asking if they would be involved in the second part of the study.

Number of Interviews

Kvale and Brinkmann (2009), suggest that commonly in interview studies the number of interviews tends to be around 15 ± 10. They recommend that researchers should "*interview as many subjects as necessary to find out what you need to know*" (p113). Following this advice, interviews were carried out until a saturation point had been achieved. 15 university students were interviewed individually about their perceptions of the risks on SNSs.

4.5 Administration

4.5.1 Survey Administration

The Tailored Design Method (Dillman *et al.*, 2009), was used to increase response rates for the questionnaires. The Tailored Design Method is based on social exchange theory. Three elements are central in social exchange theory:

1. How can the perceived rewards for responding be increased?
2. How can the perceived costs of responding be reduced?
3. How can trust be established so that people believe the rewards will outweigh the costs of responding?

The *rewards* offered were psychological rather than material/monetary. Respondents were made to feel that they were important for the study and that their particular opinions were needed. The questionnaire was made to look interesting and pleasant to respond to. Respondents were explicitly thanked after completing the questionnaire. As a reward, respondents were given a summary of the results. The *cost* in effort and time for respondents was minimised. The questionnaire was designed to be easy to complete and respondents were informed how long it would take to complete. Requests for personal information were minimised. To engender *trust*, the covering letter and participant information sheets used the official letterhead of the University. Contact information for the researcher was included. For the web-based questionnaire, these details were included in the covering e-mail. For the group administered questionnaires, these details were included on the participant information sheet and also verbally explained by the researcher.

This section describes the how the questionnaires were administered.

<u>Web-based questionnaires</u>

The questionnaires were administered by e-mail, using an undergraduate college e-mail list for the college cohort and a work e-mail list for the working adult cohort. The URL of the questionnaire was included in the covering email. A follow-up e-mail was sent out to the full list two days after emailing the questionnaire. This email thanked early respondents and reminded non-respondents to answer the questionnaire. The e-mails were sent out

mid-week. The college student web-based questionnaires were sent out in April 2009. The working adult web-based questionnaires were administered in September 2009.

Group-administered questionnaires

As stated in Section 4.4.1 the group-administered questionnaires were administered to large groups with the researcher present to deliver the introduction, to clarify problems and to assist in the survey process. For the college student cohort, a lecturer was contacted for each group selected for the sample. In all cases the lecturer agreed to have the questionnaires administered during one of their lecture slots. The questionnaires took about 20 minutes to complete. The questionnaires were administered in April 2009.

For the schools, head teachers were contacted and sent details of what was involved for the school in taking part in the study. When head teachers agreed to take part in the study, students were given information leaflets explaining the study and consent forms that had to be pre-signed by parents. In most schools these consent forms were collected by teachers. The questionnaires were administered by the researcher at dates and times agreed with the school. Younger adolescents took a full timetabled class slot (40 minutes) to complete the questionnaire and older adolescents took about 20 minutes. The questionnaires were administered from November 2009 to April 2010. The time from gaining access to schools to administering the questionnaire was much longer than anticipated.

4.5.2 Focus Group Administration

This section describes how the focus groups were conducted.

Site Selection

For the developing the survey focus group, the sample selected was sophister undergraduate students. The focus groups were held at the university in a conference room, with a rectangular conference table. For the adolescent focus group, the samples selected were from two different schools. These focus groups were held at each school using free classrooms. The desks in the classroom were re-arranged into a rectangular conference table layout. The moderator sat at one end of the table, creating a U shaped arrangement for the participants. This gave the moderator a good facial view of all the participants. This table layout also provides a protective barrier between group members

that gives more reserved members of the group a sense of security and helps establish a sense of personal space that makes participants more comfortable (Stewart *et al.*, 2007).

Timing

For the developing the survey, focus group, the focus groups were carried out over lunch times. The focus groups were an hour in duration. Light lunch was provided. For focus groups with adolescents, Kreuger and Casey (2000) suggest reducing the time allotted to the focus groups. As school students change classes every 40 minutes, it was deemed appropriate to choose a 40 minute slot for the adolescent focus group.

Role of Moderator

For the moderator, an objective, distanced interviewing style was chosen as opposed to a more intimate approach. The danger with an intimate approach is that when the moderator becomes a participating member of the group, the group tries to provide the answers that they think the interviewer wants (Stewart *et al.*, 2007). The moderator maintained an objective role was by restricting head nodding, as this may signal agreement, and care was taken not to signal approval by using responses such as "*correct*", "*good comment*" or "*excellent*".

Research indicates that the choice of moderator is critical for adolescent focus groups. Stewart *et al.* (2007) contend that groups of girls are more comfortable with a female moderator, and groups of boys are comfortable with a female interviewer, but will talk more openly about certain topics with a male moderator. It is also important that the moderator is comfortable and experienced with children. Kreuger and Casey (2000) suggest recruiting a moderator that is comfortable with children such as a teacher, youth worker or scout volunteer. Due to financial constraints it was not possible to recruit external moderators.

The moderator introduction for the adolescent focus group is important for setting the tone of the discussion. As stated by Vaughn *et al*. (1996), adolescents may not fully comprehend the research behind the focus group, but are more likely to actively participate in a research project when they feel their individual experiences are valued by others. Care was taken to ensure that the introduction was written in language suitable for adolescents and their role in the discussion was made clear. The moderator introduction for the adolescent focus group is shown in Appendix L, Section L3.

Data Collection

The focus groups were recorded on a digital voice recorder. Videotaping was not considered as it is difficult to set up and can be quite intrusive for participants. Permission was sought from all group members before recording took place. Verbatim transcriptions were made of the digital recordings. To enrich the transcriptions notes, other observations were included about the group dynamic; the mood of speakers; any interruptions and pauses and silences.

4.5.3 Interview Administration

This section describes how the qualitative interviews were conducted and transcribed.

Site Selection & Timing

The semi-structured interviews were arranged at times and venues that were convenient for the students. All students chose to hold the interviews in the researcher's office. Interviews lasted between 25 and 60 minutes.

Role of Interviewer

Each interview started with some small talk to put the interviewee at ease. In order to make the interviewee aware of what will happen during and after the interview (Cohen *et al.*, 2007), a participant information sheet (Appendix H) was given to interviewees that explained the purpose, nature and scope of the interview and also any confidentiality and ethical considerations. Interviewees were also informed that there were no right or wrong answers. The interviewer was conscious to restrict comments or gestures that would bias the discussion and to allow interviewees time express their opinions, to listen attentively and to be seen to enjoy and value the interview.

Data Collection

Like the focus groups, a digital voice recorder was used for recording the interviews. Permission was sought from all interviewees before recording took place.

Some observations were noted beside the questions during the interviews. Immediately following each interviews, as suggested by Patton (2002) and Rubin & Rubin (2005), a postinterview review was carried out. The details recorded were:

- Location of interview;
- The date and time;
- Background information about the respondent (e.g. gender, discipline, age);
- How the interviewee reacted to questions;
- How well the interviewer asked questions;
- How was the rapport?

This postinterview review allowed for reflection on the quality of each interview showing areas where the interviewer could improve and where the interview process could be changed.

Transcribing

Verbatim transcriptions were made of the digital recordings. Other observations included the tone of voice of the interviewee; any interruptions and pauses and silences.

4.6 Data Analysis

4.6.1 Survey

Before data analysis could begin the open-ended questions needed to be coded, the data entered and edit checks carried out. Each of these steps is described below.

Coding

All open-ended textual answers in the questionnaire needed to be coded into numeric data. A code structure was devised for each question. In the code structure, each code was given a unique number and a text label that fully described the category. The code structure was designed so that all responses could be assigned to a category and that no response could be assigned to more than one category.

Data Entry

The data was automatically collected for the web-based questionnaires. For the paper-based questionnaires, data was entered into a spreadsheet file keying the digits one by one. Punch and verify (100% rekeying and verification of entries) was too costly so every 10^{th} questionnaire was re-checked.

Data Editing

Data editing is the inspection and alteration of data prior to statistical analysis. A number of checks were carried out on the data. Range edits were carried out on variables such as age to ensure that suitable ages were entered, for example in the adolescent surveys the age range should be between 12 and 17. Consistency edits checked for example that the age respondents started using the Internet was less than or equal to the age that respondents started using SNSs. Surveys that were less that 75% complete were removed from the analysis.

Data Analysis

The data was analysed using SPSS 16.0 for Windows (release 16.0.1) & PASW Statistics 18, (release 18.0.0). Numerous statistical techniques were applied in this analysis. Mean values for continuous variables were compared using t tests, one way analysis of variance and MANOVA. For categorical variables, differences in the distribution of variables were estimated using χ^2 analysis. Log linear analysis was used to investigate relationships between multiple categorical variables. The assumptions underlying these statistical tests were checked.

4.6.2 Interview and Focus Group Discussion

In order to ensure analytical rigour when analysing the interview data, some of the guidelines proposed by Hycner (1985) for the phenomenological analysis of interview data were followed in the qualitative analysis. These include:

1. *Transcription*: as stated the interview and focus group tapes were transcribed, noting not only the literal statements but also other non-verbal communications.
2. *Bracketing and phenomenological reduction*: this means suspending or bracketing as much as possible the researchers meanings and interpretations and approaching the

recordings and transcriptions with openness. In this the researcher aims to understand what the interviewee is saying rather than what the researcher expects the person to say.

3. *Listening to the interview for a sense of the whole*: tapes were listened to several times and transcriptions were re-read a number of times.
4. *Delineating units of general meaning*: this involved an examination of both verbal and non-verbal gestures to elicit the interviewees meaning.
5. *Delineating units of meaning relevant to the research question*: once the units of general meaning were noted they were then reduced to units of meaning relevant to the research question. This determines if what the interviewee has said responds to and illuminates the research question.
6. *Clustering units of relevant meaning*: this involved assessing whether there seemed to be some common theme or essence that united several discrete units of relevance meaning.
7. *Writing a summary of each individual interview*: each interview was summarised incorporating the themes that were elicited from the data.
8. *Identifying general and unique themes for all the interviews*: themes were identified that were common to most or all of the interviews. These themes from the individual interviews were clustered together to indicate a general theme that emerged in most or all of the interviews.

4.6.3 Organising and Presenting Data Analysis

The analysis is organised by research question. In this approach all the relevant data from the various data sources (interviews, focus groups and questionnaires) are collated to provide a collective answer to a research question. The numerical data for a particular research question is presented, followed by the qualitative data. This allows patterns, relationships and comparisons across data types to be explored conveniently.

4.7 Credibility of Research Methodology

The steps taken to check the accuracy and credibility of findings are addressed in this section.

4.7.1 Evaluating Quantitative Research

Surveys rely on two types of inference – from the questions to constructs and from the sample statistics to the population statistics. Each of these steps is subject to imperfections, producing statistical errors in survey statistics (Groves *et al.*, 2004). The errors between the measures and the construct are issues of validity. The errors during application of the measures are called measurement errors. Editing and processing errors can arise during the preparation of the data for statistical analysis. Coverage errors arise when the sampling frame fails to cover all aspects of the target population. Sampling errors occur because surveys only measure a subset of the frame population. The failure to measure all sample persons on all measures creates nonresponse error. A perfect survey would minimise all these sources of error and the methodological survey literature suggests a variety of methods of reducing survey error. However, in a study such as this where resources are limited, it is not possible to minimise all sources of error and some compromises have to be made. The following section describes how each of these errors was addressed in this study:

Validity

Validity can be defined as the extent to which the survey measure accurately reflects the intended construct. As described in Section 4.4.1, where possible existing psychometrically tested scales were used in this study, so validity for many of the scales used in this study have already been assessed. To confirm that the measures were applicable in an Irish context and were suitable for the age cohorts being tested, some further validity checks were made.

Face Validity: this concerns the acceptability of a test to the test taker. This was assessed by the subject matter expert reviews, cognitive interviews with younger participants and the pilot studies (see Section 4.4.1). Respondents in the pilot study were asked to complete a short commentary questionnaire which covered validity questions such as the length and

comprehensiveness of the questionnaire and to highlight any questions they had difficulty understanding.

Content validity: establishes whether the measure covers the full range of the concepts meaning. This was determined a priori by soliciting the opinions of experts and carrying out a comprehensive review of the literature to identify the different aspects and dimensions of the concept.

As new scales were not being developed for this study, further methods of assessing validity, such as criterion and construct validity were deemed unnecessary for this study.

Measurement error

Groves *et al.* (2004) define measurement error as a departure from the true value of the measurement. One aspect of measurement error is *response bias* which is a systematic and consistent overestimation or underestimation of the construct in question. The wording and structure of questions can lead to response bias. Care was taken to ensure that questions were clear, precise and relatively short. Leading questions were avoided and both sides of scales were included, for example "*To what extent do you agree/disagree with these statements*?" Double-barrelled questions, where two or more issues were addressed in the same question, were avoided. Further discussion on the design of the questionnaire can be found in Appendix I.

Another example of response bias is *response set bias*. This is the tendency for a respondent to answer a series of questions in a certain direction regardless of their content. This bias occurs, typically in longer surveys, when fatigue or lack of interest sets in. To help counteract this bias, the critical questions on risk perception were moved to the middle of the survey to ensure respondents were still alert when they were filling in these questions. All responses were checked for evidence of this bias and where indicated the responses were removed.

One way that respondents can contribute to measurement error is by *socially desirable responses*. Most people like to present themselves in a favourable light so are reluctant to admit to negative behaviours in a survey. It is difficult to control for this bias, but to encourage respondents to answer honestly, respondents were informed that the survey was anonymous and confidentiality was assured for all responses. In the group-administered

questionnaire respondents were encouraged by the researcher to answer as honestly as possible.

The method of data collection can present a source of measurement error (de Leeuw *et al.*, 2008). The anonymity of the Internet can pose a problem for web-based questionnaires, as individuals can complete the questionnaire multiple times (repeat responders). The software used for hosting the survey (surveymonkey.com) could restrict that only one response is sent from each IP address, this option was not viable as a number of separate respondents could potentially use the same IP address (e.g. those who filled in the questionnaire in public access computer rooms). As suggested by Johnson (2005), consecutive entries in the entire set of item responses were compared to identify duplicate or near-duplicate entries. As no incentives were offered for completing the questionnaire and the questionnaire was long, it was felt that repeat responding was not of great concern and no further precautions were taken. Another issue with web-based questionnaires is partially completed questionnaires; questionnaires that were less that 75% complete were removed from the analysis.

With group-administered questionnaires, care needs to be taken to ensure that the researcher does not make comments that might bias answers that could vary between the different groups taking the questionnaire. A standard introductory statement was read to each group that expressed appreciation for their participation, explained the purpose of the study, described the questionnaire, emphasised the anonymity of the questionnaire, that it was not a test and encouraged participants to answer as honestly and completely as possible. All participants were also given a participant information leaflet explaining the study in detail, see Appendix H. A further concern with group-administered surveys is the possibility that respondents will feel coerced to participate. To help alleviate this, the researcher assured respondents that their participation was voluntary and they were given an opportunity to ask questions about the survey.

Another aspect of measurement error is *reliability*, this addresses whether the questionnaire is measuring constructs consistently either across occasions or across items designed to measure the same construct. As previously published scales are being used in this study, reliability indices have already been established. Reliability indices were calculated (using Cronbach's Alpha) for all the measures used in this study and compared to the original

reliability measures to ensure that the scales were consistently measuring constructs in this study (see Table 4.4 below).

		Current study		
Construct	**Original Study**	**Adolescent Cohort**	**College Student Cohort**	**Working Adult Cohort**
SNS Intensity Scale (Ellison *et al.*, 2007)	0.83	0.85	0.91	0.92
Privacy Concern Scale (Acquisti and Gross, 2006)		0.91	0.93	0.94
Disposition to Trust Scale (Gefen, 2000)	0.85	0.76	0.81	0.83
Identity Information Disclosure Scale (Stutzman, 2006)	0.82 (Fogel and Nehmad, 2009)	0.42	0.73	0.85
Peer Influence Scale (Taylor and Todd, 1995b)	0.92	0.39	0.44	0.13

Table 4.4 Reliability Indices (cronbach's α) for Original Studies and Current Study.

The SNS intensity scale, privacy concern scale and disposition to trust scale as used in this study all prove to be reliable measurements. However the Cronbach's Alpha reliability index indicates that the identity information disclosure scale is not a reliable measure for the adolescent age cohort and that the peer influence scale is not a reliable measure for any of the age cohorts. The latter finding is surprising as this is a commonly used scale in many IS studies.

Processing error:

Groves *et al.* (2004) define processing errors as those that can be introduced after the data are collected and prior to estimation. Processing error can arise in the *coding* of open-ended questions. This is the translation of non-numeric material into numeric data. Coding can be subjective and different coders may make different judgements about how to classify the text. To help avoid coding errors, as stated in Section 4.6.1, a coding structure was developed for all open-ended questions. As the researcher coded all the open-ended questions, coder variance was minimised.

Coverage Error

Coverage errors arise when the sampling frame fails to cover all aspects of the target population. For the school and College samples, theoretically coverage error is not issue as the sampling frames (i.e. list of all schools in Dublin and email list of all undergraduate students) fully represent the sampled populations. For the adult cohort, the target sample is all adults in Ireland and specifically the Dublin area. As stated, gaining access to a suitable sampling frame for adults is difficult. To overcome this difficulty, a decision was made to survey working adults. A list was constructed of a broad spectrum of large Dublin based businesses, both public and private sector, thus undercoverage is an issue as there are elements of the target population, such as non-working adults, that do not appear in the sampling frame.

Nonresponse Error

Nonresponse describes the failure to obtain measurements on sampled units. Unit nonresponse error occurs in this study at two levels. At the first level unit nonresponse is evident due to the difficulty and feasibility of accessing schools, college classes and workplaces selected as part of the initial sample. Unit nonresponse also occurs at the institutional level with regard to some respondents being unwilling to participate in the study or absent on the day that the survey was administered. Table 4.5 – 4.7 show the response rates for the school, college and workplace samples respectively. Item nonresponse was also evident for the questionnaire.

	Sample Size	**Response**	**Response Rate**
School1	120	106	88%
School2	125	56	45%
School3	100	77	77%
School4	120	77	64%
School5	170	125	73%
School6	150	116	77%
TOTAL	**785**	**557**	**71%**

Table 4.5 Response Rates in Schools.

	Sample Size	**Response**	**Response Rate**
Group Survey	1,245	539	43%
Online Survey	9,172	683	7%
TOTAL	**10,417**	**1,222**	**12%**

Table 4.6 Response Rates to College Surveys.

	Sample Size	**Response**	**Response Rate**
Online Survey	1300	127	10%

Table 4.7 Response Rates to Workplace Survey.

As stated in section 4.5.1, the Tailored Design Method (Dillman *et al.*, 2009) was used to increase unit and item response rates for the questionnaires. To further increase response rates, questionnaires were administered in group settings, however this was not feasible for all sample populations.

Demographic information about non-responders was not available; therefore it is not possible to know whether a bias exists in regards to survey participation. The demographics of this sample are compared to population information available on the gender breakdown of post primary school students (Department of Education and Skills, 2010), the undergraduate population as a whole (HEA, 2009) and working adults (CSO, 2009), see Table 4.8. This shows that in this study females are overrepresented and males are underrepresented in both the school and workplace sample. The gender breakdown of the college sample is representative of the entire university population.

	Study Demographics (% male, % female)	**Demographics (% male, % female)**
School	(42%, 58%)	(49%, 51%)
College	(42%, 58%)	(41%, 59%)
Workplace	(44%, 56%)	(55%, 45%)

Table 4.8 Comparison of Study Demographics to Population Demographics

4.7.2 Evaluating Qualitative Research

The problem of how to evaluate qualitative research is a contentious issue. Some authors evaluate qualitative research using the traditional criteria applied to quantitative studies: reliability, validity and generalisability. Other authors have suggested that qualitative research cannot be evaluated in this way and have suggested other criteria (Lincoln and Guba, 1985, Rubin and Rubin, 2005). For example, Lincoln and Guba (1985) substituted reliability and validity with the parallel concept of "*trustworthiness*," containing four aspects: credibility, transferability, dependability, and confirmability. Lincoln and Guba compared these criteria to those used in quantitative research, as shown in Table 4.9

Quantitative terms	**Naturalistic terms**
internal validity	credibility
external validity	transferability
reliability	dependability
objectivity	confirmability

Table 4.9 Comparison of Criteria for Judging the Quality of Quantitative vs. Qualitative Research. (Lincoln and Guba, 1985, p300)

Some authors (Yin, 2003, Morse *et al.*, 2008, Kvale and Brinkmann, 2009) argue that the concepts of reliability and validity can be used regardless of the research paradigm that is pursued and assert that nothing is gained by renaming these concepts or developing new ones. Morse (1999) contends that researchers that do not use these concepts have inadvertently fostered the notion that qualitative research is unreliable and invalid, is lacking in rigor and is unscientific. For the purposes of this study, the traditional terms of reliability, validity and external validity/generalisability are used.

Qualitative Internal Validity

In discussions about evaluating qualitative research, internal validity had received the most attention (Flick, 2006). Qualitative validity is based on determining whether the research findings are accurate from the standpoint of the researcher, the participant and the readers of the research (Creswell and Miller, 2000). The following strategies were adopted in this study to ensure validity:

1. Triangulation: different data sources (quantitative survey & qualitative focus groups and interviews) were examined to build a coherent justification for themes.
2. Construct validity: interview guides were used for the qualitative elements of this study (see Appendix L & M). These guides were based on the constructs used in the survey instrument, but the interview guides were structured to have a stronger qualitative focus by using open-ended questions. In order to ensure clarity of structure and avoid language misunderstandings these interview guides were pre-tested by a number of academics and emerging adults. Minor adjustments were made as a result of these pre-test findings (face validity).

Qualitative External Validity

In qualitative research, external validity refers to the ability to generalise findings across different settings. There is a commonly held view that it is not possible to make generalisations about a larger population when qualitative research is based on a small unrepresentative number of cases (Saunders *et al.*, 2007). Some authors argue that generalisations of qualitative research can be made for example when it is possible to relate research projects to existing theory and thus show a broader theoretical significance (Yin, 2003) and by utilising better sampling methods (Silverman, 2006).

As the qualitative research used in this study was primarily used to confirm and explain quantitative findings from a larger more representative study, the generalisation of qualitative findings was not of particular concern.

Qualitative Reliability

In qualitative research, reliability is concerned with whether the researchers approach is consistent across different researchers and different projects. It deals with replicability. As a single researcher carried out all the interviews/focus groups, reliability concerns concentrated on minimising biases between respondents. A number of procedures have been adopted in this thesis, as suggested by Silverman (2006) and Creswell (2009) to help improve reliability:

1. Potential errors and biases were minimised by ensuring that all interviewees followed the same semi-structured interview or focus group guide to ensure consistency across interviews and focus groups. All interviews and focus groups followed the same interview/focus group protocol.
2. Interviews and focus groups were recorded and fully transcribed.
3. Transcripts were double checked to ensure that mistakes were not made during transcription.
4. A consistent coding convention was used.
5. Cross checking of codes was carried out. A number of passages of text were selected and coded by another coder.
6. As recommended by Silverman (2006) the qualitative research process was made "*transparent*" and is described in detail in Sections 4.3.3, 4.3.4, 4.4.2, 4.4.3, 4.5.2, 4.5.3 and 4.6.2.

Objectivity

In qualitative research it is important to recognise that a researchers values and experience can influence the conduct and conclusions of a study (Maxwell, 2005). This '*interviewer bias*' can be reflected through the questions asked and how responses are interpreted (Saunders *et al.*, 2007). It is important for researchers to self-disclose their assumptions, beliefs and biases that may shape their inquiry (Creswell and Miller, 2000, Creswell, 2009). The researchers biases are acknowledged in Section 4.3.2.

There can also be '*interviewee*' or '*response bias*', this bias may be caused by perceptions about the interviewer. Taking part in an interview is an intrusive process and can introduce a number of interview biases, such as interviewees withholding information; interviewees being reluctant to reveal sensitive information, interviewees only providing partial answers and interviewees aiming to cast themselves in a '*socially desirable'* role (Saunders *et al.*, 2007). To reduce this bias, interviewees were informed at the start of interviews and focus groups that their comments would be kept confidential, there were no right or wrong answers and they were encouraged to be as honest as possible (See Appendix L & M).

Bias can also result from the participants who agree to take part in the study. Care was taken in sampling for the qualitative interviews to ensure that varying levels of SNS users and non-users were selected, gender and technical skills were also considered. In the adolescent focus group interviews age and gender balance was addressed.

4.8 Summary

This chapter has explained the methodology as well as the philosophical considerations underlying the methods chosen to undertake this research. The ontological and epistemological position of this research combines characteristics of positivism and interpretivism. The research follows a mixed methods sequential explanatory research design. This chapter demonstrates that a survey methodology is the most suitable and efficient approach to study users risk perception on SNSs, complemented by interviews and focus groups to provide a deeper insight into the findings. The procedures adopted for the design, collection and analysis of both the quantitative and qualitative phases are outlined. The final section addresses the credibility of the research methods used in this study.

5. Analysis and Findings

5.1 Introduction

The chapter presents the main results and findings of the research. This chapter begins by presenting demographic details of the sample. Following this background information on respondents use and behaviour on SNSs is presented. This is followed by an analysis of risk perceptions on SNSs and a detailed examination of the factors that contribute to high personal risk perception. The final sections examine unrealistic optimism and questionnaire effect.

Both the quantitative survey findings and the qualitative findings of the focus group discussions and in-depth interview are presented. Unless stated otherwise, ** indicates statistical significance levels of $p < 0.001$, * indicates $p < 0.005$. Direct quotations from the qualitative interviews are included to illustrate points. To aid readability, unnecessary text is shaded.

5.2 Demographic Data

The sample data is divided into 4 age cohorts for ease of interpretation:

1. Adolescent aged 12-14;
2. Adolescent aged 15-17;
3. Emerging Adults aged 18-25;
4. Adults aged 26+.

The gender breakdown and descriptive statistics for age are presented in Table 5.1.

Demographic	**Female** % (N)	**Male** % (N)	**Age** Mean ± SD (N)
Adolescent (12 – 14)	59.8% (177)	40.2% (119)	13.3 ± 0.65 (296)
Adolescent (15 – 17)	56.9% (145)	43.1% (110)	15.7 ± 0.67 (255)
Emerging Adult	57.6% (607)	42.4% (447)	20.2 ± 1.47 (1044)
Adult	60.5% (95)	39.5% (62)	[1]33.5 ± 7.80 (156)
TOTAL	58.1% (1024)	41.9% (738)	

[1]Converted from ordinal scales using mid-point of response category (e.g., 20-25 = 23)

Table 5.1 Demographic Details by Sample Cohort

Respondent's level of experience using the Internet is measured as low, medium and high. A low self-rating indicates users that can use the Internet, but there are still things they cannot do. A medium self-rating represents users that can do pretty much everything they want to do, while a high self-rating represents those users that are expert that others come to for advice. Chart 5.1 shows a bar chart of Internet experience broken down by age cohort and gender.

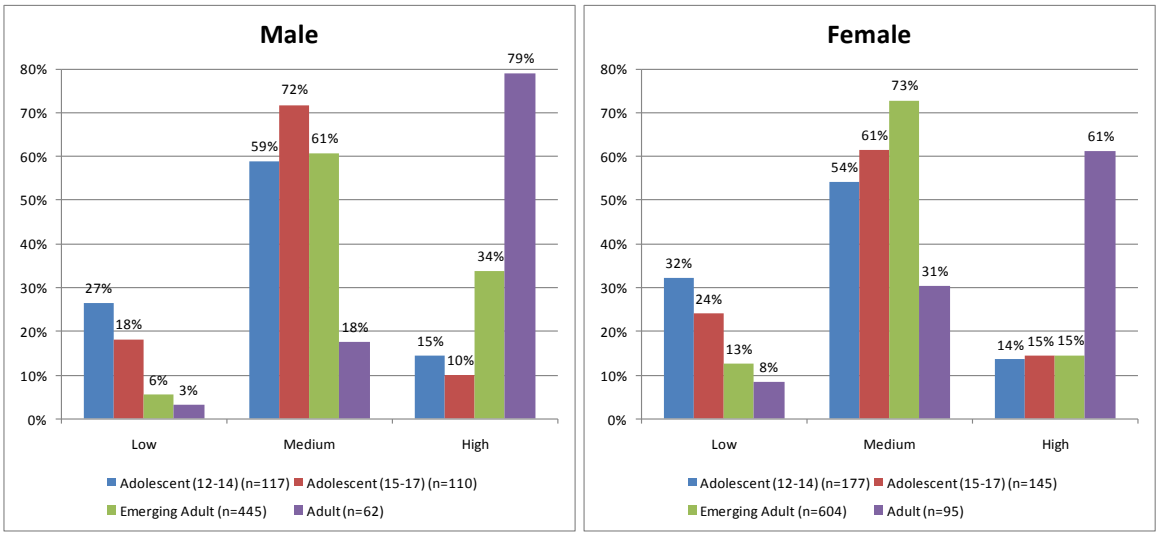


Chart 5.1 Internet Experience by Age Cohort and Gender

A three-way loglinear analysis produces a final model that retains all effects. The likelihood ratio of this model is $\chi^2(0) = 0$, p=1. This indicates that the highest-order interaction (Internet experience x age cohort x gender) is significant, $\chi^2=21.287$, df=6, p= 0.002. Chart 5.1 shows that males in the emerging adult and adult cohorts rate themselves as having higher levels of Internet experience when compared to females in the same age cohorts. Adult males are 2.4 times more likely to rate themselves as experienced Internet users compared to adult females and emerging adult males are 3 times more likely to rate themselves as experienced Internet users compared to emerging adult females.

5.3 Use and Behaviour on SNSs

This section provides some background information on respondents use and behaviour on SNSs. This includes the SNSs currently use, the frequency of SNS use, the features commonly use and the primary reasons for using SNSs. This is followed by a description of the information respondents reveal on SNSs and their privacy settings. Respondents' privacy and trusting beliefs and peer influence are also described. The final section describes respondent's experience of specific risks on SNSs.

5.3.1 SNS Use

This section examines whether respondents currently use SNSs and which sites are most commonly use. The profile of respondents who have never use SNSs is also examined.

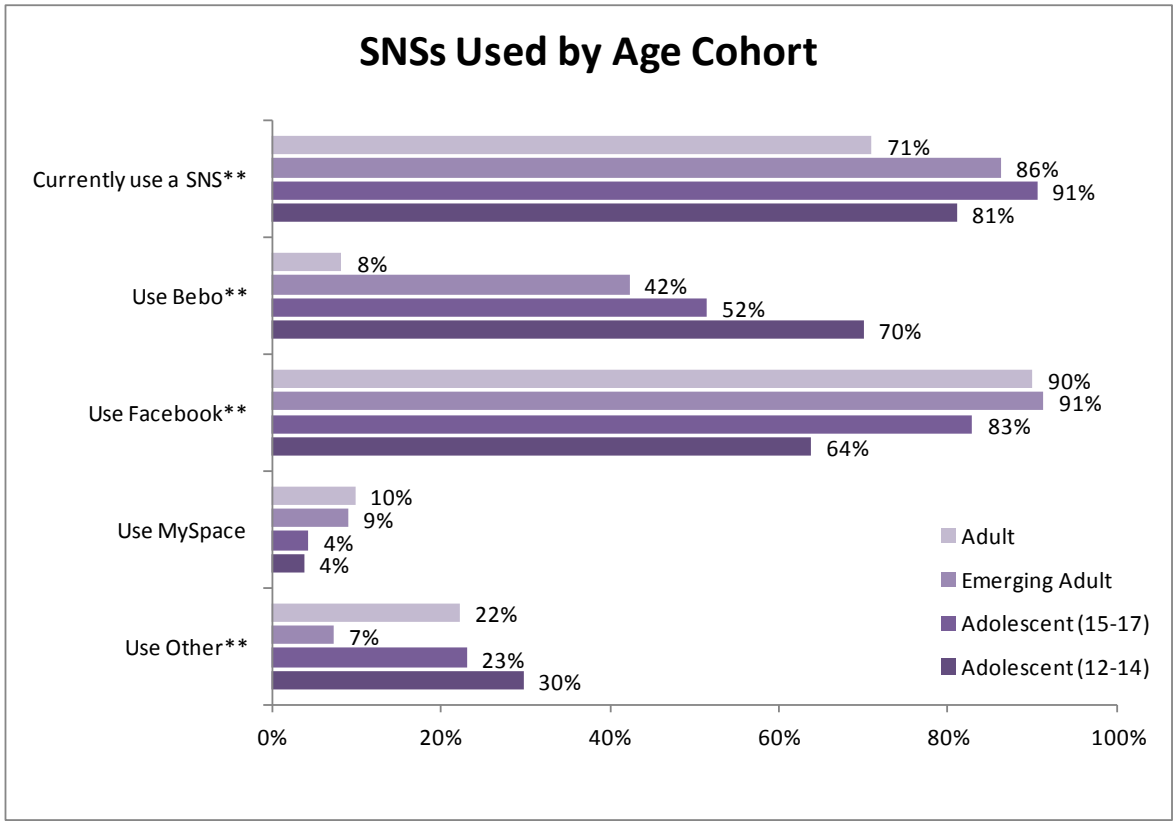


Chart 5.2 Basic Details of SNS Use by Age Cohort

As shown in Chart 5.2, a high proportion of sample respondents are current users of SNSs (84.6%), with the highest proportion in the older adolescent age cohort (91%), closely followed by the emerging adult cohort (86%) and a significantly lower proportion of current SNS users in the adult cohort (71%). More females (87%) than males (80%) are current users of SNSs. Facebook is the most popular SNS for all age cohorts although

Bebo is also popular with the younger adolescent cohort (70%). A sizeable proportion of the adolescent (27%) and the adult (22%) cohorts use other SNS sites. For adolescents the most commonly use sites are MSN (15%) followed by Twitter (4.7%). For the adult cohort, the most commonly use sites are Twitter (22%) and LinkedIn (13%). There is no evidence of a gender effect in the SNSs use by respondents.

Findings from the qualitative interviews and focus groups with adolescents and emerging adults reflect the findings of the survey. Facebook is the predominant SNS use by interviewees. Over 60% of the interviewees had previously use Bebo but have switched to using Facebook. The majority have switched because their current friends or family had migrated to Facebook. Some interviewees commented that Facebook has better functionality and is easier to use, has less spam and is more secure. Few emerging adults are still using Bebo, but over 40% of adolescents are currently using both Bebo and Facebook.

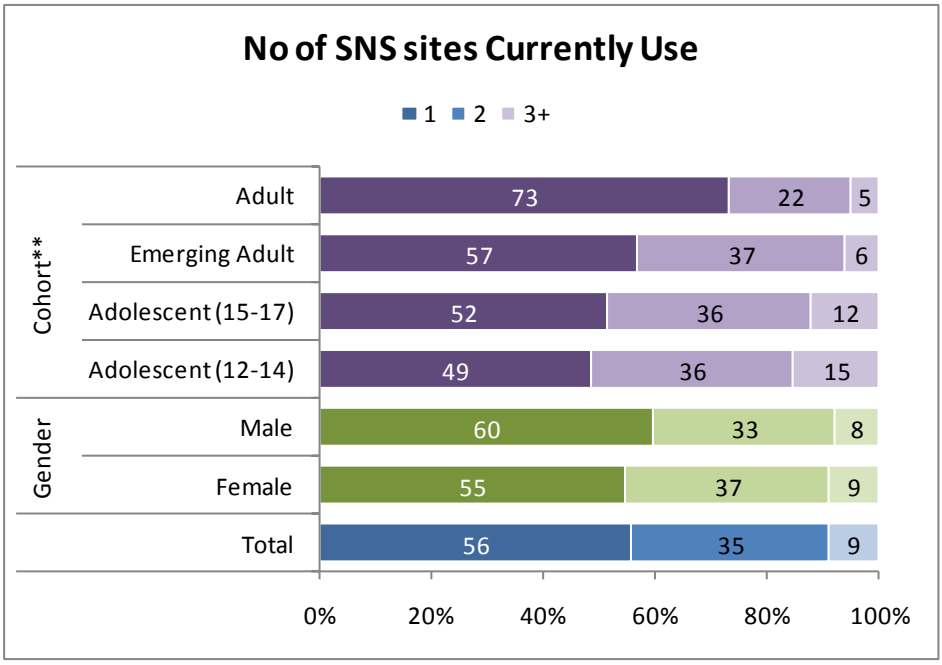


Chart 5.3 No of SNS Sites Currently Use by Age Cohort and Gender

Chart 5.3 shows whether respondents use multiple SNS sites. Over half the respondents only use one SNS, adolescents and emerging adults are more likely than adults to use multiple SNSs.

7.1% (n = 136) of respondents have never use SNSs. A higher proportion of males (9.2%) have never use SNSs compared to females (5.7%). The highest proportion of non-users are in the adult age cohort (18.7%) as compared with 11.1% in the younger adolescent age

cohort, 4.3% in the older adolescent age cohort and 5.1% in the emerging adult age cohort. Table 5.2 highlights the reasons given by respondents as to why they have never use SNSs. The main reason given by 41.9% of non-users is lack of interest and that respondents do not see the point of SNSs, a considerable proportion of non-users (23.5%) feel that using SNSs takes up too much time. 22.1% of non-users prefer to meet friends FtF or use the phone or other technologies such as e-mail to keep in contact with friends, with some non-users specifically stating that they feel friendships on SNSs are not real (5.9%). One respondent went so far as to rename SNSs "*Anti-social networking sites*". 20% of non-users express concern about the privacy implications of using SNSs.

Reason for not using SNSs	**Total N = 136 % (N)**
Not interested/don't see the point	41.9% (57)
Time wasting	23.5% (32)
Prefer to meet/talk with friends in real life	16.2% (22)
Use other technologies to keep in contact with friends	5.9% (8)
Privacy Concerns	19.8% (27)
Concerned about dangers (incl. stalking, bullying, id theft)	6.6% (9)
Parents don't allow to use (adolescent cohort only)	6.6% (9)
Difficult to set up	5.1% (7)
Friendships on SNSs are not real	5.9% (8)
Very few of my friends use them	3.7% (5)
Hype aversion / to be different	2.2% (3)
See as a popularity contest	1.5% (2)
Do not trust	2.2% (3)
Did not respond	8.8% (12)

Table 5.2 Reasons for not using SNSs

A number of in-depth interviews were carried out with respondents that have never use SNSs. They do not use SNSs primarily because they do not have any interest in SNSs and prefer FtF communication with their friends. These interviewees express strong privacy concerns and do not want others viewing their personal information.

"I have seen that everybody can see what you are saying and what your views are and I tend to keep my views to myself. I don't think everyone can see all the risks of a having a profile. Everybody can see your profile and even people half way across the world can see what you do and say. And I just don't understand that bit of it." Male, Aged 21

5.3.2 Intensity of SNS Use

Two measures are use to assess the level of SNS usage: how often users access SNSs and how much time users spend on these sites?

	On average, how OFTEN do you access social networking sites? 1=Several times a day; 2=About once a day; 3=A couple of times a week; 4=About once a week; 5=A couple of times a month; 6=About once a month; 7=Less often	**On average, how many minutes per day have you spent on social networking sites?** 1=Less than 10 minutes; 2=Between 10 and 30 minutes; 3=Between 31 and 60 minutes; 4=Between 1-2 hours; 5=Between 2-3 hours; 6=More than 3 hours
Adolescent (12 – 24) (n = 264)	2.84 ± 1.68	3.07 ± 1.56
Adolescent (15 – 17) (n = 246)	2.48 ± 1.66	3.28 ± 1.62
Emerging Adult (n = 1109)	2.54 ± 1.71	2.50 ± 1.35
Adult (n = 140)	3.11 ± 1.91	2.08 ± 1.33
TOTAL	2.62 ± 1.73	2.66 ± 1.46

Table 5.3 Summary Statistics for How Often and How Long Respondents Access SNSs by Age Cohort

As shown in Table 5.3, both the adolescent and the emerging adult cohorts report accessing a SNS about once a day on average, the adult cohort, on average, access SNSs less often at a couple of times a week. Adolescents spend more time on SNSs than the other age cohorts.

A more detailed measure use to capture the intensity of SNS use is the SNS intensity scale (adapted from the Facebook Intensity Scale created by Ellison *et al.* (2007)). This includes measures of a respondent's number of SNS "*friends*" and the amount of time they spend per day on SNSs. The scale also includes a series of Likert-scale attitudinal questions about SNS usage. Due to the fact that individual items have different scale ranges, each item is standardized before taking an average to create the scale. Respondents are divided into low intensity users (z-scores between -3 to -0.5), mid intensity users (z scores between -0.49 to +0.49) and high intensity users (z scores between +0.5 to +3). Chart 5.4 shows the intensity of SNS use broken down by age cohort and gender. A higher proportion of females (31%) compared to males (20%) are high intensity users of SNSs but there is no significant difference in intensity of use over age cohorts.

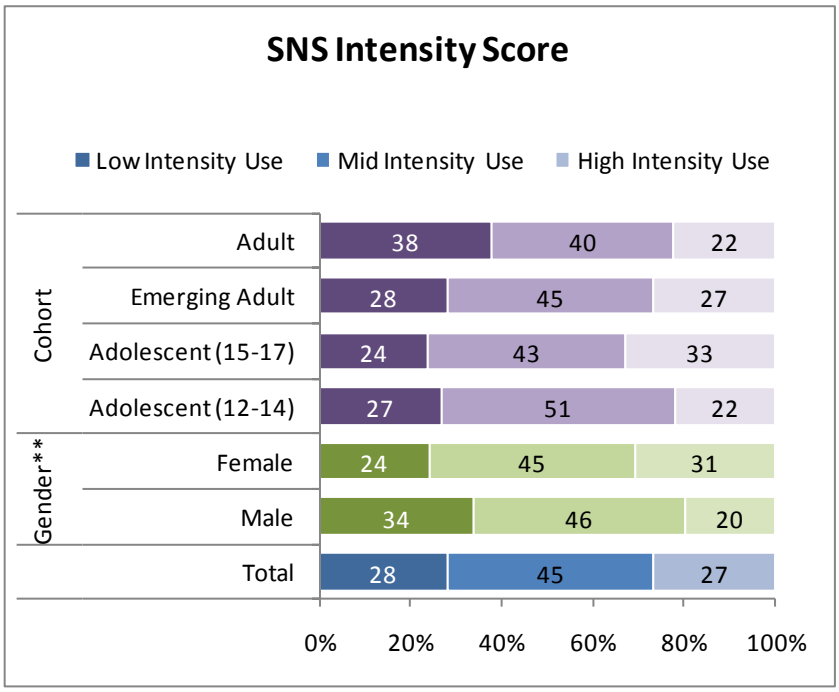


Chart 5.4 Intensity of SNS Use by Age Cohort and Gender

The focus group and individual interviews with adolescents and emerging adults indicate that these measures under represent the amount of time users spend on SNSs. Most of the interviewees, once on a computer, leave SNSs constantly running in the background. Like e-mail they regularly check their SNS accounts, but unlike e-mails that can usually be dealt with quickly, SNSs can absorb a lot more time.

"You [kind of] waste an awful lot of time before you even know it, [it's like] before you do work [or something] you'll check your email and start work, then you'll [start] check[ing your] Bebo and [checking your] Facebook. You get lost [then kind of] travelling around on the sites." Female, Aged 23.

"I live on Facebook. Facebook is my idol. If I can't sleep I go on Facebook and it doesn't even tire me out. I read everything on it and I look at other people's videos and pictures [and all]. I don't get bored of it, I spend hours on it." Female, Aged 15

The way people are accessing SNSs is also changing and some interviewees regularly use their mobile phone to access SNSs.

Many of those interviewed in the qualitative research express concern about the amount of time they spend on SNSs and that they are a distraction from studying. Some interviewees have even given up using SNSs during exam time.

"I mean you can definitely spend too much time on it … Especially coming up to exam time when everyone is on it talking about how they are not studying. I think if it aren't there we would probably all get better grades." Male, Aged 22

"[Yeah or even like] if I am doing my homework and I need to go on Google to translate something, but when I turn my laptop on, the first thing I have to go on is Facebook. Even though I go on to translate something I [do] end up going on Facebook and [when I go on] I can't just take 5 minutes because I see someone's picture [and then I look at the picture] and then I go through the whole album." Female, Aged 16.

5.3.3 Uses of SNSs

Chart 5.5 shows the ways that respondents use SNSs. The primary use of SNSs is to keep in contact with friends.

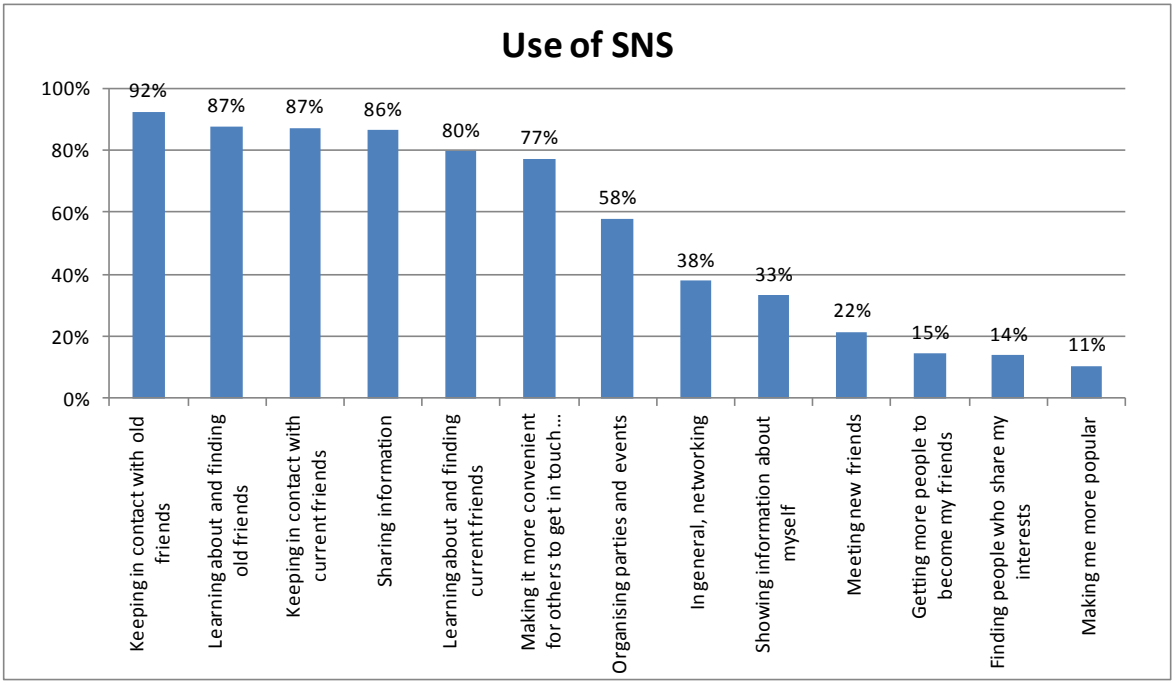


Chart 5.5 Common Uses of SNSs

There is evidence of a difference in how SNSs are use by age cohort. As shown in Chart 5.6, the adolescent cohort use SNSs differently to the emerging adult and adult age cohorts and are more likely to use SNSs to meet and find new friends and to help increase their popularity. Compared to emerging adults, older adolescents are 8.6 times more likely to use SNSs to meet new friends.

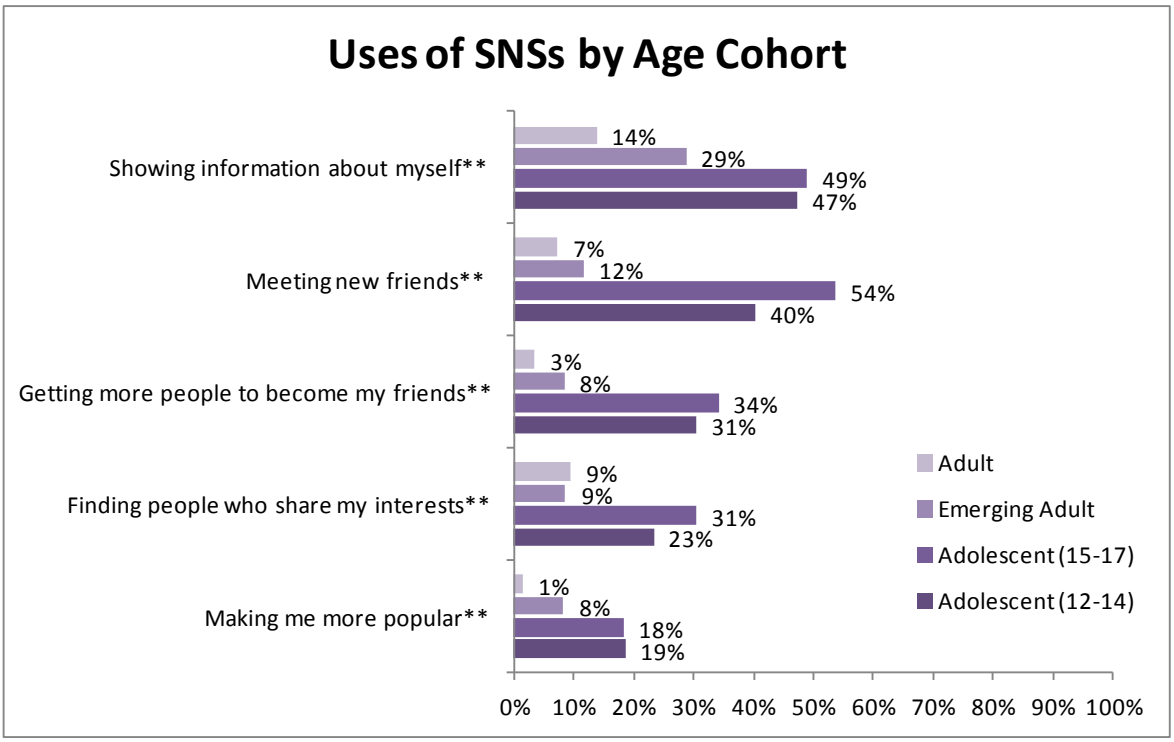


Chart 5.6 Uses of SNSs by Age Cohort

Gender differences are also evident in how respondents use SNSs. This is depicted in Chart 5.7. Males are more likely than females to use SNSs to meet and find new friends and to help increase their popularity.

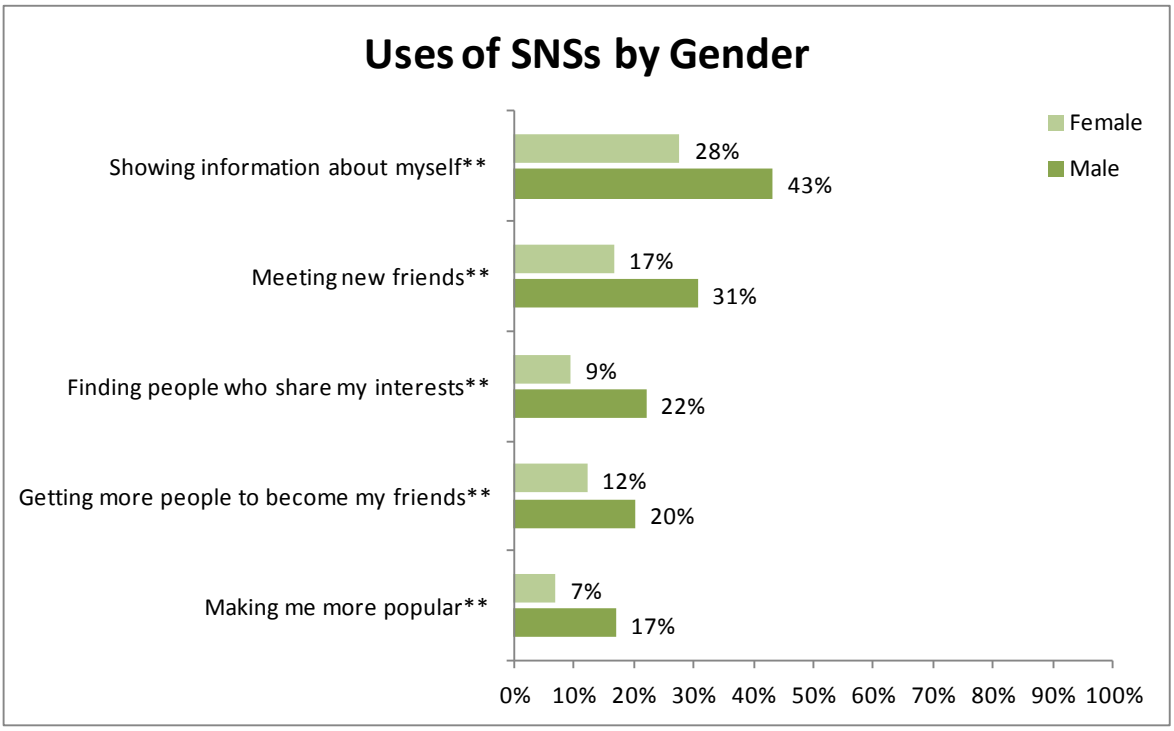


Chart 5.7 Uses of SNSs by Gender

5.3.4 Information Placed On SNSs

Table 5.4 shows the information placed on SNSs by each age cohort. The cells highlighted in green show the age cohorts with the lowest proportions. ** indicates statistical significance levels of p< 0.001, * indicates p < 0.005.

	Adolescent (12-14) % (N)	Adolescent (15-17) % (N)	Emerging Adult % (N)	Adult % (N)	TOTAL % (N)
Picture of yourself**	84.7% (221)	93.5% (229)	96.5% (1077)	84.9% (118)	93.4% (1517)
Photos of friends**	78.5% (204)	90.2% (220)	94.3% (1051)	70.5% (98)	89.5% (1573)
Date of birth**	46.3% (119)	74.7% (183)	78.0% (864)	58.3% (81)	71.3% (1247)
First name	95.8% (250)	98.0% (239)	98.0% (1094)	97.8% (136)	97.7% (1719)
Last name**	66.0% (171)	87.3% (213)	90.4% (1007)	89.9% (125)	86.3% (1516)
Full name**	65.3% (169)	86.5% (212)	89.9% (1003)	89.9% (125)	85.8% (1509)
Email address**	53.1% (138)	69.4% (170)	62.8% (698)	54.0% (75)	61.6% (1081)
IM address**	52.6% (133)	57.1% (137)	34.1% (374)	16.5% (23)	38.6% (667)
Phone number**	3.1% (8)	3.3% (8)	14.9% (164)	13.7% (19)	11.5% (199)
Home address	3.5% (9)	3.7% (9)	7.2% (79)	5.0% (7)	6.0% (104)
Name of School/Course/ Work**	68.7% (180)	72.3% (175)	69.0% (762)	51.1% (71)	68.0% (1188)
Hobbies and interests**	81.2% (211)	82.8% (202)	80.3% (891)	54.7% (76)	78.7% (1380)
List of friends**	79.5% (206)	80.4% (197)	76.6% (848)	54.0% (75)	75.8% (1326)
Comments on others profiles**	85.7% (222)	91.8% (224)	92.7% (1029)	56.1% (78)	88.6% (1553)
Sexual orientation**	-	-	46.3% (451)	21.3% (27)	43.4% (478)
Relationship status	-	-	67.2% (660)	58.3% (74)	66.2% (734)

Table 5.4 Information Placed on SNSs by Sample Cohort

Adolescents are clearly exercising caution in some categories, for example only 3.2% of adolescents put their phone number on their profile and 3.6% place their home address online. Younger adolescents are less likely that those in other age cohorts to place their full name on SNSs, but this is not reassuring as 65% of young adolescents have revealed their full name on SNSs. Adolescents, on the other hand, are more likely than the other

age cohorts to reveal their Instant Messaging (IM) address (55%), the name of their school (70%), their hobbies and interests (82%) and lists of their friends (80%). Overall the adult cohort appear to be the most cautious in the amount of information they reveal. Table 5.5 shows the information placed on SNSs by gender.

	Male % (N)	**Female** % (N)	**TOTAL** % (N)
Picture of yourself	91.2% (608)	94.7% (916)	93.3% (1524)
Photos of friends**	84.5% (561)	92.3% (893)	89.1% (1454)
Date of birth	71.0% (468)	70.9% (685)	71.0% (1153)
First name	97.1% (646)	97.8% (947)	97.6% (1593)
Last name	88.4% (586)	84.1% (812)	85.8% (1398)
Full name	87.2% (580)	83.9% (811)	85.2% (1391)
Email address	64.4% (427)	59.9% (579)	61.7% (1006)
IM address**	45.7% (298)	34.7% (330)	39.2% (628)
Phone number**	15.6% (102)	8.8% (84)	11.5% (186)
Home address	7.5% (49)	4.7% (45)	5.8% (94)
Name of School/Course/Work	68.2% (451)	68.2% (655)	68.2% (1106)
Hobbies and interests**	85.8% (567)	74.6% (721)	79.2% (1288)
List of friends	76.0% (500)	76.9% (743)	76.5% (1423)
Comments on others profiles	88.2% (582)	90.2% (871)	89.4% (1453)
Sexual orientation**	54.4% (245)	35.6% (235)	43.2% (480)
Relationship status	68.9% (313)	64.5% (428)	66.3% (741)

Table 5.5 Information Placed on SNSs by Gender

Females are more likely than males to place pictures online, but males are more likely to reveal their IM address, phone number, hobbies and interests and sexual orientation. Further analysis indicates that there are no gender and age cohort interaction effects.

To further investigate the extent to which respondents' reveal information on SNSs, an information revealed score adapted from Livingstone *et al.* (2011a) is created. This score is generated by summing the number of 7 salient items of personal information respondents have placed online. The items include: a picture of respondent, their last name, their home address, their phone number, the name of their school/college or work place, their date of birth and their email address. Table 5.6 shows the summary statistics

for information revealed broken down by age cohort. There is a significant effect of age cohort on information revealed, $F(3,411) = 33.2$, $p<0.001$. Post hoc tests (Games-Howell) indicate that the older adolescent and emerging adult age cohorts reveal significantly more information than the younger adolescent and adult age cohorts.

	Information Revealed Score Mean ± SD
Adolescent (12 – 24) (n = 255)	3.24 ± 1.47
Adolescent (15 – 17) (n = 240)	4.04 ± 1.21
Emerging Adult (n = 1091)	4.17 ± 1.37
Adult (n = 140)	3.54 ± 1.44
TOTAL	3.96 ± 1.41

Table 5.6 Summary Statistics for Information Revealed Score by Age Cohort

Table 5.7 shows the summary statistics for information revealed broken down by gender. There is no significant gender effect.

	Male Mean ± SD N = 495	**Female** Mean ± SD (N) N = 969	**TOTAL** Mean ± SD (N) N 1591
Information Revealed Score	4.04 ± 1.49	3.91 ± 1.37	3.96 ± 1.42

Table 5.7 Summary Statistics for Information Revealed Score by Gender

Table 5.8 shows the summary statistics for information revealed broken down by level of SNS usage. There is a significant effect of level of SNS usage on information revealed, $F(2,995) = 130.7$, $p<0.001$. A linear trend can be observed with the amount of information revealed increasing with intensity of use, $F(2,1725) = 274.5$, $p<0.001$.

	Low Intensity Mean ± SD N = 474	**Mid Intensity** Mean ± SD (N) N = 782	**High Intensity** Mean ± SD (N) N = 464	**TOTAL** Mean ± SD (N) N 1720
Information Revealed Score	3.24 ± 1.47	3.99 ± 1.27	4.66 ± 1.22	3.96 ± 1.42

Table 5.8 Summary Statistics for Information Revealed Score by Level of SNS Use

The qualitative interviews give some further insight into why some users display personal information such as their home address and mobile phone number on a SNS. Four out of 14 interviewees display such personal information. The main reason they display this information is so their SNS friends could contact them. The interviewees feel it is safe to do so as they have their profiles restricted to be only viewable by their SNS friends.

"Yes I have everything, but I am quite cautious with regard to the privacy controls in my account. So while I am aware that I have all my contact details it is all restricted to my direct friends". Male, Aged 23.

Over a quarter of respondents (26.1%, n = 498) have removed personal information from SNSs. The most commonly removed items of personal information are those that indicate how old a person is (19%) and contact information such as address (17%), email address (16%) and phone number (13%). 40% of respondents have removed this information due to privacy concerns. From the qualitative interviews, interviewees state that they filled in all the fields when initially creating their SNS profiles and through experience learnt that certain information should be removed.

"They actually have the fields there, [so if they're there] you [kind of] feel when you're filling out your profile [because the fields are there you kind of like] "Oh well maybe I will put in my address." Even though in the back of your head you're going that's stupid". Female, Aged 22.

"I wouldn't put up my number." Male, Aged 16
"But, you see a lot of people might make a mistake, not knowing at the start because it's their first time." Male, Aged 17

5.3.5 Privacy Settings on SNSs

Chart 5.8 shows whether respondents have restricted the privacy settings on their SNS profile by gender and by age cohort. Females (72%) are more likely than males (55%) to restrict their privacy settings. Compared to the other age cohorts, a higher proportion of adolescents do not know if they have changed their settings and a lower proportion of adolescents have not changed their settings.

There is no evidence of a statistically significant relationship between privacy settings and the amount of information a user reveals, indicating that users who restrict their privacy settings do not also restrict the amount of information they reveal.

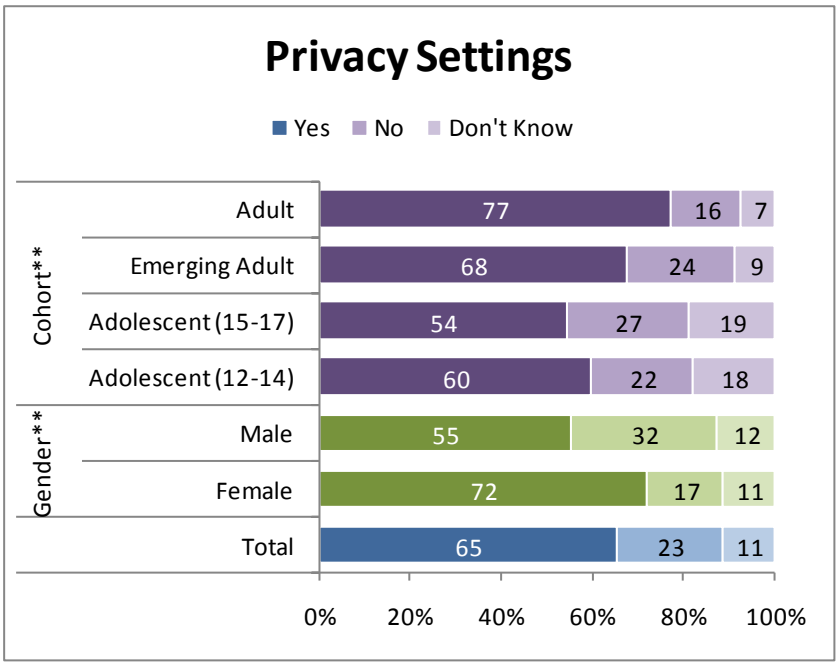


Chart 5.8 Privacy Settings by Age Cohort and Gender

The main reasons that users have changed their privacy setting is to restrict who can see their profiles and in particular to prevent randomers (a stranger/unknown person, usually a friend of a friend) and strangers viewing their personal information (44%) and to have control over who sees their profile (36%). Table 5.9 shows the reasons why respondents restrict their profiles.

Why Changed Privacy Settings	% (N)
Don't want strangers/randomers to see profile/personal information	46.6% (545)
Can control who can see profile	35.7% (418)
Safety/Security/Privacy concerns	9.1% (107)
Potential/current employers cannot see profile	5.8% (68)
Avoid unsolicited e-mails/spam & advertising	3.5% (41)
Avoid unwanted attention/comments	3.1% (36)
Parents/other relatives cannot see profile	2.3% (27)
Avoid stalking	2.1% (24)
Recommended by friend/press/lecture/teacher	0.8% (9)
Information from profile is misused	0.6% (7)
SNS takes care of privacy settings	0.5% (6)
No Reason Given	10.4% (122)

Table 5.9 Reasons Given Why Privacy Settings are Changed

Further findings related to how respondents protect themselves on SNSs is presented is Section 5.4.6.

5.3.6 Privacy Beliefs

Respondents privacy concern is measured using a scale developed by Acquisti and Gross (2006) to assess privacy concerns with SNSs. The scale contains five items measuring privacy concerns. Each item is measured using a 7 point bipolar (1 = strongly disagree; 7= strongly agree) Likert scale. For example, an item in this scale is, ‘‘I am concerned about what social networking sites can know about you”.

Chart 5.9 shows that females express higher levels of privacy concern (t (1617) =4.79, p< 0.001) and that privacy concern increases with age (F (1,256) =6.44, p<0.001).

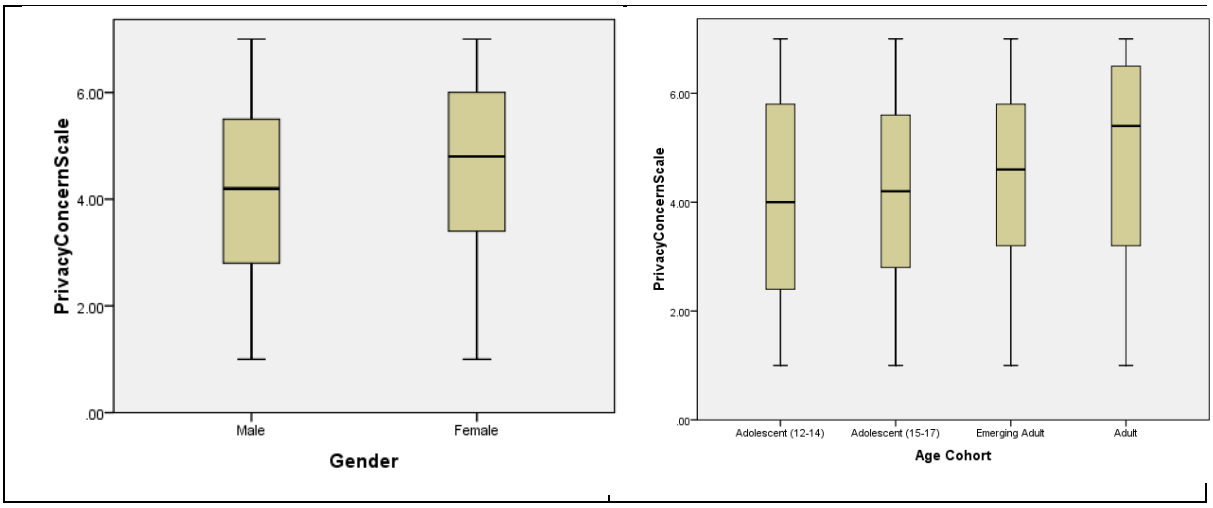


Chart 5.9 Privacy Concern by Gender and Age Cohort

Chart 5.10 shows that there is a significant relationship between privacy concern and privacy settings (t (1345) =9.40, p< 0.001), indicating that those users that express higher levels of privacy concern are more likely to restrict their privacy settings on SNSs. However, like for privacy settings, there is no significant relationship between expressed privacy concern and information disclosure. This trend is evident in the qualitative interviews, some interviewees comment on the dangers of revealing personal information on SNSs, but this is not reflected in their behaviour, all interviewees display their full name on their SNS profile, include photos of themselves, regularly make comments on other users profiles and name the course they are taking in College. 12 out of the 14 interviewees display their email details.

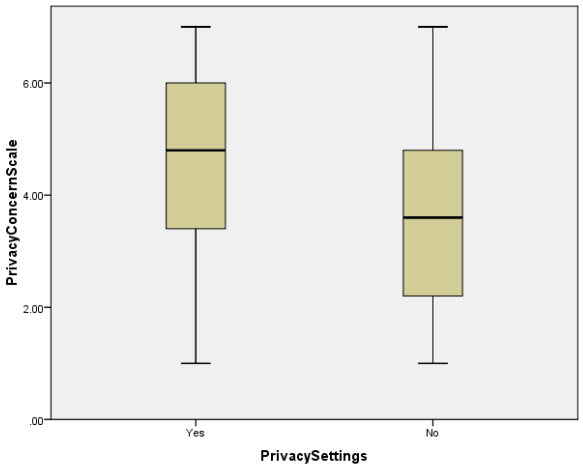


Chart 5.10 Privacy Concern by Privacy Settings

5.3.7 Trusting Beliefs

Gefen's (2000) disposition to trust scale is used to measure trust. This scale measures trust dispositions in general rather than measuring trust in a particular technology or company. This scale measures four trust items such as "I generally trust other people" and is measured on a 7 point bipolar (1 = strongly disagree; 7= strongly agree) Likert scale.

Neither gender nor age cohort show a statistical significant difference for disposition to trust. No relationship is evident between disposition to trust and privacy settings.

Chart 5.11 shows that a linear trend can be observed, showing that the amount of information revealed increases with disposition to trust, $F(7,1499) = 8.38$, $p<0.001$. This indicates that individuals that are more trusting are more likely to reveal more information on SNSs.

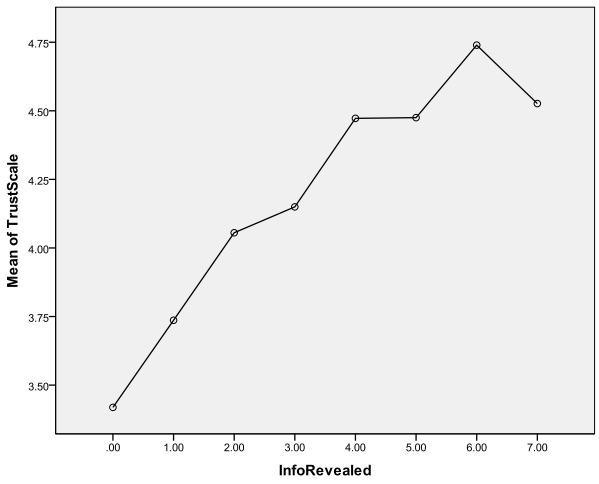


Chart 5.11 Mean of Disposition to Trust by Information Revealed Score

A further single item measure is included to measure trust in SNS companies "Overall, I trust social networking sites (the companies)". This item is measured on a 7 point bipolar (1 = strongly disagree; 7= strongly agree) Likert scale. The scale is collapsed into three groups for ease of interpretation: Low Trust in SNSs (points 1 & 2 on the scale), Medium Trust in SNSs (points 3, 4 & 5) and High Trust in SNSs (points 6 & 7). Chart 5.13 shows the level of trust in SNS companies broken down by age cohort and gender. Adolescents are more likely to trust SNS companies compared to the older age cohorts. There is no gender effect related to trust in SNS companies.

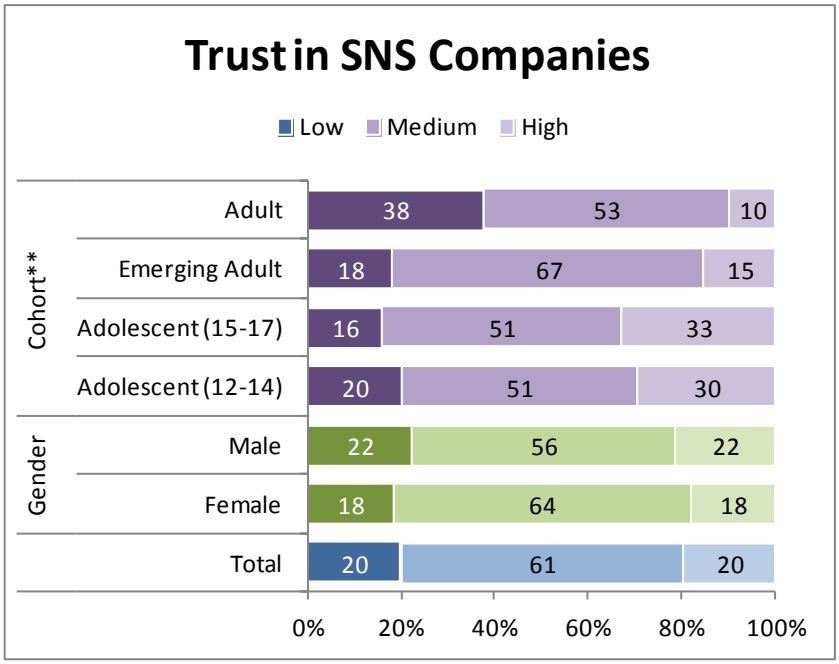


Chart 5.12 Trust in SNS Companies by Age Cohort and Gender

The qualitative interviews show that although some respondents do not trust the SNS companies, the majority of respondents either trust SNS companies or have not thought about this issue. The majority of respondents are unaware of the business practices of SNS companies.

When asked about trust in SNS companies:

"I can't really answer that because I do not know a huge amount about how they do their business [on the outside]" Male, Aged 23

"I think it is credible [anyway] and the 30 million who use it can't be wrong" Male, Aged 20

5.3.8 Peer Influence

As discussed in Section 4.4.1, an adapted scale by Taylor and Todd (1995b) is used in this study to measure peer influence. This scale does not reliably measure peer influence (Cronbach's α = 0.407) so a single item measurement based on Thomson *et al.* (1991) "I use social networking sites because many of my friends use them", is used as a measure of peer influence. This item is measured on a 7 point bipolar (1 = strongly disagree; 7= strongly agree) Likert scale. The scale is collapsed into three groups for ease of interpretation: Low Peer Influence (points 1 & 2 on the scale), Medium Peer Influence (points 3, 4 & 5) and High Peer Influence (points 6 & 7).

Chart 5.13 shows the level of peer influence broken down by age cohort and gender. Older adolescents are the most likely to be influenced by their peers (high = 44%) with adults being the least likely (high = 25%). There is no gender effect for peer influence.

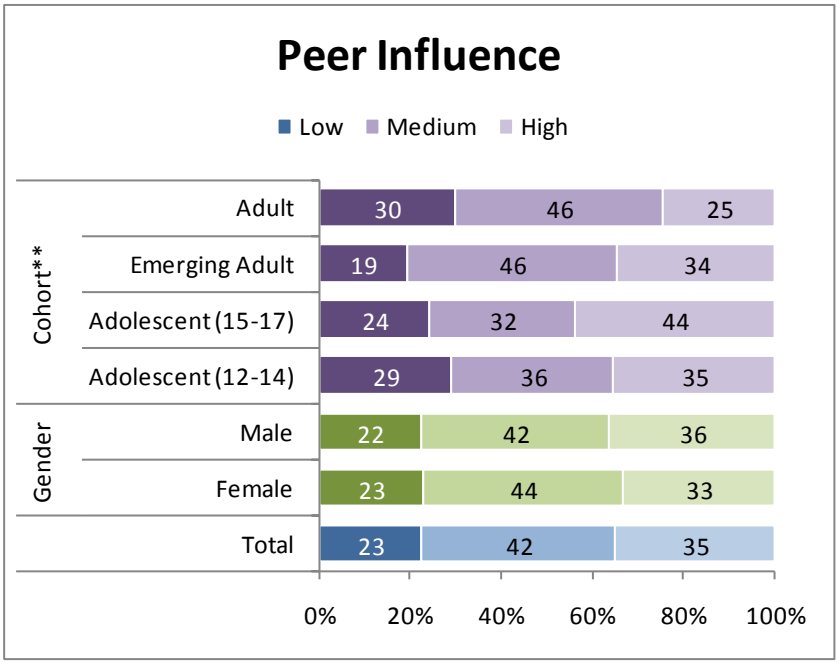


Chart 5.13 Peer Influence by Age Cohort and Gender

Chart 5.14 shows that a linear trend can be observed, showing that the amount of information revealed increases as peer influence increases, $F(2,1565) = 19.3$, $p<0.001$ and the intensity of SNS use increases as peer influence increases, $F(2,1601) = 67.1$, $p<0.001$. This indicates that individuals that display higher levels of peer influence are more likely to reveal more information on SNSs and are more likely to use SNSs more intensively.

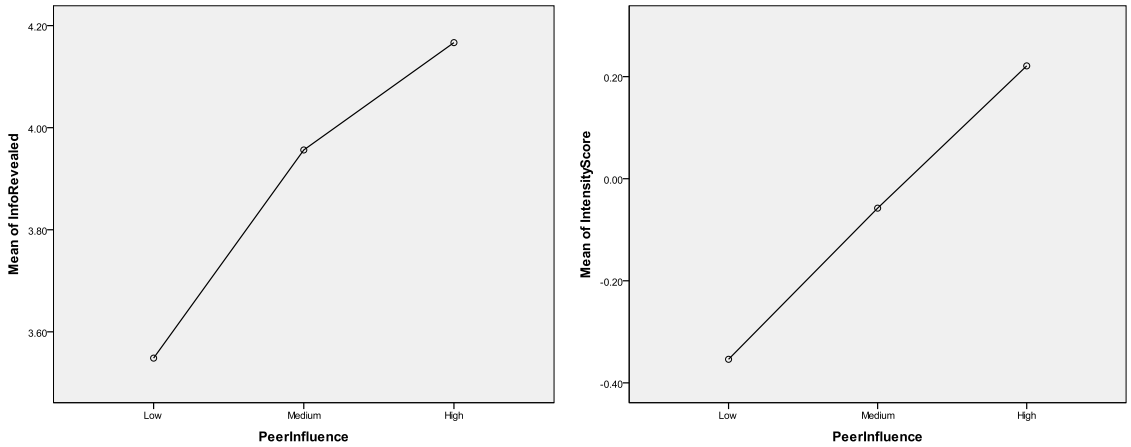


Chart 5.14 Mean of Information Revealed and SNS Intensity Score by Peer Influence

5.3.9 Prior Experience of Event

Chart 5.15 shows the proportion of respondents that have prior experience of the 12 risks examined in this study. 50% of respondents have experience of spending too much time on SNSs. 42% have embarrassing information of themselves seen by others and 41% have experienced spam.

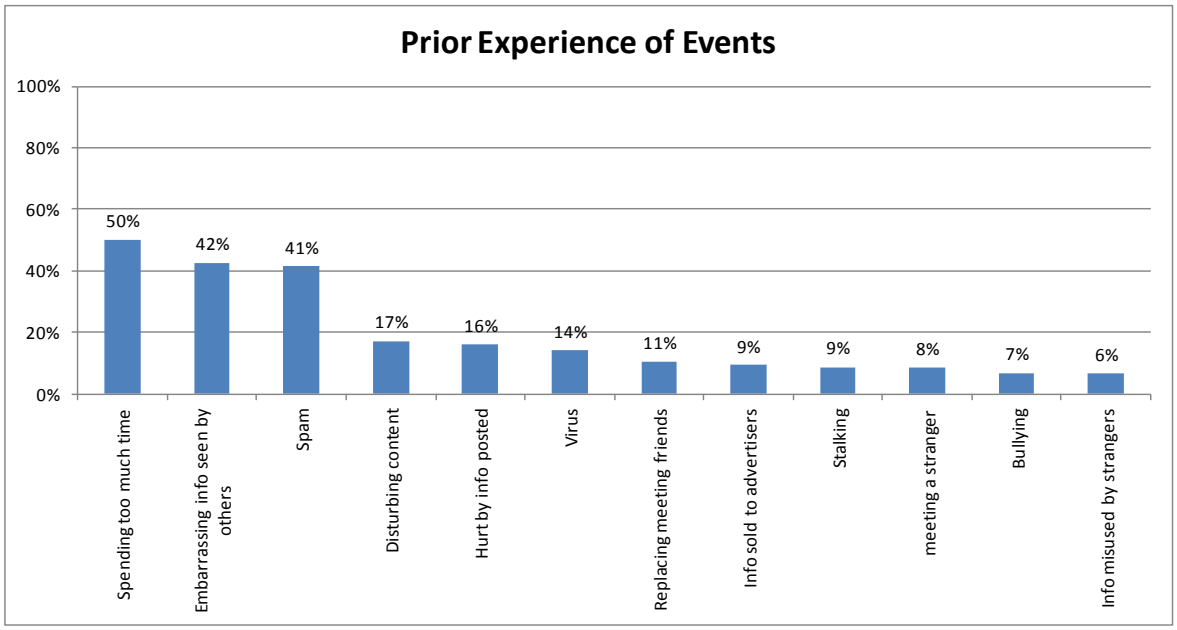
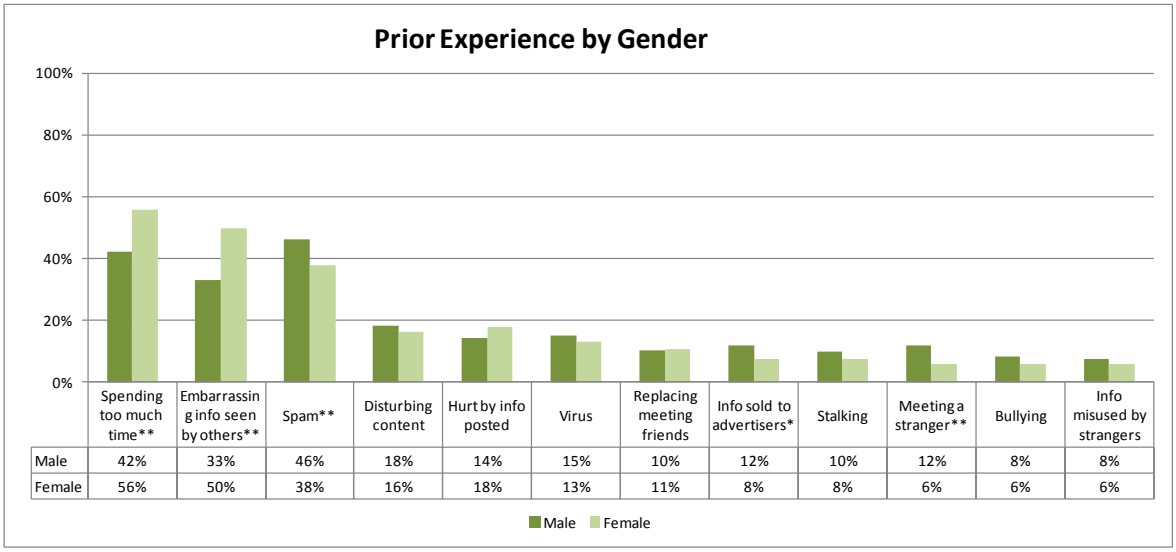


Chart 5.15 Prior Experience of Event

Chart 5.16 shows prior experience by gender. Males (46%) are more likely than females (38%) to have experienced spam and twice as likely as females to have met in person a stranger that they initially met on a SNS. Females (56%) are more likely than males (42%) to have spent too much time on SNSs and females (50%) are more likely than males (33%)

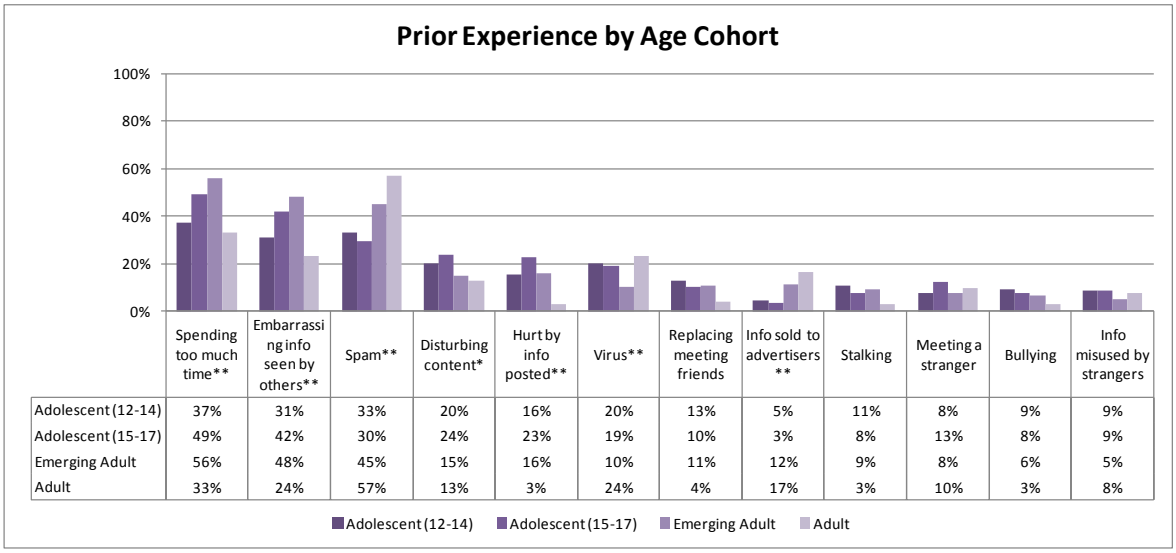
to have had embarrassing information or photos seen by people they would prefer didn't see them.

Chart 5.17 shows prior experience by age cohort. Compared to the other age cohorts, emerging adults are more likely to have spent too much time on SNSs and to have had embarrassing information or photos seen by people they would prefer didn't see them, but least likely to have encountered viruses via SNSs. Adolescents are least likely to have experienced spam or to have experienced their information being sold to advertisers but older adolescents are more likely to have encountered disturbing content. Adults are the least likely to be hurt by information posted on SNSs.



	Spending too much time**	Embarrassing info seen by others**	Spam**	Disturbing content	Hurt by info posted	Virus	Replacing meeting friends	Info sold to advertisers*	Stalking	Meeting a stranger**	Bullying	Info misused by strangers
Male	42%	33%	46%	18%	14%	15%	10%	12%	10%	12%	8%	8%
Female	56%	50%	38%	16%	18%	13%	11%	8%	8%	6%	6%	6%

Chart 5.16 Prior Experience by Gender



	Spending too much time**	Embarrassing info seen by others**	Spam**	Disturbing content*	Hurt by info posted**	Virus**	Replacing meeting friends	Info sold to advertisers**	Stalking	Meeting a stranger	Bullying	Info misused by strangers
Adolescent (12-14)	37%	31%	33%	20%	16%	20%	13%	5%	11%	8%	9%	9%
Adolescent (15-17)	49%	42%	30%	24%	23%	19%	10%	3%	8%	13%	8%	9%
Emerging Adult	56%	48%	45%	15%	16%	10%	11%	12%	9%	8%	6%	5%
Adult	33%	24%	57%	13%	3%	24%	4%	17%	3%	10%	3%	8%

Chart 5.17 Prior Experience by Age Cohort

Apart from stalking, no other gender and age cohort interaction effects are evident. For stalking, a three-way loglinear analysis produces a final model that retains all effects. The likelihood ratio of this model is $\chi^2(0) = 0$, p=1. This indicates that the highest-order interaction (stalking x age cohort x gender) is significant, $\chi^2=13.37$, df=3, p= 0.004. Males in the young adolescent (12-14) and adult cohorts are more likely to have been cyberstalked than females in the same age cohorts. Young adolescent males are 3 times more likely to have experienced cyberstalking compared to young adolescent females and adult males are 5 times more likely to have experienced cyberstalking compared to adult females.

Summary

Table 5.10 summarises both the quantitative and qualitative findings presented in this section.

SNS Behaviour	General Findings	Gender	Age	Qualitative Findings
Currently use SNSs	High proportion of respondents are current users (85%) 7% of respondents do not use SNSs	More females than males are current users More males than females do not use SNSs	Highest proportions of current users are in the older adolescent and emerging adult age categories with the lowest proportion in the adult age cohort Highest proportion of non-users are in the adult age group	Confirm quantitative findings
SNS use	Facebook most popular SNS, followed by Bebo	No gender differences	Bebo more popular with younger adolescents	Confirm quantitative findings
Intensity of SNS use	Users access SNSs on average once a day.	A higher proportion of females compared to males are high intensity users	No age cohort differences	The quantitative measure underestimates the amount of time users spend on SNSs
Use of SNSs	Respondents primarily use SNSs to keep in contact with existing friends	Males are more likely to use SNSs to find and meet new friends and help increase popularity	Adolescents are more likely to use SNSs to find and meet new friends and help increase popularity	Confirm quantitative findings
Information revealed	Respondents reveal substantial amounts of personal information on SNSs Amount of information revealed increases with Intensity of SNS use	Males are more likely than females to reveal contact information	Older adolescent and emerging adults reveal significantly more personal information than younger adolescents and adults. Adults are the most cautious in the amount of personal information they reveal	Those that reveal personal contact information feel is safe to do so as they have restricted privacy settings Users tend to fill in all the details when they first join SNSs and learn through experience to remove certain information

SNS Behaviour	General Findings	Gender	Age	Qualitative Findings
Privacy settings	Nearly a quarter of respondents have not restricted their privacy settings Users who restrict their privacy settings do not also restrict the amount of information they reveal	Females are more likely than males to have restricted their privacy settings	Adolescents are less likely than the other age cohorts to have restricted their settings A higher proportion of adolescents compared to the other age cohorts do not know if they have changed their privacy settings	See Section 5.4.6.
Privacy concern	Users that express higher levels of privacy concern are more likely to restrict their privacy settings, but not necessarily restrict the personal information they reveal	Females express higher levels of privacy concern than males	Privacy concern increases with age	Confirm quantitative findings
Disposition to trust	Amount of personal information revealed increases with disposition to trust	No gender differences	No age cohort differences	
Trust in SNS company	A fifth of respondents place high levels of trust in SNSs	No gender differences	Adolescents are more likely to trust SNS companies compared to the other age cohorts	The majority of respondents either trust SNS companies or have not thought about it The majority of respondents are unaware of the business practices of SNSs

SNS Behaviour	General Findings	Gender	Age	Qualitative Findings
Peer influence	Respondents that display higher levels of peer influence are more likely to reveal more information on SNSs and are more likely to be high intensity users of SNSs	No gender differences	Older adolescents are the most likely to be influenced by their peers	
Prior experience of risk	Most commonly experienced risks are: • spending too much time on SNSs; • embarrassing information seen by others; and • spam. Young adolescent males are 3 times more likely to have experienced cyberstalking compared to young adolescent females and adult males are 5 times more likely to have experienced cyberstalking compared to adult females.	Males are more likely than females to have experienced: • spam; and • meeting a stranger. Females are more likely than males to have experienced: • spending too much time on SNSs; • embarrassing information and photos being seen by others	Adolescents are the: • least likely to have experienced spam; • least likely to have experienced their information being sold to advertisers; • most likely to have encountered disturbing content. Emerging adults are the: • most likely to have spent too much time on SNSs; • most likely to have experienced having embarrassing information and photos seen by others; • least likely to have encountered viruses. Adults are the least likely to be hurt by information posted on SNSs.	See Section 5.4.6.

Table 5.10 Summary of Findings – Use and Behaviour on SNSs

5.4 Risk Perceptions

This section examines a number of characteristics that have been found to be important in previous studies of risk perception. This includes perceived risk to self, knowledge of risk, concern about risk, control of risk and the harmful effects of the risk.

5.4.1 Personal Risk

Respondents are asked to indicate their personal likelihood of risk for a selection of 12 risks associated with SNSs. Each risk is measured on a 7 point bipolar (1 = not at all at risk; 7= very much at risk) Likert scale. For ease of interpretation, the risk measures are collapsed into three categories to indicate those that perceived themselves at Low Risk (points 1 & 2 on the scale), Medium Risk (points 3, 4 & 5) and High Risk (points 6 & 7). Chart 5.18 shows a summary of respondents perceived personal risk (likelihood) level for each of the risks associated with SNSs. Approximately 30% of respondents perceive themselves to be at a high risk of spam on SNSs and having embarrassing information or photos of themselves being seen by people they did not want to see them. Few respondents perceive that they are at a high risk that SNSs would replace the need to meet up with existing friends (7%), of meeting in person a stranger that they had only met online (12%) and being bullied or harassed (12%).

Chart 5.19 & Chart 5.20 show the mean score values (on the Likert scale) for perceived personal likelihood of risk by gender and age cohort. In these charts and all subsequent line charts, the points have been joined in order to improve the visual presentation and readability of the charts. These lines are not trend lines.

A MANOVA is used to compare personal likelihood of risk across all twelve risks by age cohort and gender. The multivariate result is significant for gender, Pillai's Trace = 0.92, $F = 13.26$, $df = (12,1563)$, $p < 0.001$, indicating a difference in perceived likelihood of risk between males and females. Chart 5.19 shows that males perceive themselves to be at a higher risk than females for meeting in person a stranger that they had only met online and having their personal information sold to advertisers, but at a lower risk of spending too much time on SNSs, having embarrassing information or photos of themselves being seen by people they did not want to see them and getting a virus.

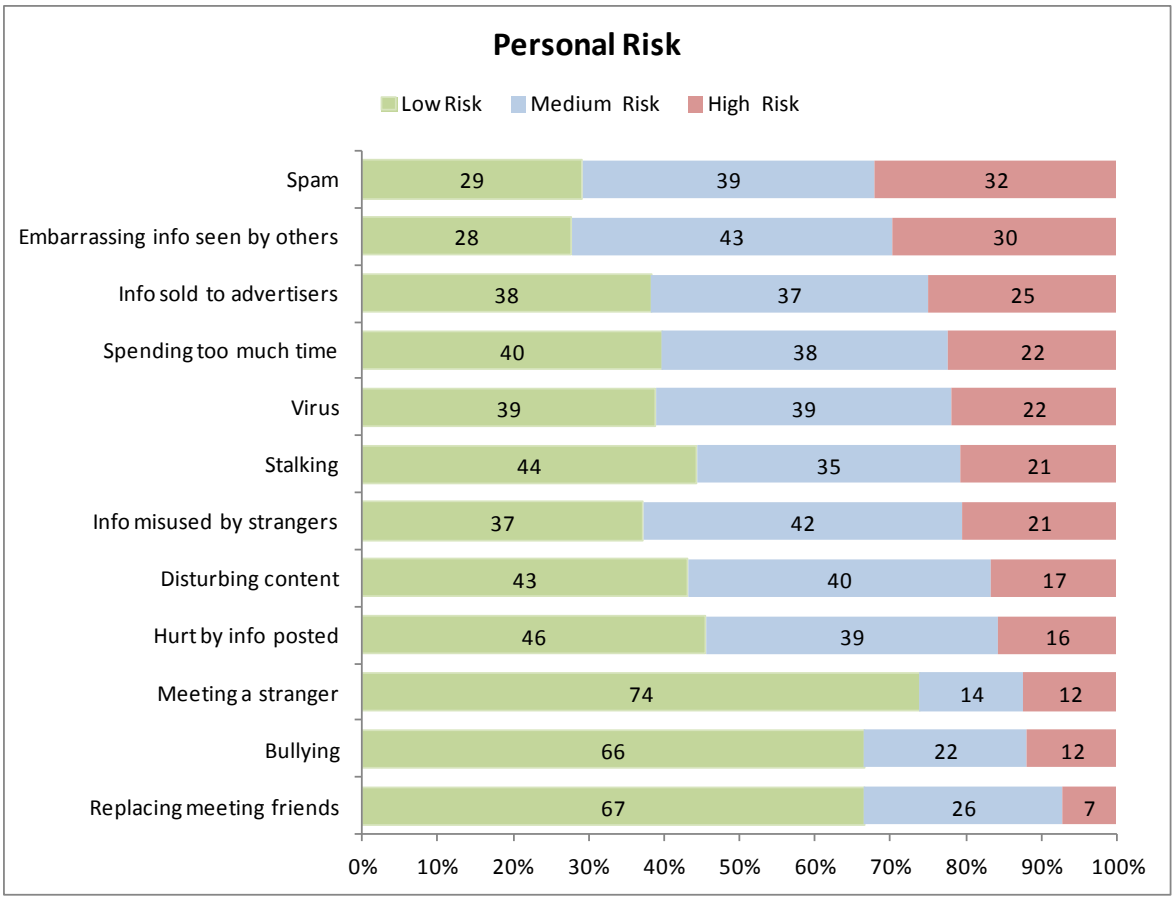


Chart 5.18 Perceived Personal Risk

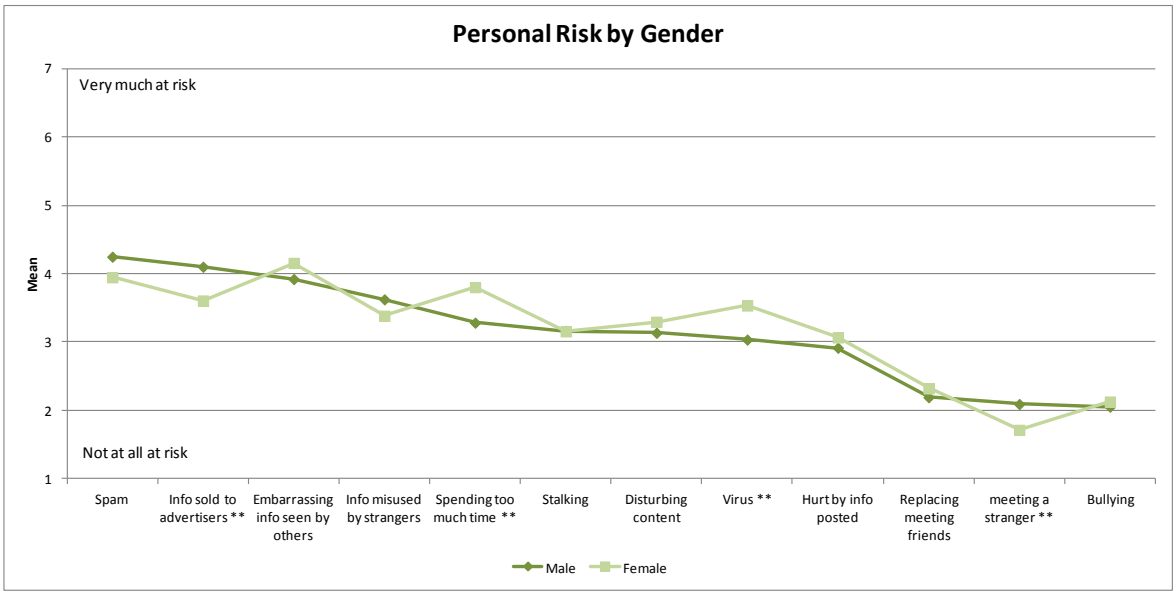


Chart 5.19 Mean Score for Perceived Personal Risk by Gender

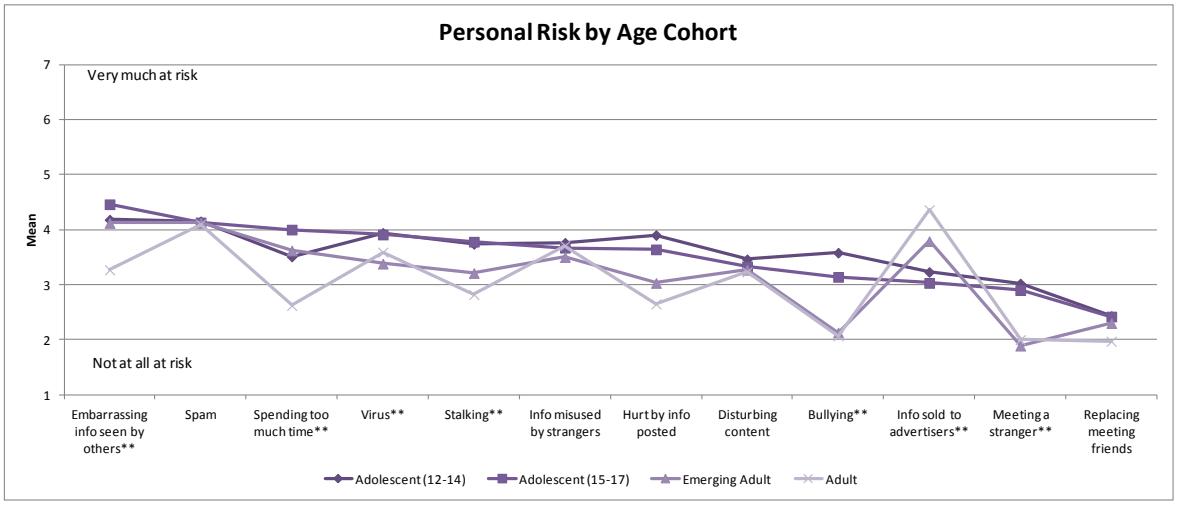


Chart 5.20 Mean Score for Perceived Personal Risk by Age Cohort

The multivariate result is significant for age cohort, Pillai's Trace = .263, F = 13.44, df = (36,5034), $p < 0.001$, indicating a difference in personal likelihood of risk across age cohorts. From Chart 5.20 it is evident that adolescents perceive themselves to be at a higher risk than the other age cohorts for all risks except for their personal information being sold to advertisers. Adolescents perceive themselves to be at a considerably higher risk than the other age cohorts for being hurt by information posted, being bullied or harassed or meeting in person a stranger that they had only met online. The adult age cohort, compared to the other age cohorts, perceive themselves to be at a lower risk of spending too much time on SNSs, but at a higher risk for their personal information being sold to advertisers. Emerging adults perceive themselves to be at a lower risk of getting a virus than the other age cohorts. The personal likelihood of risk associated with having embarrassing information or photos' being seen by others reduces with age.

A table summarising the findings of this section and subsequent sections can be found after at the end of Section 5.4.5., see Table 5.11.

5.4.2 Knowledge of Risks

Respondents are asked to indicate, on a 7 point bipolar (1 = very well known; 7= not very well known) Likert scale, whether they think people their age know about the 12 risks associated with SNSs. For ease of interpretation, the results are collapsed into three categories, Very well known (points 1 & 2 on the scale), Known (points 3, 4 & 5) and Not Well Known (points 6 & 7). Chart 5.21 shows that most respondents feel that the risks associated with SNSs are well known by people their age. The less well known risks are

that information on SNSs can be sold to advertisers (36% - not well known) and that viruses can be transmitted via SNSs (26% - not well known).

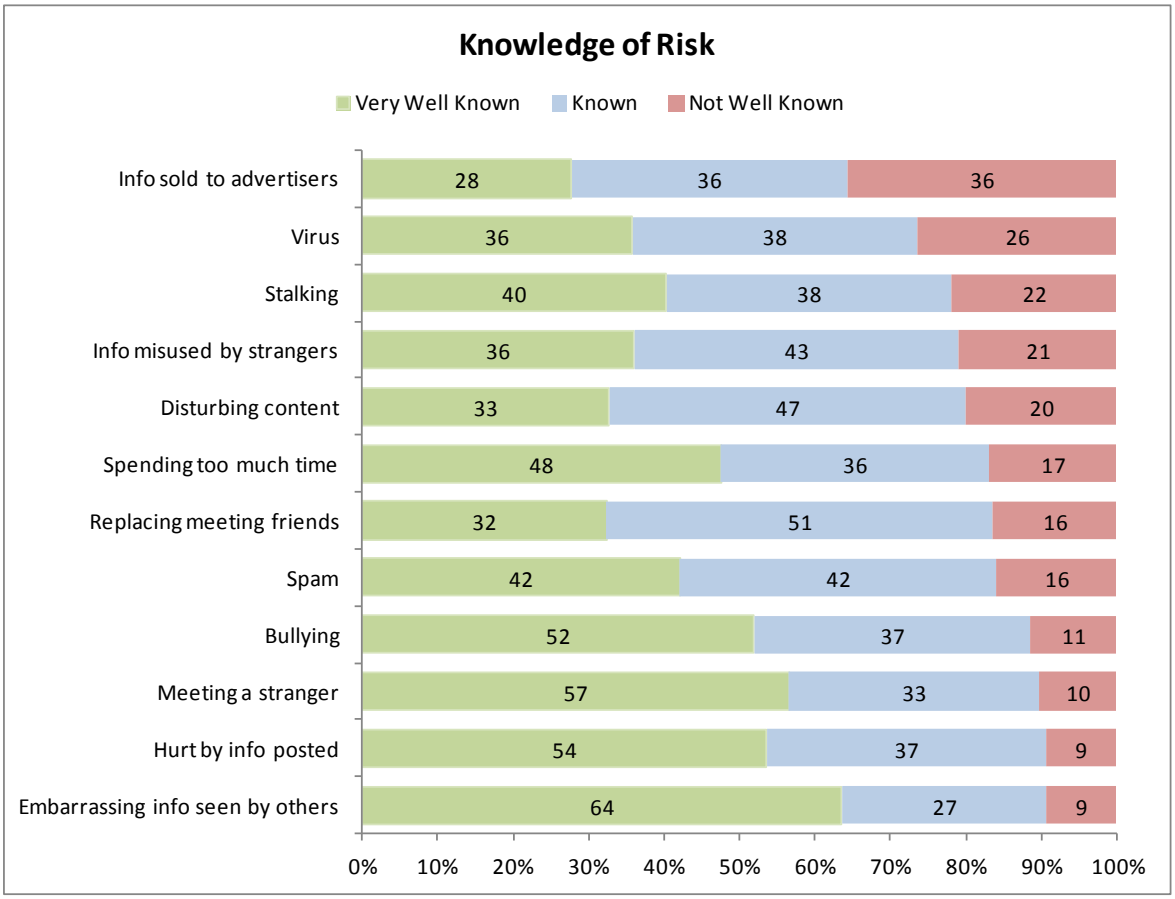


Chart 5.21 Knowledge of Risk

A MANOVA is used to compare knowledge of risk across all twelve risks by age cohort and gender. The multivariate result is not significant for gender indicating no evidence of a gender difference in knowledge of risks. The multivariate result is significant for age cohort, Pillai's Trace = .167, F = 4.26, df = (36,2598), $p < 0.001$, Chart 5.22 illustrates that compared to the other age cohorts, adolescents in the 15 to 17 year old age group have the highest level of knowledge about all 12 risks. Adolescents are significantly more aware than emerging adults and adults of the risks associated with getting a virus on a SNS, their information being misusedby strangers, stalking and bullying.

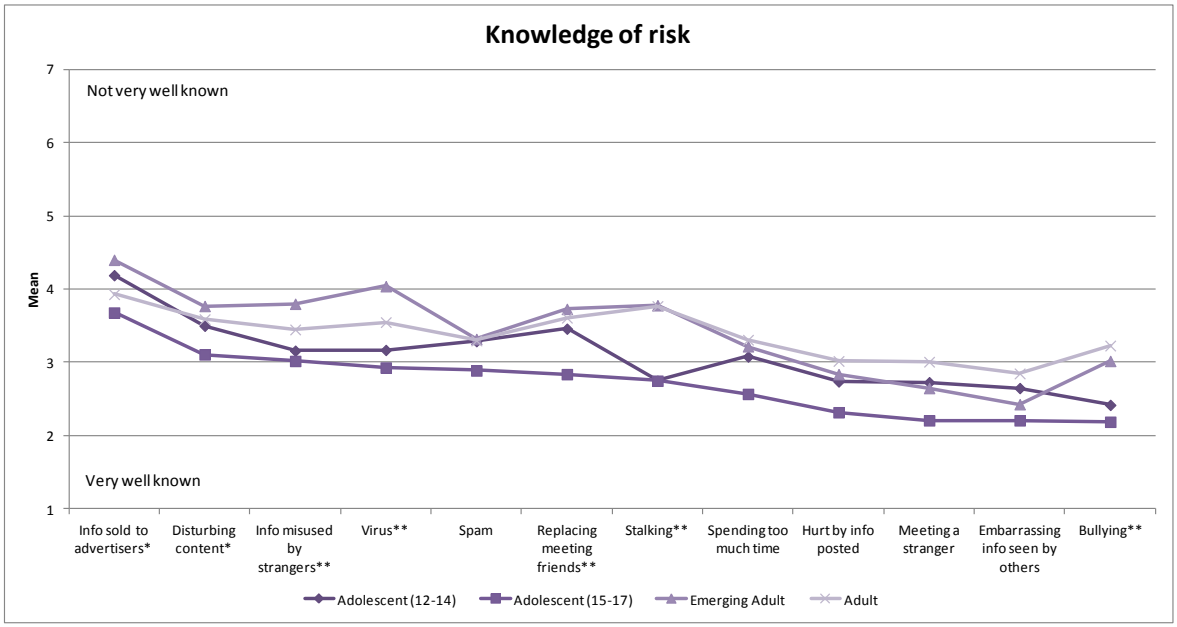


Chart 5.22 Mean Score for Knowledge of Risk by Age Cohort

The qualitative focus groups discussions and in-depth interviews illustrate that adolescents show more awareness of the risks. Respondents were asked to produce a list of risks associated with SNSs and the adolescent discussion groups produced more extensive lists. The qualitative discussions and interviews confirm the findings of the survey and show that SNS users are least aware of the risks to their personal information and the technical risks. Most respondents think that their peer groups are not aware that personal information can be harvested from SNSs and are not aware of phishing and malware attacks.

"Most of them wouldn't have a clue about information getting kept, and about the applications collecting information. No way, no one has a clue." Female, Aged 22.

The qualitative interviews indicate that SNS users learn about the risks from informal sources, such as their peer group, siblings and other family members or from personally experiencing the risk.

"You learn not to click on them from your parents or brothers or sisters, or someone like that." Male, Aged 17.

"A girl in our class was adding a guy and we told her [about it like] you wouldn't know who he is and she [was like] said no. [And we were like] does he have a picture up and she [was like] said no. She was going in that day to meet him in town and we told her no. When we seen her the next day she said she hadn't gone in. So we kind of told her." Female, Aged 17.

Some of the adolescent groups had classes in school that had informed them of the risks associated with the Internet and SNSs, they had found them useful, leading to some students restricting their privacy settings on SNSs. The adolescent groups feel that schools have a role in informing students of the risks associated with SNSs.

A number of interviewees suggest that the SNS company should inform users of the risks, but only two interviewees recognise that SNS companies would not want to restrict what you place online as that is what makes them commercially viable. One respondent, however, feels that she is not aware of the risks as the SNS has not informed her.

"Because [it is kind of] you are on the website and you are prompted to put in the information and no big warning sign comes up. Or when someone adds you as a friend there is no warning" Female, Aged 24.

As suggested by one adolescent, even if the SNS listed the risks, users are likely to ignore them.

"Put them on the homepage. Say you are at risk of and list them." Male, Aged 14.
"I don't think anyone our age would care if that is on it. They'd just scroll down." Male, Aged 14.

A number of respondents feel that users that have suitable computer experience and technical skills are more likely to see the risks and are better able to protect themselves.

"I am doing Economics so most of [them] my peers would have less experience with computers than me and I'd see them not being as aware of the risks. [So I'd say] it's definitely something to do with knowledge and familiarity with computers in general. Not only just [kind of] with the website [or whatever] or networking [thing], but I think if you have a familiarity with computers you know what to look for [nearly] or you know that things are sometimes default." Male, Aged 20.

To investigate this further, a MANOVA is used to compare knowledge of risk across all twelve risks by Internet experience. The multivariate result is not significant indicating that those with higher Internet experience do not show an increased knowledge of the risks.

5.4.3 Concern about Risks

Respondents are asked to indicate whether they think people their age are concerned about the risks. Concern is measured on a 7 point bipolar (1 = not at all concerned; 7= very concerned) Likert scale. For ease of interpretation the concern measures are collapsed into three categories, Not Concerned (points 1 & 2 on the scale), Concerned (points 3, 4 & 5) and Very Concerned (points 6 & 7). Chart 5.23 shows that reputational risks such as embarrassing information or photos being seen by others (83% concerned or very concerned) and being hurt by information posted (73% concerned or very concerned) are of most concern to respondents. Respondents are least concerned about spending too much time on SNSs (42% concerned or very concerned) and that SNSs can replace the need for meeting up with existing friends (49% concerned or very concerned).

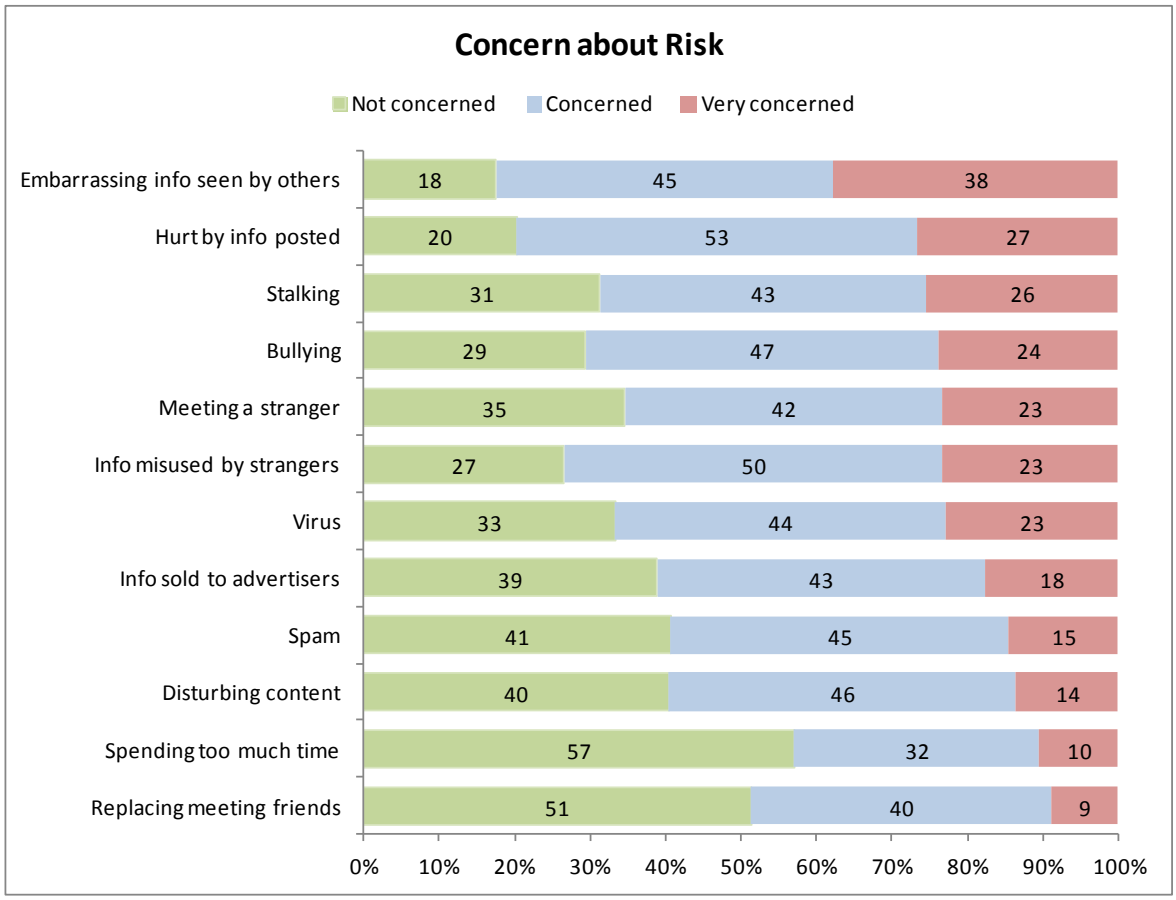


Chart 5.23 Concern about Risk

A MANOVA analysis shows no evidence of a gender difference in concern about risks. A significant difference in concern about risks is evident for age cohort, Pillai's Trace = .215, $F = 5.41$, df = (36,2523), $p < 0.001$.

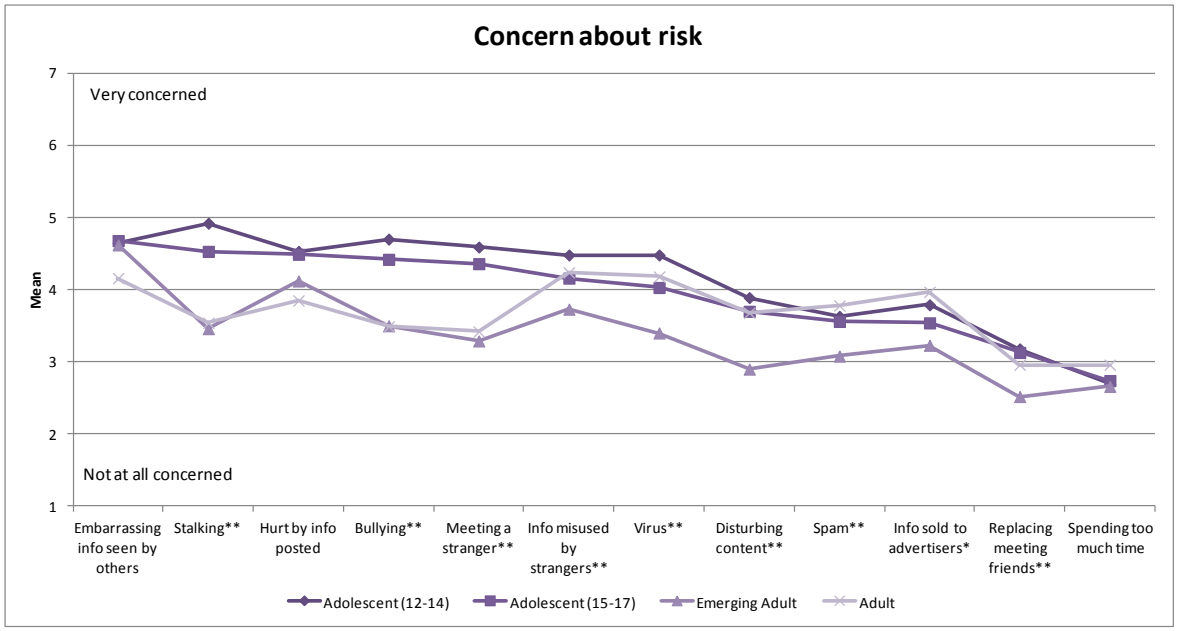


Chart 5.24 Mean Score for Concern about Risk by Age Cohort

Chart 5.24 shows that apart from embarrassing information being seen by others and being hurt by information posted, emerging adults show the lowest levels of concern about all other risks. Adolescents are significantly more concerned than the other age cohorts about the risks of being bullied and stalked on SNSs and meeting in person a stranger that they had met on a SNS. Emerging adults are significantly less concerned than the other age cohorts about their personal information being misused by strangers or being sold to advertisers, getting a virus or spam on SNSs, accidentally stumbling across content that made them uncomfortable and SNSs replacing the need to meet up with existing friends.

The qualitative interviews and discussion groups back up some of the survey findings, with one notable exception time wasting. For the emerging adults, most think that time wasting on SNSs is the risk of greatest concern to their peer group. Many respondents refer to this time wasting as an addiction.

"Time wasting definitely is. [Like] some people are way worse. They would be on it during the night, [like] they actually come in from a night out and log in." Female, Aged 21

"I also think people get caught up in it and they just get addicted, and it becomes more than just a social thing it becomes more of a need and you are just participating and using it as a tool." Male, Aged 22

Other concerns highlighted by the emerging adult interviews are the reputational risks of personal information (in particular photos) being seen by others and being hurt by information that others posted. Some comment on the permanence of postings on SNSs.

"Probably because it's always there. [Like] if someone says something to you in person, [you know], they just say it and it's over, but [like] on Facebook or any network site, there's a permanent record of that comment [still being there so every time you go on your profile it's just there]. So it's probably a lot more hurtful [you know], and also everybody can see it unless you delete it." Male, Aged 20.

Emerging adults are also concerned about the privacy implications of SNSs and that their personal information can be harvested. However, some emerging adults express no concern about the risks on SNSs.

Although the adolescent group are concerned about their profile being viewed by others (particularly their parents), their concerns are different to the emerging adult age cohort and they consider impersonation, adding/meeting strangers and cyberbullying and stalking as risks that are of more concern to their age group.

5.4.4 Control of Risks

Respondents are asked to indicate whether they think people their age can control or stop the 12 risks associated with SNSs. Their control of each risk is measured on a 7 point bipolar (1 = very easily; 7= not easily) Likert scale. For ease of interpretation the risk measures are collapsed into three categories, Can Control (points 1 & 2 on the scale), Some Control (points 3, 4 & 5) and Not Much Control (points 6 & 7). Chart 5.25 shows that respondents perceive that they have most control of meeting in person a stranger that they have met on a SNS (94% can control or some control), that SNSs could replace the need to meet up with existing friends (94% can control or some control) and spending too much time on SNSs (86% can control or some control). Respondents perceive they have less control over the remaining risks.

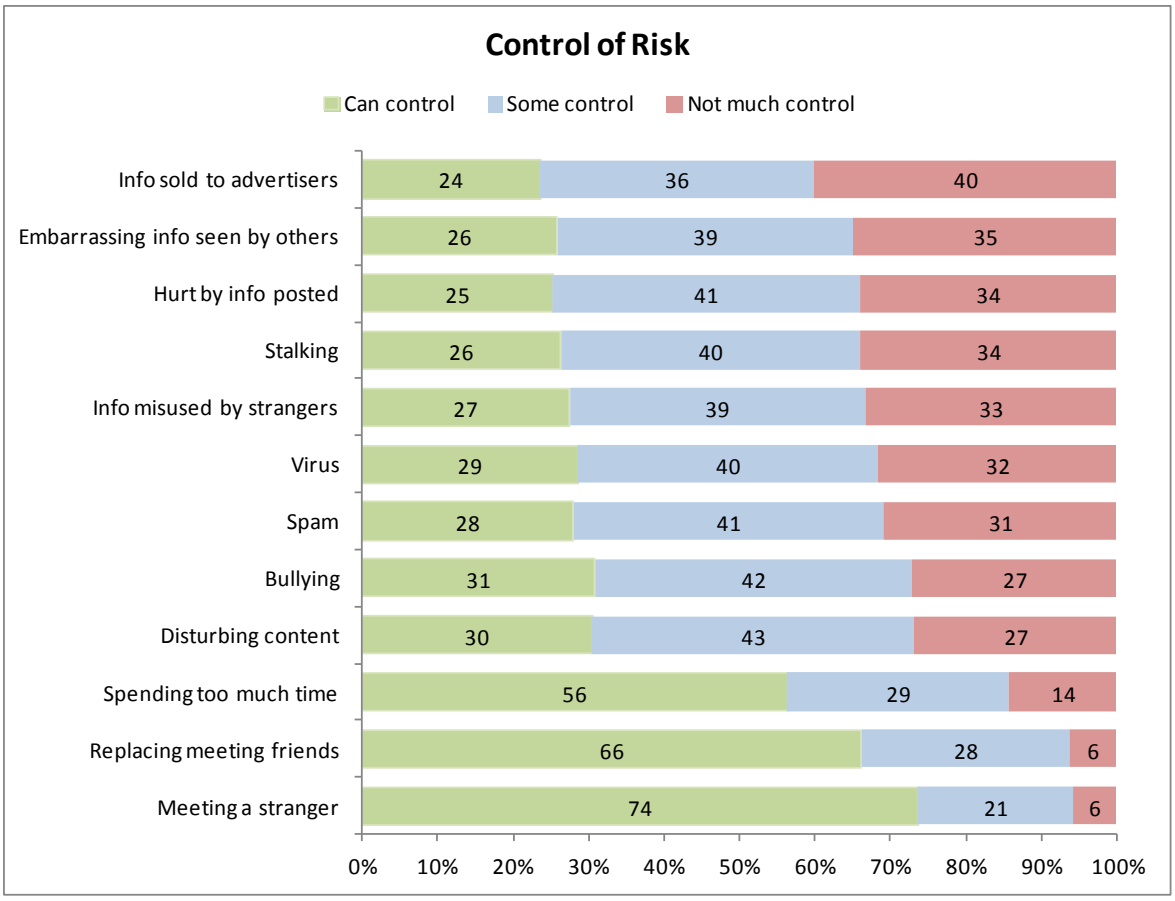


Chart 5.25 Control of Risk

A MANOVA analysis shows no evidence of a gender difference with regard to control over risk. There is evidence of an overall age cohort difference, Pillai's Trace = .156 F = 3.85, df = (36,2526), $p < 0.001$. From Chart 5.26 it can be seen that emerging adults perceive that they have significantly less control compared to the other age cohorts over embarrassing information being seen by others and being hurt by information that other post. Adults express higher levels of control over the time they spend online compared to the other age cohorts.

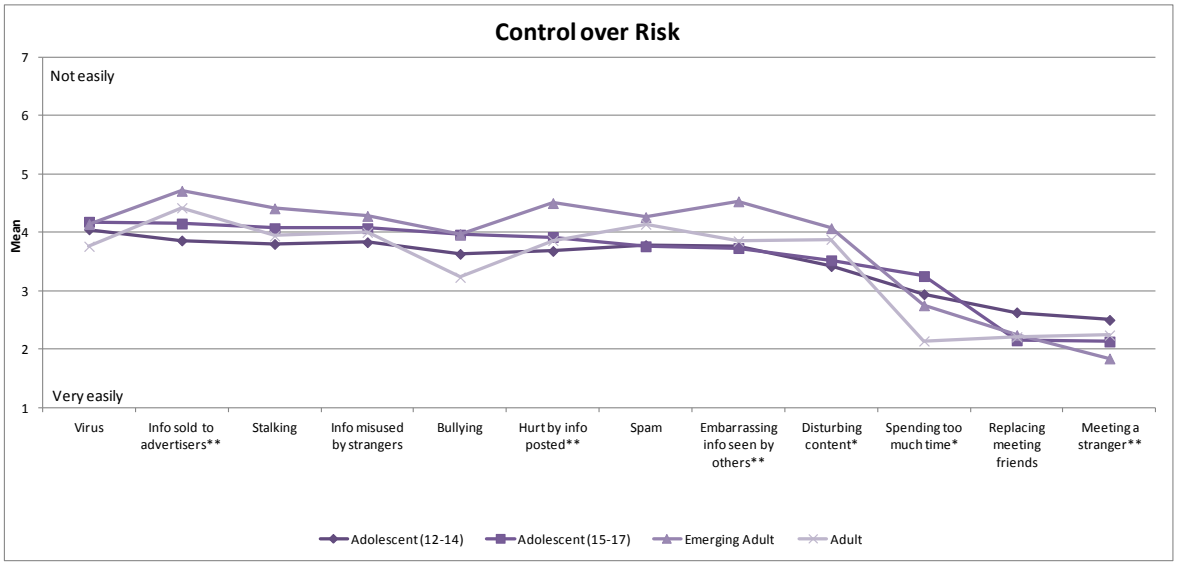


Chart 5.26 Mean Score for Control of Risk by Age Cohort

5.4.5 Severity of Risks

Respondents are asked about the harmful effects of the 12 risks associated with SNSs. Their rating for harm is measured on a 7 point bipolar (1 = not very severe; 7= very severe) Likert scale. The risk measures are collapsed into three categories, Not Severe (points 1 & 2 on the scale), Severe (points 3, 4 & 5) and Very Severe (points 6 & 7). Chart 5.27 shows that bullying and stalking are considered the most harmful risks on SNSs. 33% of respondents feel Spam is not a severe risk and nearly a quarter of respondents feel that spending too much time on SNSs is not a harmful risk.

A MANOVA is used to compare severity of risk across all twelve risks by age cohort and gender. The multivariate result is significant for gender, Pillai's Trace = .050, F = 3.46, df = (12,798), $p < 0.001$ and for age cohort, Pillai's Trace = .183, F = 4.45, df = (36,2466), $p < 0.001$. Chart 5.28 & Chart 5.29 show the mean score for severity of risk by gender and age cohort. Females score all the risks as more serious than males and in particular bullying, stalking, being hurt by information others post about you, information being misused by strangers, meeting a stranger and accidentally stumbling across uncomfortable content. To assess the gender effect on risk perceptions, a three-way loglinear analysis of severity of risk x personal likelihood of risk x gender is carried out for each risk. No significant higher order interactions are evident, indicating no evidence of a gender effect on risk perceptions.

In general adolescents compared to the other age cohorts rate the risks as more severe.

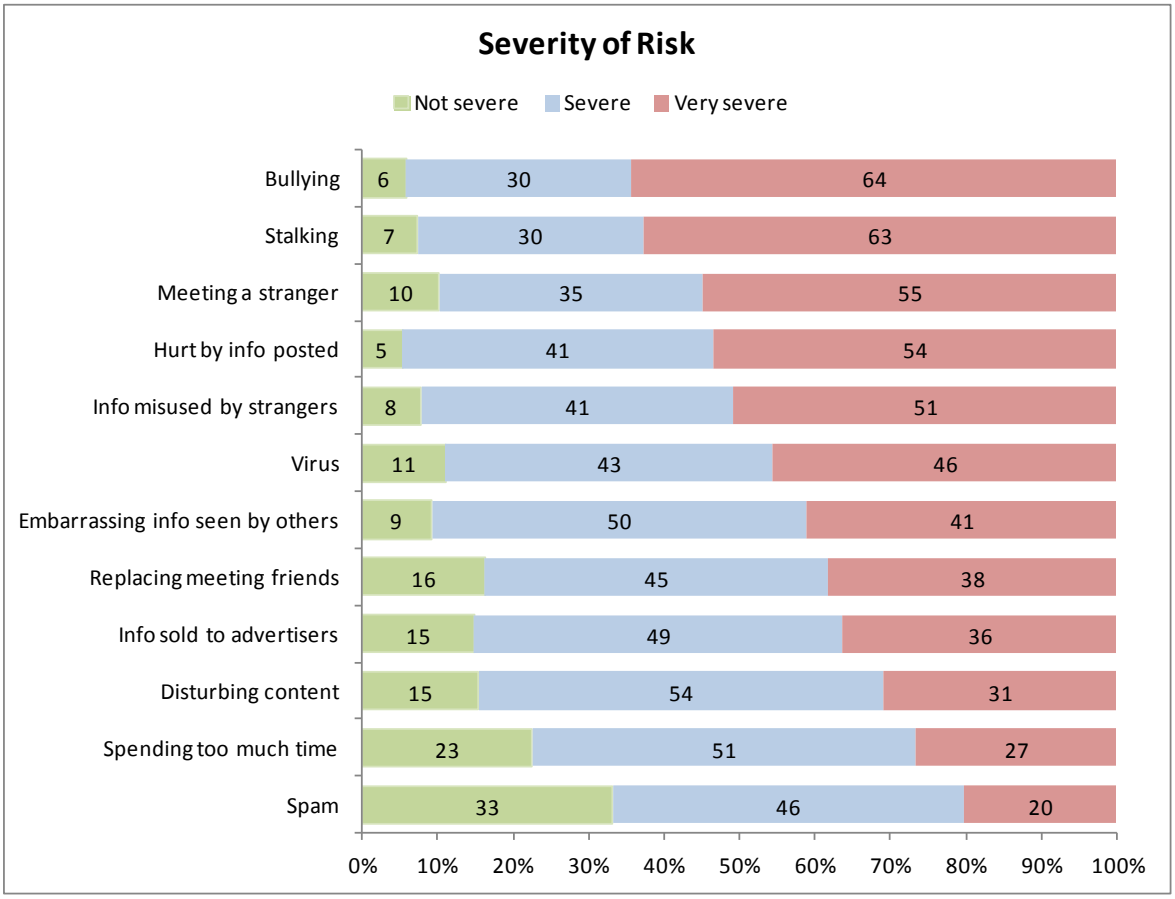


Chart 5.27 Severity of Risk

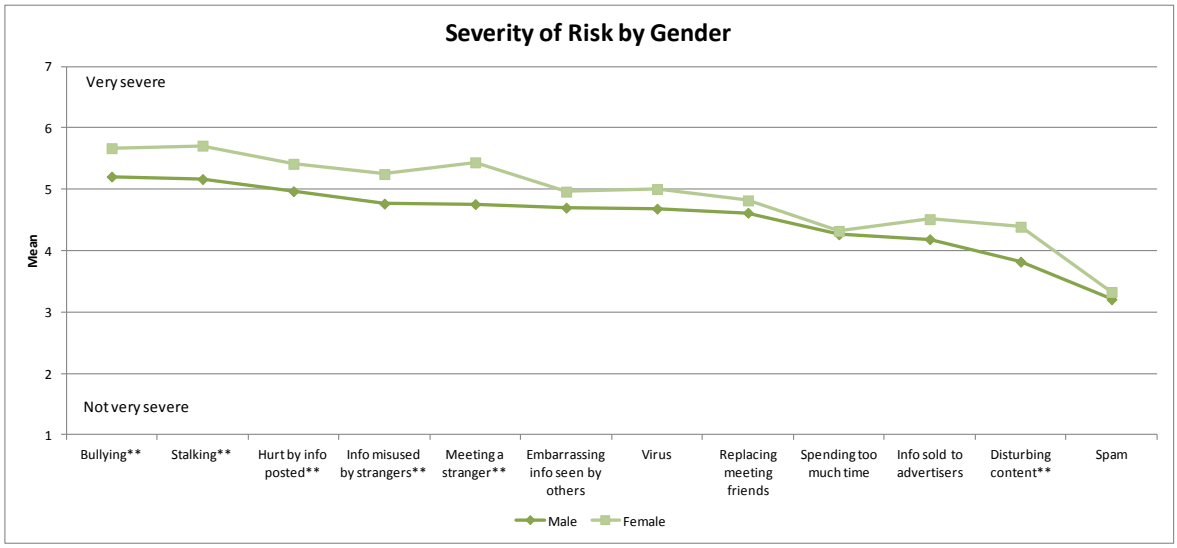


Chart 5.28 Mean Score for Severity of Risk by Gender

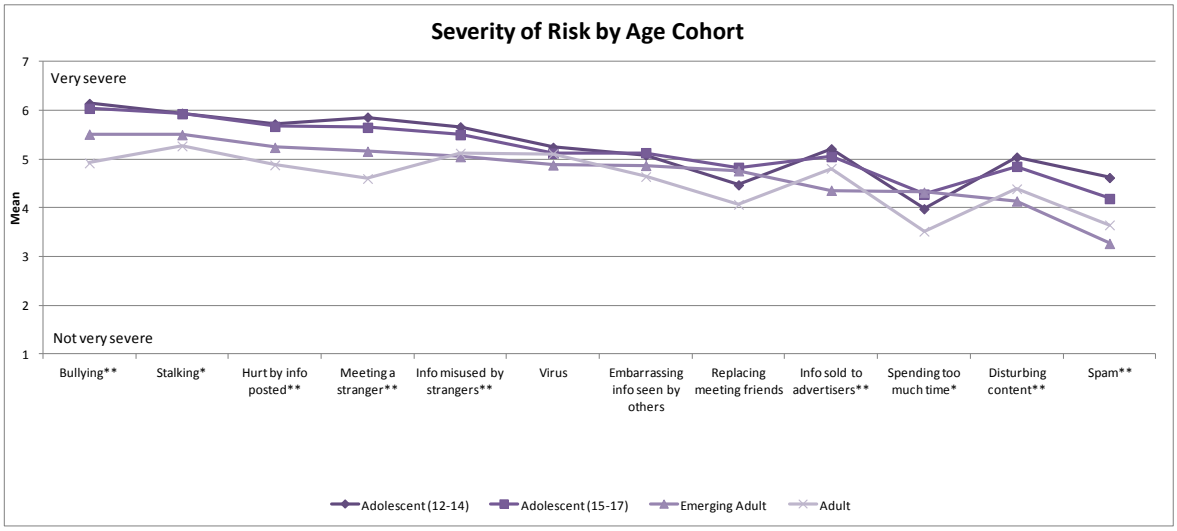


Chart 5.29 Mean Score for Severity of Risk by Age Cohort

Summary

Table 5.11 summarises the quantitative findings of Sections 5.4.1 to 5.4.5. The qualitative findings are summarised at the end of Section 5.4.6.

Risk Characteristic	General Findings	Gender	Age
Personal Risk (Likelihood)	The risks respondents perceive they are most likely to encounter are: • spam; • embarrassing information seen by others. The risks respondents perceive they are least likely to encounter are: • SNSs replacing the need to meet up with friends; • meeting strangers; • being bullied or harassed.	Males perceive that they are at a higher likelihood than females of: • meeting strangers; • personal information being sold to advertisers Females perceive that they are at a higher likelihood than males of: • spending too much time on SNSs; • having embarrassing information seen by others; • getting a virus.	Adolescents perceive themselves to be at a higher likelihood than the other age cohorts of encountering all the risks except for their personal information being sold to advertisers. Emerging adults perceive themselves to be at a lower likelihood than the other age cohorts of getting a virus. Adults perceive themselves to be at a lower likelihood than the other age cohorts of spending too much time on SNSs, but at a higher likelihood of their personal information being sold to advertisers.
Knowledge of Risk	Most risks are well known. Least well known risks are: • information on SNSs can be sold to advertisers; • viruses can be transmitted via SNSs. Those with higher levels of Internet experience do not show an increased knowledge of the risks.	No gender differences	Older adolescents have the highest level of knowledge about all 12 risks.

Risk Characteristic	General Findings	Gender	Age
Concern about Risks	Respondents are most concerned about the reputational risks that: • embarrassing information can be seen by others; • they can be hurt by information posted Respondents are least concerned about: • spending too much time on SNSs; • SNSs replacing the need to meet up with friends	No gender differences	Emerging adults show the lowest levels of concern about most risks. Adolescents are significantly more concerned than the other age cohorts about: • being bullied; • cyberstalking and • meeting strangers.
Control of Risks	Respondents feel they have most control over: • meeting strangers; • spending too much time on SNSs; • SNSs replacing the need to meet up with friends	No gender differences	Emerging adults perceive they have significantly less control compared to the other age cohorts over: • embarrassing information being seen by others; • being hurt by information that other post. Adults express higher levels of control over the time they spend online compared to the other age cohorts.
Severity of Risk	Respondents feel that the most harmful risks are: • bullying; • stalking. The least harmful risks are: • spam; • spending too much time on SNSs.	Females compared to males scored all the risks as more harmful.	Adolescents compared to the other age cohorts rate the risks as more severe.

Table 5.11 Summary of Findings – Risk Perceptions

5.4.6 Risk Perceptions – Other Qualitative Findings

This section presents further findings from the qualitative focus group discussions and in-depth interviews. The section discusses the benefits users perceive in SNSs, their views on specific risks and how they protect themselves from the risks on SNSs.

The interviewees highlight many benefits of using SNSs. All interviewees use SNSs to keep in contact with existing friends and family and in particular with those that they do not see very often.

"I think they're [kind of] useful for staying in touch more with your friends that you already have. Not for making new friends [or anything like that]." Male, Aged 20

Many interviewees find SNSs particularly useful for keeping in contact with weak ties as it is easier to make contact and communicate using SNSs.

"Facebook chat is [the lowest,] the most informal you can get [if you know what I mean]. If someone rang a person who you didn't speak to in years you'd be like hmmm but if they talk to you on Facebook you don't think anything of it [like]." Male, Aged 22.

"There is more of a reason [to chat] than to text someone out of the blue. It's easier to talk to them on Facebook." Male, Aged 16.

SNSs also fill a social need, in allowing users to see what is going on in their social circle. This means that users check their profiles regularly to make sure they are not missing out on anything.

"I think it [kind of] taps into a more basic need. [I mean] we are social animals and we like to feel connected and we like to feel as though we are interacting with people. And 'oh I have a notification, somebody is on my profile, somebody is interested in me or somebody had something that they wanted to say to me and I think that is addictive. It's looking for attention almost." Male, Aged 20

"Keeps you in the loop of everything that is going on." Male, Aged 16

A number of interviewees mention that SNSs are a form of distraction and a good form of entertainment. SNSs are increasingly becoming a common way to communicate online and many interviewees have friends that no longer use e-mail.

The qualitative interviews and discussion groups provide a deeper understanding of how users view the risks on SNSs. Neither the emerging adult nor the adolescent age groups perceive any risk with advertising. Advertising is not seen as intrusive and can be easily ignored.

"Advertising is annoying but it's just something you put up with [I suppose]. I would rather it was not there but it doesn't really bother me. I take no notice of it, and I would very rarely click into something. But if the other option is for us paying for it, I would have advertising any day of the week." Male, Aged 22.

"It's all on the side, don't look at it that much." Male, Aged 13.

Some interviewees think that the positive benefits of advertising outweigh the negative effects and some even see it as a business opportunity.

"[Maybe not, like they help, like for] advertising and commercial persuasion I think they're quite good [like cos] it's more efficient than having to waste a lot of paper having to hand out flyers [and stuff. And like] it's targeted really well for what people want, [you know] the advertisements at the side and [like] I don't think there's any big problem with that [like, it's just,] it's just a more efficient way of doing things [like. Like] it makes sense and [like] it does help people a lot, it's not all negative [at all like.]" Male, Aged 20.

Many of the emerging adult interviewees see stalking as a voyeuristic or nosey activity where they follow friends, ex partners etc. on SNSs and do not see it as a threatening risk.

"If a friend is stalking your page it doesn't really matter that much as long as it is not someone you don't know" Female, Aged 22.

Emerging adults feel that bullying is a bigger issue for younger users with only one interviewee perceiving it as an issue for emerging adults.

"But I do think bullying starts to fade out apart from a few exceptions as you go through life." Male, Aged 20

Spam is seen by some as an annoyance rather than a risk, but others recognise that spam and phishing attacks are increasingly coming from friends. Spam and phishing attacks occur more commonly on Bebo than on Facebook.

A number of emerging adult users feel that meeting a stranger is not a risk as users generally only accept friend requests from people they know or where they have a friend in common.

The adolescent groups highlight some emerging risks such the ability to pinpoint a user's location.

"Another risk is that there is a new thing if you have an iphone [or something] and it can say XXX is at the, and you can say exactly where you are right then. I think that is very risky [like] if you are writing it on Facebook everyone knows where you are and you don't know who could turn up or someone could start following you because they know where you are." Female, Aged 17

The qualitative interviews assess what measures users take to avoid risks. The risk avoidance techniques in use by the interviewees include:

- restricting profiles to be viewed by friends only;
- not accepting friend requests from strangers;
- restricting personal information revealed.

Most of the emerging adult interviewees use at least one of these avoidance techniques, but one interviewee uses none. Only half of the respondents use more than one technique. For emerging adults, the most commonly used technique is to restrict privacy settings and set profiles to be viewable by friends only. For the majority of users this is the only protective mechanism they use. Many interviewees state that they feel protected once they have restricted their profile to friends only.

Most of the adolescents interviewed have restricted their privacy settings to friends, but state that many of their peer group have not. Some adolescents admit that they find the

privacy settings on SNSs difficult to understand and therefore have not restricted their settings, as the following discussion illustrates:

"People can look at your details, the privacy settings aren't that good. Male1, Aged 15
That's your choice; you can hide your details. Male2, Aged 15
Privacy settings aren't that good, same on Bebo. Male3, Aged 14
Nah, you can set them however you want. It's your choice. Male2, Aged 15
I didn't know that. Male4, Aged 13
Some people don't know how to use that. Male3, Aged 14*"*

It is possible with SNSs to further customise privacy settings and only allow certain groups access to certain images, posts etc. A third of emerging adults have customised their privacy settings in this way and some express that it is difficult to do.

"But it really does require so much effort and so much conscious thought." Male, Aged 20

After restricting profiles, the next way that users protect themselves is to only accept friend requests from people they know. Some emerging adults state that they are careful who they add as friends, and generally only accept friend requests from someone they know or from friends of friends. All the adolescent groups acknowledge that there is a danger in accepting friend requests from strangers, but say that their peer group are likely to add strangers as friends as many adolescents compete to have the highest number of friends. There are games on SNSs that encouraged them to add more friends.

"[There is this like] on Facebook, if you have less than 50 friends everyone hates ya, if ya have 50-100 friends still everyone hates ya, if you have 100-150 you are alright [and all] and if you have over 10,000 friends you are a legend and everybody loves ya. I have about 140 friends on Facebook and they are all people I know. I don't understand how people, unless you are a celebrity and you have [like] 50,000 friends, how can you have like 1,000 friends. At least I can say every one of my friends on Facebook I have met them before and I know who they are. 150 people I know, not just a load of strangers." Female, Aged 15.

"Therewas a guy on Bebo and his afro got bigger depending on how many friends you had. That was a thing, people used to add people just to get that." Female, Aged 16.

All of the adolescent groups state that restricting the personal information displayed is a way to avoid risk but only a few emerging adults see this as a risk avoidance technique.

Many users (both emerging adult and adolescent) initially accept the default settings on the SNS and then in reaction to some incident or experience subsequently restrict their settings. These incidents include:

- something viewed on another users profile;
- becoming aware that employers or strangers might be looking at their profile;
- something negative happening to them on a SNS.

"[So let's say] if you're in a relationship with someone and you break up and you [can] change your relationship status in Facebook [down] to single. [Of course then] that goes in the news feed and everyone sees that you're now single. So I think those kinds of incidents along with trying to get jobs make you think about what do I want to share, what do I not want to share and then people start looking at stuff on their profile. But generally the first time someone is on Facebook they put it all out there and then it takes a few months to figure out [ok, well] I don't want everything out there and start taking things down. So eventually people find a happy balance that they're happy with and leave things the way they are." Male, Aged 22.

"[It's the thing] I only became aware of it from seeing other peoples stuff [cos] you don't really see your own stuff especially on Facebook, you wouldn't see what information of your own is going out you only see other peoples." Male, Aged 20.

"I only just changed it and if you consider I've been on Facebook for [what like] three or four years." Female, Aged 22.

Summary of Qualitative Findings – Risk Perceptions

Many of the qualitative findings back-up the findings of the quantitative analysis, but the qualitative findings also provide some interesting insights into how respondents perceive risk on SNSs. Further insights from the qualitative interviews show that:

- SNSs users tend to learn about the risks on SNSs from informal rather than formal sources;

- Adolescents feel that schools have an important role in informing students about the risks on SNSs;
- Some respondents feel it is the responsibility of SNS companies to inform users of the risks;
- A number of respondents feel that users with better IT skills are more likely to be aware of the risks and to be better protected. A quantitative analysis contradicts this assertion;
- In contrast to the quantitative findings, emerging adults think that time wasting on SNSs is the risk of greatest concern for their peer group;
- SNSs are seen as a form of distraction and a good form of entertainment;
- SNSs are increasingly becoming a common way to communicate online, sometimes surpassing email;
- Advertising on SNSs is not seen as intrusive and can be easily ignored;
- Many respondents see stalking as voyeuristic, rather than as a serious threat;
- Emerging adults do not see bullying as a concern for their age group;
- Spam is seen as an inconvenience, but respondents do recognise that phishing attacks are increasingly coming from friends;
- Emerging adults feel meeting a stranger is not a risk for them, as they do not accept friend requests from people they do not know;
- The adolescent focus groups highlight some new and emerging risks, such as the dangers associated with the ability to track location on mobile devices;
- The measures users take to avoid risk include:
    - restricting profiles to be viewed by friends only;
    - not accepting friend requests from strangers;
    - restricting personal information revealed.
- The most common measure used is to restrict profiles to be viewable by friends only and many users feel adequately protected by this measure;
- Many adolescents find it difficult to manage the privacy settings on SNSs;
- Adolescents are more likely to add strangers as friends as adolescents often compete to have the highest number of friends on SNSs and there are games on SNSs that encourage them to add more friends;
- Many users accept the default settings on SNSs and only change these settings in reaction to some incident or negative experience.

5.5 Logistic Regression

Binary logistic regression is applied in this analysis to help assess and describe the relative contribution of a number of variables to a respondent's perceived personal risk (likelihood) for a number of different risks that can occur on SNSs. The logistic regression analysis is carried out using the Block Logistic Regression procedure in SPSS 16.0 for Windows (release 16.0.1). Odd ratios (OR) are presented in these analyses. The odds ratio is a measure of association that approximates how much more likely (or unlikely) it is for the outcome to be present among those with x=1 (those at high risk) than those with x=0 (those not at high risk).

The effectiveness of each logistic regression model is assessed by examining: overall model evaluations; statistical tests of each explanatory variable; and goodness of fit statistics. The assumptions underlying logistic regression are checked. To test for collinearity, tolerance and VIV collinearity statistics, eigenvalues, condition indexes and variance proportions are examined.

From a review of the risk perception and social networking literature a model is derived of the factors that could influence perceived personal risk. This model is shown in Figure 5.1. This model suggests the factors that could influence perceived personal risks, including risk beliefs (such as knowledge of the risks, concern about the risks and how controllable the risks are), personal beliefs (such as an individual's disposition to trust and their level of privacy concern), contextual variables (such as intensity of SNS usage and the amount of personal information revealed on SNSs) and moderating variables including age cohort, gender, level of Internet experience and prior experience of the event.

An analysis is carried out to identify which of these characteristics are significant predictors of the likelihood of high personal risk perceptions.

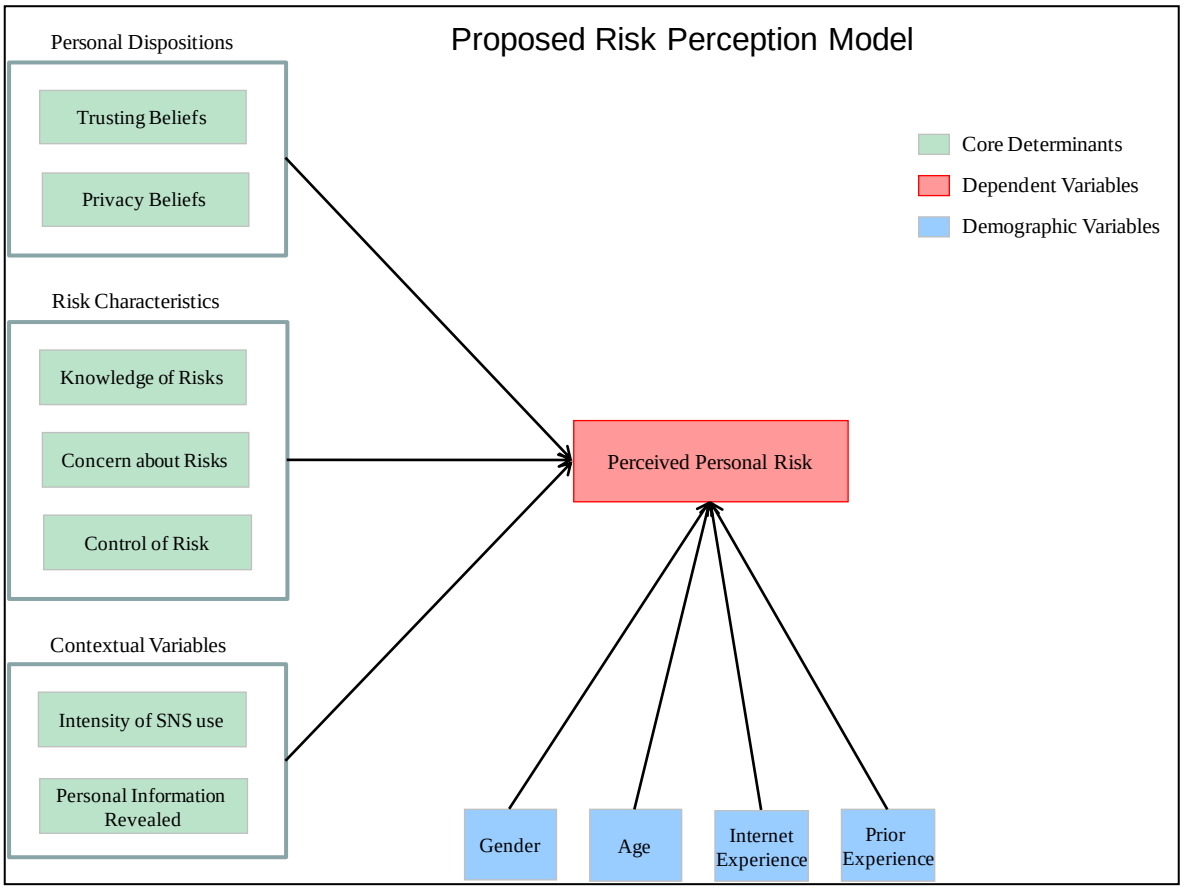


Figure 5.1 Proposed Model for Perceived Personal Risk

Personal risk perceptions are examined for five different risks that can be encountered on SNSs, to investigate if the type of risk produces different findings. The risks examined are:

1. Excessive use risk: spending too much time on SNSs;
2. Threatening risk: being bullied or harassed;
3. Reputational risk: embarrassing information or photos being seen by people who you would prefer didn't see it;
4. Personal information risk: personal information being sold to advertisers;
5. Technical risk: receiving spam

5.6 Logistic Regression – Excessive Use Risk

This section describes the binary logistic regression analysis of perceived personal risk for an excessive use risk such as spending too much time on SNSs. The outcome variable (perceived personal risk) is coded as 0 for not at high risk and 1 for high risk.

5.6.1 Univariate analyses – excessive use risks

From Chart 5.30 it can be seen that the proportions that perceive themselves to be at a high likelihood of spending too much time on SNSs increases with intensity of use. Respondents that have prior experience of spending too much time on SNSs are 6.5 times more likely to perceive themselves at high risk than those that have no prior experience.

Table 5.12 shows that respondents that perceive themselves to be at a high risk of spending too much time on SNSs express higher levels of knowledge about the risk, higher levels of concern about the risk and perceive the risk to be less controllable. Two variables, trusting beliefs and Internet experience have a p-value >0.25 and are not included in the multivariable model.

	Not at High Risk		At High Risk		
Variable	**Mean**	**SD**	**Mean**	**SD**	**Significance Test**
Personal Information Revealed	4.0	1.4	4.2	1.5	
Privacy Beliefs	4.3	1.7	4.6	1.7	
Trusting Beliefs	4.4	1.3	4.4	1.4	
Knowledge of Risk**	3.2	2.0	2.5	1.9	t(851)=4.58, p<0.001
Concern about Risk**	2.6	1.7	3.3	2.2	t(892)=4.98, p<0.001
Risk Controllable**	2.6	1.8	3.5	2.2	t(817)=5.26, p<0.001

Table 5.12 Summary Analysis of Continuous Variables by Perceived Personal Risk of Spending Too Much Time on SNSs.

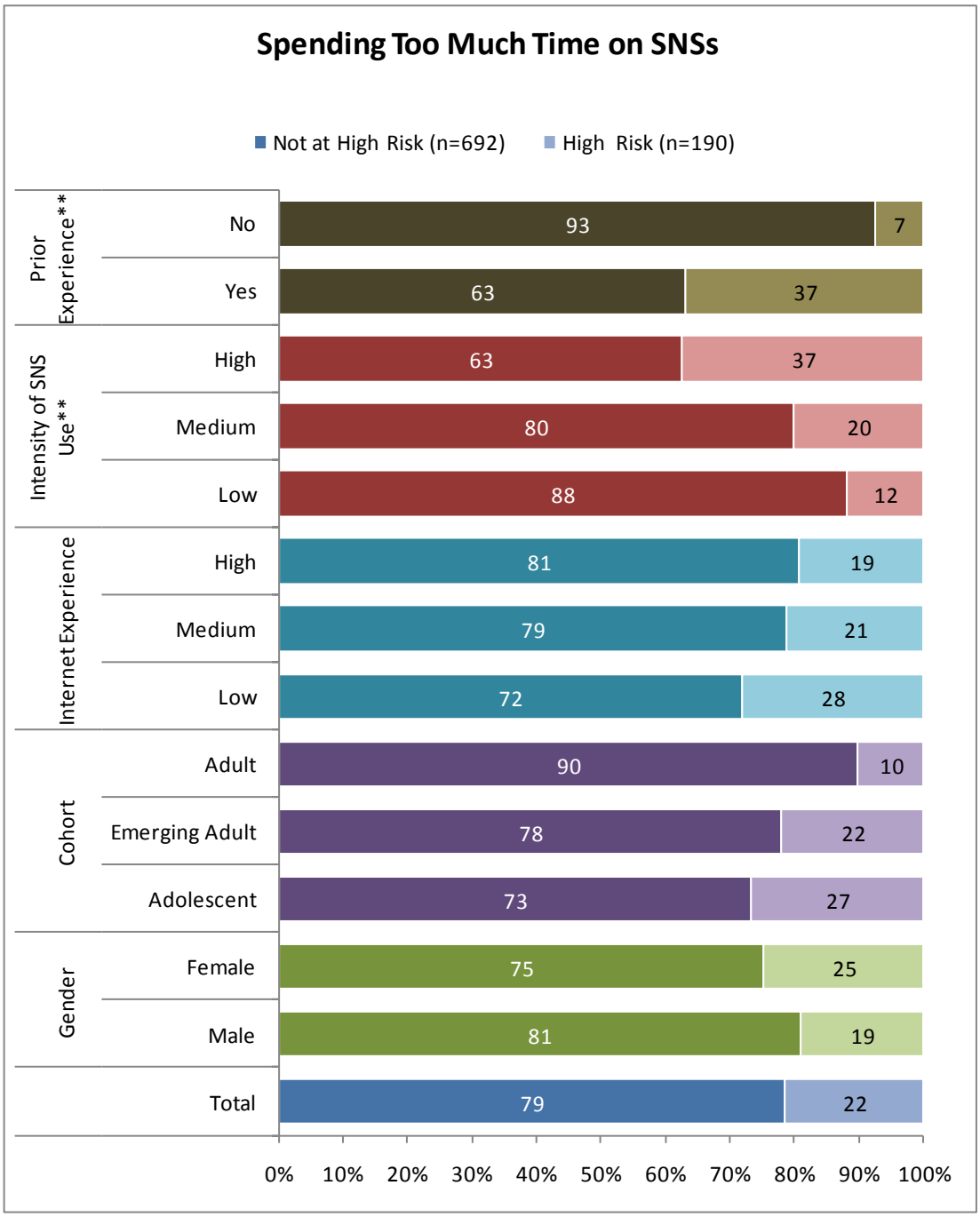


Chart 5.30 Summary Analysis of Categorical Variables by Perceived Personal Risk of Spending Too Much Time on SNSs.

5.6.2 Binary logistic analysis – excessive use risks

A sequential logistic model is fitted to the data and shows that a high perceived personal risk of spending too much time on SNSs is significantly predicted by knowledge of the risk, concern about the risk, perceived controllability of the risk and an interaction between age cohort and prior experience. Table 5.13 shows the odds ratios with 95% confidence intervals for the significant predictors of the logistic regression analysis. Full results are shown in Appendix N, Table N.1.

Predictor	e^{β} (OR)	95% CI for e^{β} Lower	Upper
Constant**	.108		
Prior Experience* (1 = Yes, 0 = No)	2.659	1.399	5.053
Knowledge of Risk*	1.165	1.048	1.295
Concern about Risk*	1.173	1.063	1.295
Risk Controllable**	1.192	1.086	1.308
Age Cohort (Adolescent) (reference)*	-	-	-
Age Cohort (Emerging Adult)**	.093	.026	.325
Age Cohort (Adult)	.737	.198	2.742
Age Cohort (Adolescent) by Prior Experience*	2.659	1.399	5.053
Age Cohort(Emerging Adult) by Prior Experience**	3.089	1.899	4.279
Age Cohort(Adult) by Prior Experience	2.282	0.548	4.016

Table 5.13 Logistic Regression Analysis of Perceived Personal Risk of Spending too Much Time on SNSs(1= High Risk, 0 = Not at High Risk). *p<0.05, **p<0.001

Controlling for all other variables in the model, a 1 unit increase in the concern about risk scale increases the odds of a individual perceiving themselves to be at high risk by 1.17 or 17%, a 1 unit increase in whether an individual perceives the risk to be less controllable increases the odds of a individual perceiving themselves to be at high risk by 19%. A 1 unit increase on the knowledge of risk scale (indicating a higher knowledge of the risk) increases the odds of an individual perceiving themselves to be at high risk by 16%.

As a statistically significant interaction effect is evident between age cohort and prior experience, these variables have to be interpreted together. Emerging adults that have experienced spending too much time on SNSs are 3 times as likely to perceive themselves at high risk, adolescents that have prior experience are 2.7 times as likely to perceive themselves at high risk and adults that have prior experience are 2.3 times as likely to perceive themselves at high risk.

Combining the explanatory variables that are found to be statistically significant in the logistic regression, individuals that perceive themselves to be at a high risk of spending too much time on SNSs express higher levels of concern about this risk, feel the risk to be less controllable, have an increased knowledge/awareness of the risk and of those that have prior experience, emerging adults perceive themselves to be at a higher risk, followed by the adolescent and adult age cohorts.

5.7 Logistic Regression – Threatening Risk

This section examines the binary logistic regression analysis of perceived personal risk of a threatening risk such as being bullied or harassed.

5.7.1 Univariate analyses – threatening risks

From the summary of the univariate analysis shown in Chart 5.31 it can be seen that a higher proportion of adolescents compared to emerging adults and adults perceive themselves to be at high risk of bullying and harassment. Those with lower levels of Internet experience perceive themselves to be at a higher risk of being bullied or harassed. Respondents that have prior experience are 4.4 times more likely to perceive themselves at high risk than those that have no prior experience.

Table 5.14 shows that respondents that perceive themselves to be at a high risk of being bullied and harassed express higher levels of concern about the risk. Three variables, intensity of use, privacy concern and knowledge of risk have a p-value >0.25 and are not included in the logistic regression model.

	Not at High Risk		At High Risk		
Variable	**Mean**	**SD**	**Mean**	**SD**	**Significance Test**
Personal Information Revealed	4.0	1.4	3.8	1.4	
Privacy Beliefs	4.3	1.7	4.4	1.7	
Trusting Beliefs	4.4	1.3	4.1	1.4	
Knowledge of Risk	2.8	1.7	2.7	2.2	
Concern about Risk**	3.6	1.8	5.5	1.8	t(824)=9.53, p<0.001
Risk Controllable	3.8	2.0	4.2	2.4	

Table 5.14 Summary Analysis of Continuous Variables by Perceived Personal Risk of Being Bullied or Harassed.

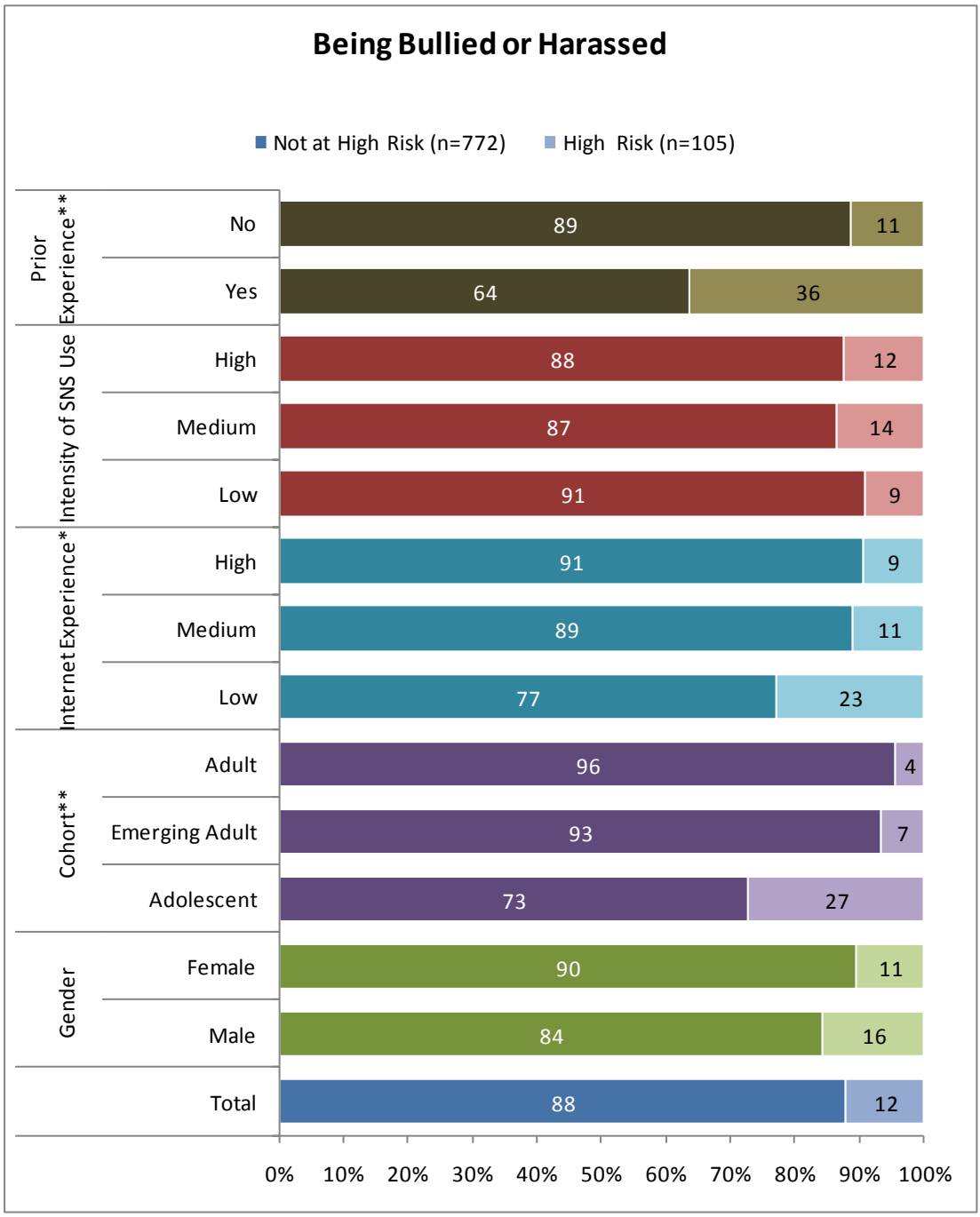


Chart 5.31 Summary Analysis of Categorical Variables by Perceived Personal Risk of Being Bullied or Harassed.

5.7.2 Binary logistic analysis – threatening risks

A sequential logistic model is fitted to the data to test the variables and interaction effects highlighted in the univariate analysis. The result shows that a high perceived personal risk of being bullied or harassed is significantly predicted by prior experience, concern about the risk, disposition to trust and age cohort. Table 5.15 shows the results for the statistically significant predictors of the logistic regression analysis. Full results are shown in Appendix N, Table N.2.

Predictor	e^{β} (OR)	95% CI for e^{β} Lower	Upper
Constant**	.077		
Prior Experience* (1 = Yes, 0 = No)	3.157	1.483	6.723
Concern about Risk**	1.574	1.365	1.814
Age Cohort (Adolescent) (reference)**	-	-	-
Age Cohort (Emerging Adult)**	.301	.181	.502
Age Cohort (Adult)	.208	.026	1.650
Disposition to Trust*	1.216	1.011	1.464

Table 5.15 Logistic Regression Analysis of Perceived Personal Risk of Being Bullied or Harassed (1= High Risk, 0 = Not at High Risk). *p<0.05, **p<0.001

Controlling for all other variables in the model, a 1 unit increase in the concern about risk scale increases the odds of an individual perceiving themselves to be at high risk of being bullied or harassed by 57%, a 1 unit increase on the disposition to trust scale (indicating an individual is less trusting) increases the odds of an individual perceiving themselves to be at high risk of being bullied or harassed by approximately 22%.

For the experience of risk categorical variable, individuals that have prior experience are just over 3 times as likely as those that have no prior experience to perceive themselves to be at a high risk of being bullied or harassed.

For age cohort, adolescents are the reference group. The odds of an individual perceiving themselves to be at a high risk of being bullied or harassed are .3 times lower for emerging adults compared to adolescents.

Combining the explanatory variables that are found to be statistically significant in the logistic regression, individuals that perceive themselves to be at a high risk of being bullied or harassed on SNSs express higher levels of concern about this risk, are less trusting, are more likely to have prior experience and are more likely to be adolescents as opposed to emerging adults.

5.8 Logistic Regression – Reputational Risk

This section describes the binary logistic regression analysis of perceived personal risk of a reputational risk such as having embarrassing information being seen by people the respondent would prefer didn't see it.

5.8.1 Univariate analyses – reputational risk

A univariate analyses is carried out to highlight variables that have a significant relationship to the outcome variable and to find variables that can be removed from the model. From Chart 5.32 it can be seen that a higher proportion of adolescents compared to emerging adults and adults perceive themselves to be at high risk of having embarrassing information/photos or photos being seen by people who they would prefer didn't see it. The perception of this risk rises with intensity of SNS use, with 35% of high intensity users perceiving themselves to be at risk, as opposed to 19% of low intensity users. Respondents that have prior experience are 3.3 times more likely to perceive themselves at high risk than those that have no prior experience.

Table 5.16 shows that respondents that perceive themselves to be at a high risk of having embarrassing information/photos or photos being seen by people who they would prefer didn't see it express higher levels of knowledge about the risk, higher levels of concern about the risk and perceive the risk to be less controllable. They also express higher levels of privacy concern. One variable, trusting beliefs exceeds the cut-off and is not included in the multivariable model. Further analysis is carried out to examine interactions among variables.

	Not at High Risk		At High Risk		
Variable	**Mean**	**SD**	**Mean**	**SD**	**Significance Test**
Personal Information Revealed	4.0	1.4	4.2	1.3	
Privacy Beliefs*	4.2	1.7	4.6	1.7	t(760)=2.80, p=0.005
Trusting Beliefs	4.4	1.3	4.3	1.3	
Knowledge of Risk**	2.6	1.7	2.1	1.7	t(841)=3.27, p=0.001
Concern about Risk**	4.2	1.9	5.3	1.8	t(822)=7.80, p<0.001
Risk Controllable**	3.9	2.0	4.8	2.1	t(808)=5.40, p<0.001

Table 5.16 Summary Analysis of Continuous Variables by Perceived Personal Risk of Embarrassing Information or Photos Being Seen by People Who you Would Prefer Didn't See it.

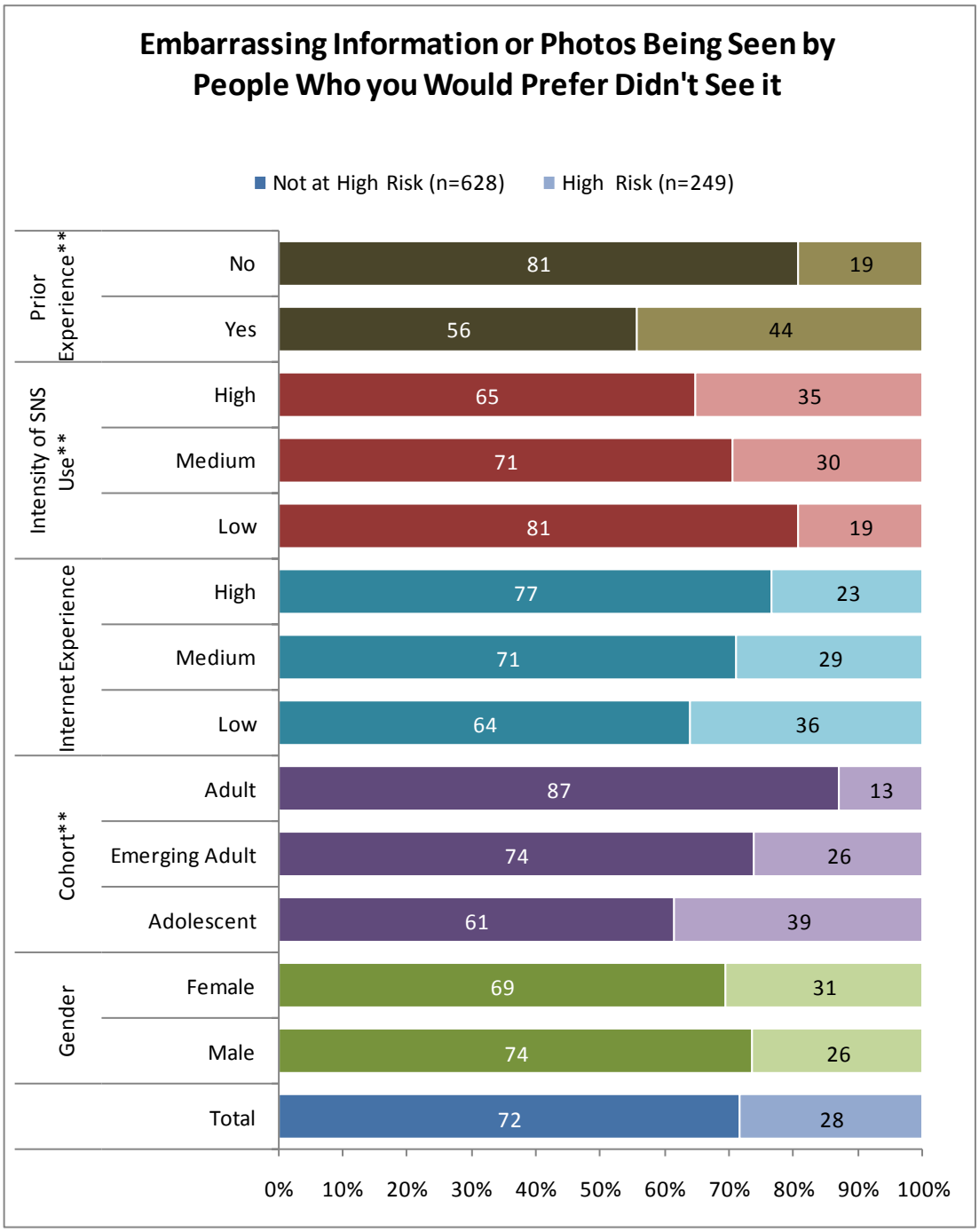


Chart 5.32 Summary Analysis of Categorical Variables by Perceived Personal Risk of Embarrassing Information or Photos Being Seen by People Who you Would Prefer Didn't See it.

5.8.2 Binary logistic analysis – reputational risk

A sequential logistic model shows that a high perceived personal risk of having embarrassing information/photos being seen by people who you would prefer didn't see them is significantly predicted by prior experience, concern about the risk, perceived controllability of the risk and age cohort. Table 5.17 shows the odds ratios and 95% CI for

the statistically significant predictors of the logistic regression analysis. Full results are shown in Appendix N, Table N.3.

Predictor	e^{β} (OR)	95% CI for e^{β} Lower	Upper
Constant**	.064		
Prior Experience** (1 = Yes, 0 = No)	2.957	2.077	4.209
Concern about Risk**	1.320	1.194	1.460
Risk Controllable*	1.149	1.052	1.256
Age Cohort (Adolescent) (reference)**	-	-	-
Age Cohort (Emerging Adult)**	.427	.292	.624
Age Cohort (Adult)*	.363	.147	.893

Table 5.17 Logistic Regression Analysis of Perceived Personal Risk of Embarrassing Information or Photos Being Seen by People Who you Would Prefer Didn't See it (1= High Risk, 0 = Not at High Risk). *p<0.05, **p<0.001

Controlling for all other variables in the model, a 1 unit increase in the concern about risk scale increases the odds of a individual perceiving themselves to be at high risk of having embarrassing information/photos being seen by people they would prefer didn't see them by 32%, a 1 unit increase on the control of risk scale increases the odds of a individual perceiving themselves to be at high risk by 1.15 or by 15%.

For the prior experience categorical variable, individuals that have prior experience are nearly 3 times as likely to perceive themselves to be at high risk compared to those that have no prior experience.

For age cohort, adolescents are the reference group. The odds of an individual perceiving themselves to be at a high risk of having embarrassing information/photos being seen by people they would prefer didn't see them are .43 times lower for emerging adults compared to adolescents and .36 times lower for adults compared to adolescents.

Overall individuals that perceive themselves to be at a high risk of having embarrassing information/photos being seen by people they would prefer didn't see them on SNSs express higher levels of concern about this risk, perceive the risk to be less controllable are more likely to have prior experience and are more likely to be adolescents as opposed to emerging adults or adults.

5.9 Logistic Regression – Personal Information Risk

This section describes the binary logistic regression analysis of high perceived personal risk of a personal information risk such as personal information being misused by strangers.

5.9.1 Univariate analyses – personal information risk

From Chart 5.33 it can be seen that a higher proportion of adolescents compared to emerging adults and adults perceive themselves to be at high risk of having their personal information misused by strangers. Respondents that have prior experience of this risk are 4.3 times more likely to perceive themselves at high risk than those that have no prior experience.

Table 5.18 shows that respondents that perceive themselves to be at a high risk express higher levels of concern about the risk, express higher privacy concern levels and have a lower disposition to trust. Three variables, intensity of use, personal information revealed and internet experience have a p-value >0.25 and are not included in the multivariable model.

	Not at High Risk		At High Risk		
Variable	**Mean**	**SD**	**Mean**	**SD**	**Significance Test**
Personal Information Revealed	4.0	1.4	3.9	1.5	
Privacy Beliefs**	4.2	1.6	4.8	1.7	t(762)=3.70, p<0.001
Trusting Beliefs*	4.4	1.3	4.1	1.4	t(765)=2.63, p=0.009
Knowledge of Risk	3.5	1.9	3.4	2.2	
Concern about Risk**	3.7	1.8	4.8	2.0	t(819)=7.40, p<0.001
Risk Controllable	4.0	2.1	4.4	2.2	

Table 5.18 Summary Analysis of Continuous Variables by Perceived Personal Risk of Personal Information Being Misused by Strangers.

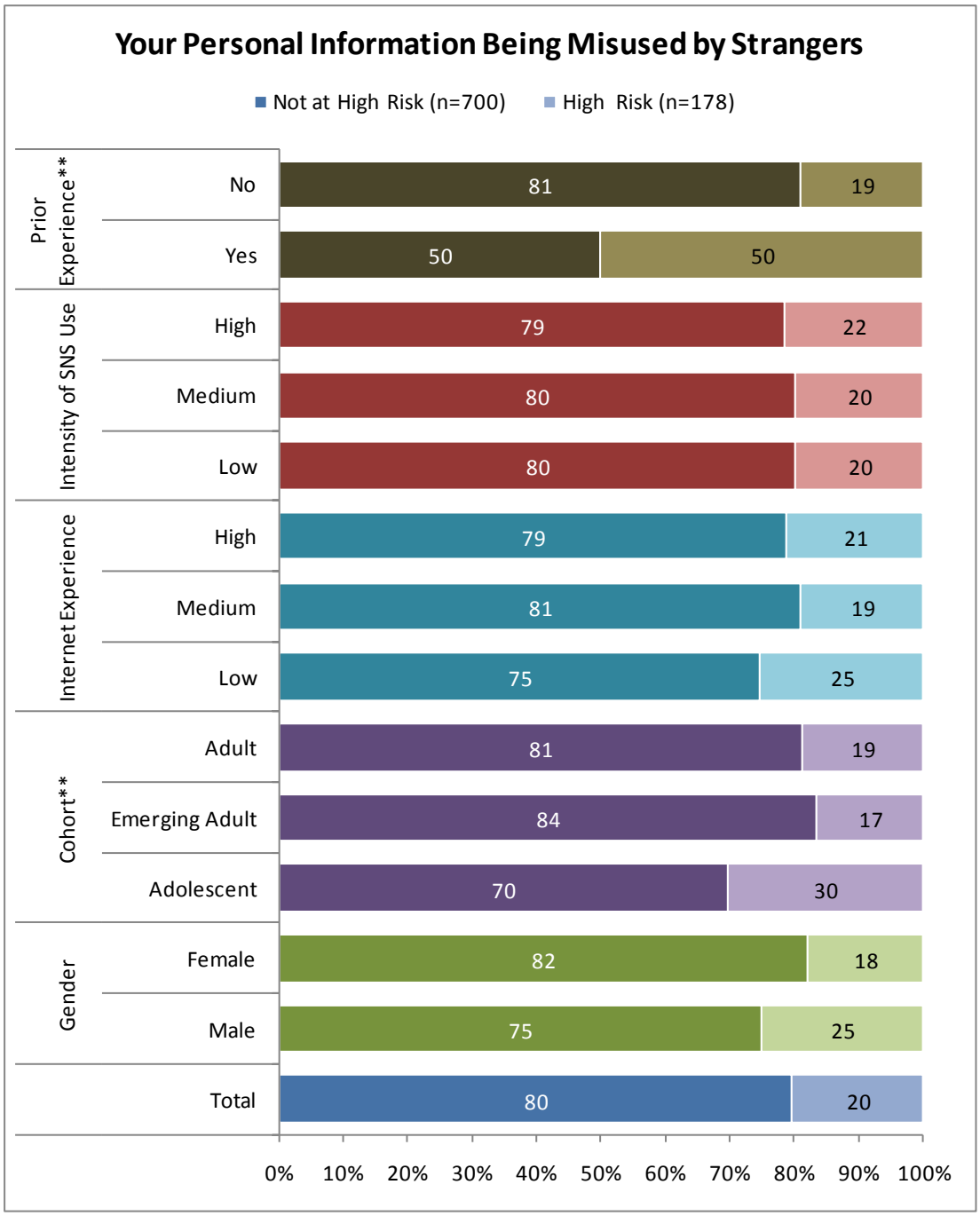


Chart 5.33 Summary Analysis of Categorical Variables by Perceived Personal Risk of Personal Information Being Misused by Strangers.

5.9.2 Binary logistic analysis – personal information risk

A sequential logistic model shows that a high perceived personal risk of personal information on SNSs being misused by strangers is significantly predicted by prior experience, concern about the risk and age cohort. Table 5.19 shows the results of the logistic regression analysis. Full results are shown in Appendix N, Table N.4.

Predictor	$e^{ß}$ (OR)	95% CI for $e^{ß}$ Lower	Upper
Constant**	.037		
Prior Experience**	4.224	2.183	8.173
(1 = Yes, 0 = No)			
Concern about Risk**	1.367	1.229	1.520
Privacy Concern*	1.233	1.093	1.390
Age Cohort (Adolescent) (reference)*			
Age Cohort (Emerging Adult)*	.531	.354	.796
Age Cohort (Adult)	.872	.304	2.505

Table 5.19 Logistic Regression Analysis of Perceived Personal Risk of Personal Information Being Misused by Strangers (1= High Risk, 0 = Not at High Risk). *p<0.05, **p<0.001

Controlling for all other variables in the model, a 1 unit increase in the concern about risk scale increases the odds of an individual perceiving themselves to be at high risk of having their personal information being misused by strangers by 1.37. A 1 unit increase on the privacy concern scale increases the odds of a individual perceiving themselves to be at high risk of getting this risk by 23%.

For the prior experience categorical variable, individuals that have experienced having their personal information misused by strangers are 4.2 times as likely to perceive themselves to be at high risk compared to those that have no prior experience.

For age cohort, adolescents are the reference group. The odds of an individual perceiving themselves to be at a high risk of this risk are .53 times lower for emerging adults compared to adolescents.

Overall individuals that perceive themselves to be at a high risk of having their personal information on SNSs being misused by strangers express higher levels of concern about this risk, are more likely to have prior experience, express increased online privacy concerns and are more likely to be adolescents.

5.10 Logistic Regression – Technology Risk

This section describes the binary logistic regression analysis of high perceived personal risk of a risk attributable to technology such as getting spam on SNSs.

5.10.1 Univariate analyses – technology risk

Chart 5.34 shows that a higher proportion of males compared to females perceive themselves to be at higher risk of spam. Respondents that have prior experience of spam are 4 times more likely to perceive themselves at high risk than those that have no prior experience.

Table 5.20 shows that respondents that perceive themselves to be at a high risk of spam express higher levels of concern about the risk, have a higher knowledge of the risk and perceive the risk to be less controllable. One variable, intensity of use has a p-value >0.25 and is not included in the multivariable model.

	Not at High Risk		At High Risk		
Variable	**Mean**	**SD**	**Mean**	**SD**	**Significance Test**
Personal Information Revealed	4.0	1.4	4.0	1.4	
Privacy Beliefs	4.3	1.7	4.5	1.6	
Trusting Beliefs	4.4	1.3	4.3	1.3	
Knowledge of Risk**	3.4	1.9	2.9	2.0	t(835)=3.73, p<0.001
Concern about Risk**	3.0	1.7	4.0	2.0	t(817)=7.20, p<0.001
Risk Controllable**	3.8	2.0	4.6	2.2	t(802)=4.80, p<0.001

Table 5.20 Summary Analysis of Continuous Variables by Perceived Personal Risk of Spam.

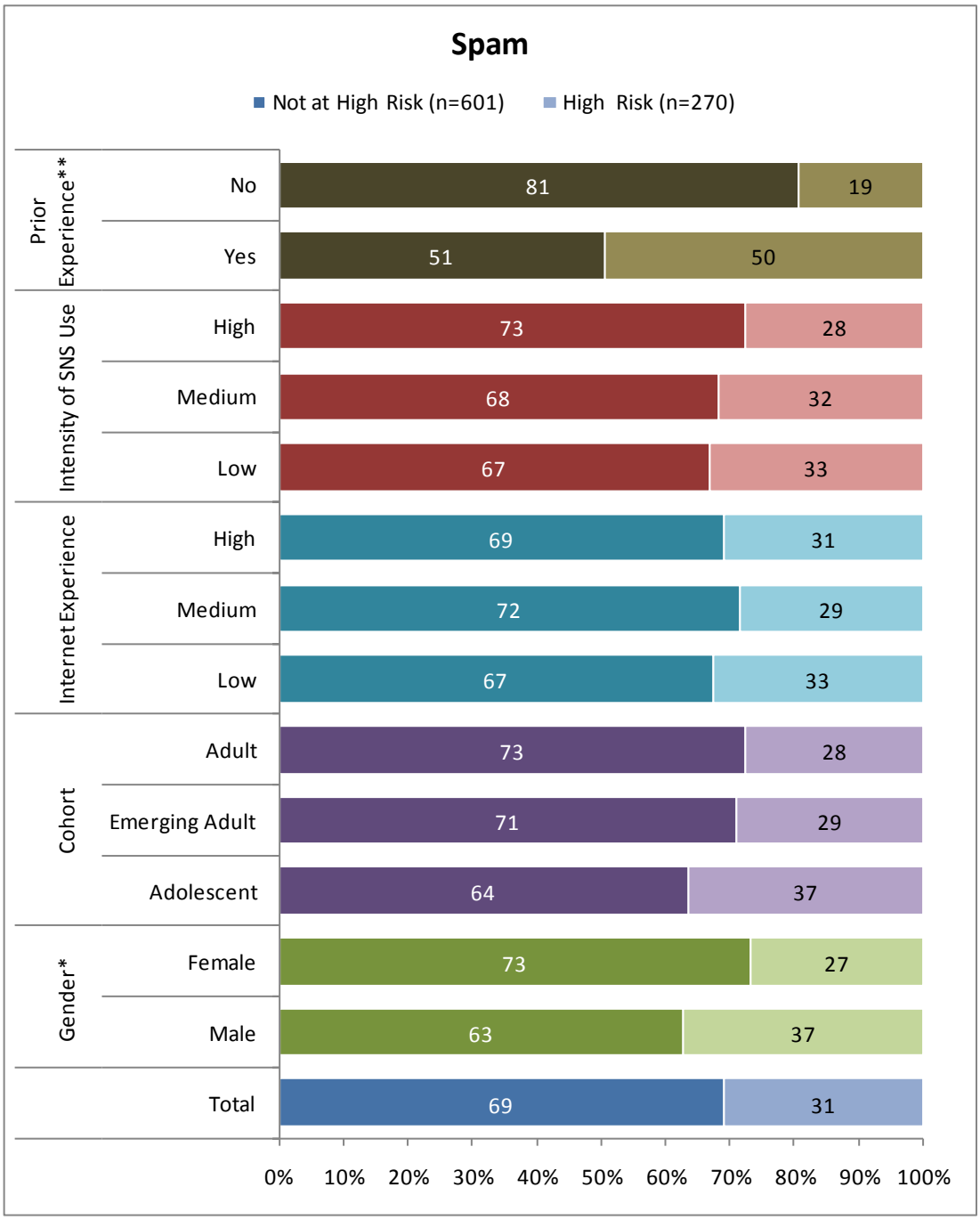


Chart 5.34 Summary Analysis of Categorical Variables by Perceived Personal Risk of Spam.

5.10.2 Binary logistic analysis – technology risk

A sequential logistic model fitted to the data showed that a high perceived personal risk of getting spam on SNSs is significantly predicted by prior experience, concern about the risk, perceived controllability of the risk, disposition to trust and age cohort. Table 5.21 shows the results of the logistic regression analysis. Full results are shown in Appendix N, Table N.5.

Predictor	e^{β} (OR)	95% CI for e^{β} Lower	Upper
Constant**	.182		
Prior Experience** (1 = Yes, 0 = No)	3.891	2.732	5.540
Concern about Risk**	1.268	1.158	1.389
Risk Controllable*	1.129	1.038	1.228
Disposition to Trust*	1.17	1.020	1.340
Age Cohort (Adolescent) (reference)*	-	-	-
Age Cohort (Emerging Adult)**	.586	.403	.854
Age Cohort (Adult)	1.075	.397	2.911

Table 5.21 Logistic Regression Analysis of Perceived Personal Risk of Spam (1= High Risk, 0 = Not at High Risk). *p<0.05, **p<0.001

Controlling for all other variables in the model, a 1 unit increase in the concern about risk scale increases the odds of a individual perceiving themselves to be at high risk of getting spam on SNSs by 27%, a 1 unit increase on the control of risk scale increases the odds of a individual perceiving themselves to be at high risk by 1.13 or by 13%. A 1 unit increase on the disposition to trust scale (indicating a lower disposition to trust) increases the odds of a individual perceiving themselves to be at high risk of getting spam on SNSs by 17%.

For the prior experience categorical variable, individuals that experienced getting spam on SNSs are nearly 4 times as likely to perceive themselves to be at a high risk compared to those that have not received spam on SNSs.

For age cohort, adolescents are the reference group. The odds of an individual perceiving themselves to be at a high risk of getting spam on SNSs are .586 times lower for emerging adults compared to adolescents.

Overall individuals that perceive themselves to be at a high risk of getting spam on SNSs express higher levels of concern about this risk, perceive the risk to be less controllable, are less trusting, are more likely to have prior experience of receiving spam and are more likely to be adolescents as opposed to emerging adults.

5.11 Summary Perceived Personal Risk

Table 5.22 summarises the findings of the logistic regressions carried out in sections 5.6 through to 5.10.

Controlling for all other variables in the model, for all five risks, prior experience is the most significant predictor of a respondent perceiving themselves to be at high risk. Depending on the risk, individuals that have prior experience of a risk are between 3 and 4 times as likely to perceive themselves at high risk compared to those that have no prior experience. For the excessive use risk of spending too much time on SNSs, emerging adults that have experienced spending too much time on SNSs are 3 times as likely to perceive themselves at high risk, adolescents that have prior experience are 2.7 times as likely to perceive themselves at high risk and adults that have prior experience are 2.3 times as likely to perceive themselves at high risk compared to those that have no prior experience.

Age cohort effects are evident for all the risk categories. For all the risks apart for the excessive use risk adolescents are more likely that the other age cohorts to perceive themselves at high risk.

Concern about risk is a significant predictor for the likelihood of high risk perception for all types of risk. A 1 unit increase in the concern about risk scale increases the odds of an individual perceiving themselves to be at high risk by somewhere between 17% to 57%, depending on the risk. This indicates that individuals that perceive themselves to be at a high risk express higher levels of concern about these risks. Control over risk is a significant predictor (increased odds between 13% and 19%) for the likelihood of high risk perception for the excessive use risk, reputational risk and technical risk. Individuals that perceive themselves to be at a high risk perceive these risks to be less controllable. Knowledge of risk is only a significant predictor (increased odds of 16%) for the likelihood of high risk perception for the excessive use risk of spending too much time on SNSs. Individuals that perceive themselves to be at a high risk of spending too much time on SNSs have an increased knowledge/awareness of this risk. A 1 unit increase on the disposition to trust scale (indicating a lower disposition to trust) increases the odds of an individual perceiving themselves to be at high risk of being bullied or harassed by 22% and getting spam on SNSs by 17%. Overall individuals that perceive themselves to be at a

high risk of being bullied or harassed and getting spam are less trusting. A 1 unit increase on the privacy concern scale (indicating a increased concern about privacy) increases the odds of an individual perceiving themselves to be at high risk of their personal information being misused by strangers by 23%. Overall individuals that perceive themselves to be at a high risk of this personal information risk are more concerned about their online privacy.

The level of Internet experience, intensity of SNS use, amount of personal information revealed and an individual's online privacy concern are not significant predictors of the likelihood that an individual perceives themselves to be at high risk. Gender is not a significant predictor for any of the risk categories.

It is important to note that no conclusions can be drawn with regard to which variable is causing changes to the other. For example, it is unclear whether having an increased concern about a risk is a cause or a consequence of a high risk perception.

	Odds Ratios (95% CI Lower, Upper)				
	Excessive Use Risk	**Threatening Risk**	**Reputational Risk**	**Personal Information Risk**	**Technical Risk**
	Spending Too Much Time on SNS	Being Bullied or Harassed	Embarrassing Info/Photos Seen by Others	Information misused by strangers	Receiving Spam
Moderating Variables					
Gender (1 = Male,0 = Female)					
Age Cohort (Adolescent)(reference)	Interaction	-**	-**	-*	-*
Age Cohort (Emerging Adult)		0.30** (0.18, 0.50)	0.43** (0.29, 0.62)	0.53** (0.35, 0.80)	0.58** (0.40, 0.85)
Age Cohort (Adult)			0.36* (0.15, 0.89)		
Prior Experience (1 = Yes,0 = No)	Interaction	3.16** (1.48, 6.72)	2.96** (2.08, 4.21)	4.22** (2.18, 8.17)	3.89** (2.73, 5.54)
Internet Experience (1 = Low,2 = Medium,3 = High)					
Age Cohort (Adolescent) x Prior Experience	2.66 (1.40, 5.05)				
Age Cohort (Emerging Adult) x Prior Experience	3.09 (1.90, 4.28)				
Age Cohort (Adult) x Prior Experience	2.28 (0.55, 4.02)				
Risk Beliefs					
Increasing Concern about Risk	1.17* (1.06, 1.30)	1.57** (1.36, 1.81)	1.32** (1.19, 1.46)	1.37** (1.22, 1.52)	1.27** (1.16, 1.39)
Decreasing Control over Risk	1.19* (1.09, 1.31)		1.15* (1.05, 1.26)		1.13* (1.04, 1.23)
Increasing Knowledge of Risk	1.16* (1.05, 1.30)				
Personal Disposition					
Decreasing Disposition to Trust		1.22* (1.01, 1.47)			1.17* (1.02, 1.34)
Increasing Privacy Concern				1.23* (1.09, 1.39)	
Contextual Variables					
Intensity of SNS Use (1 = Low,2 = Medium,3 = High)					
Personal Information Revealed					

Table 5.22 Summary of Logistic Regression Analysis (odds ratios) of Perceived Personal Risk (1= High Risk, 0 = Not at High Risk). *p<0.05, **p<0.001

5.12 Optimistic Bias

Previous research has shown that individuals tend to believe that they are less likely to encounter negative events and more likely to encounter positive events than the average person (Weinstein, 1980). This phenomenon is known as "*unrealistic optimism*" or "*optimistic bias*". To assess optimistic bias, for each risk, respondents are asked to rate the likelihood that they personally will experience the risk and rate the likelihood that the average person their age will experience the same event. Both of these items are measured on a 7 point bipolar (1 = not at all at risk; 7= very much at risk) Likert scale. The participant's personal likelihood estimate is then subtracted from the peer group estimate to generate a difference score. A positive score indicates an optimistic bias, the larger the score, the greater the optimistic bias.

Chart 5.35 shows the mean score for perceived personal risk compared to the mean score for perceived risk to others. For all the risks, except spam and information from SNSs being sold to advertisers, respondents perceived the risk to others is higher than the risk to themselves.

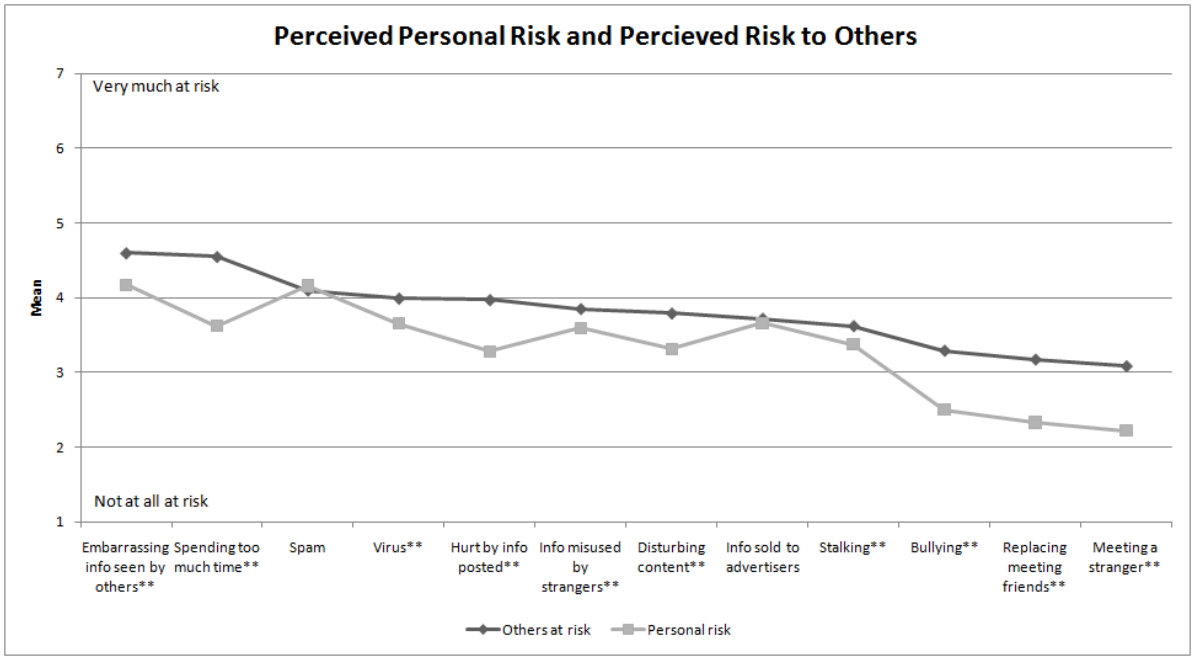


Chart 5.35 Mean Score for Perceived Personal Risk and Perceived Risk to Others.

Chart 5.36 shows the mean difference scores for each of the 12 risks.

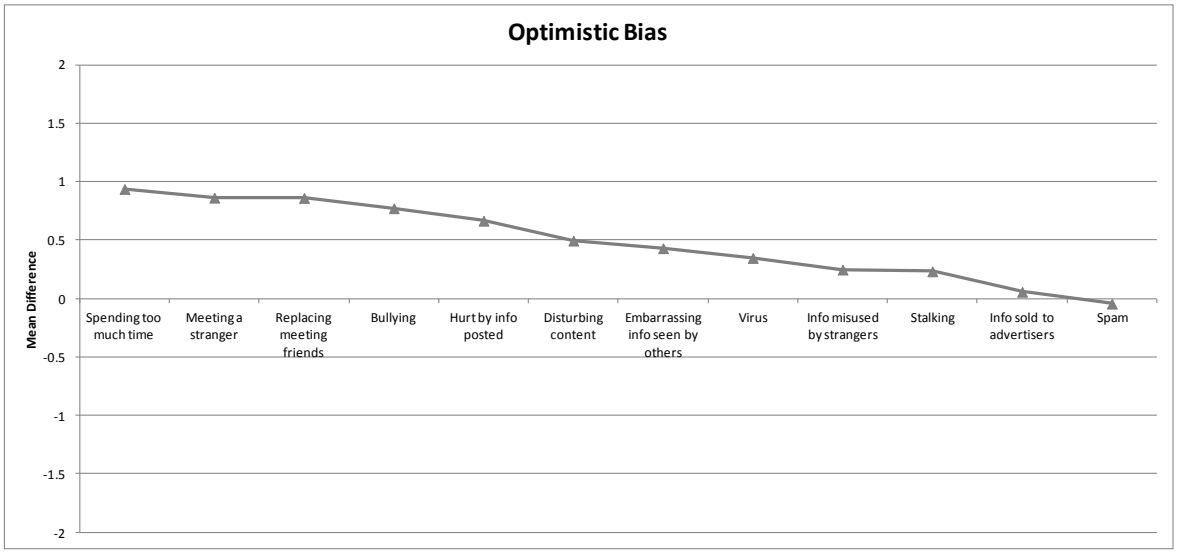


Chart 5.36 Optimistic Bias – Mean Difference Scores.

A MANOVA is used to compare the difference scores across all 12 risks. The multivariate result is significant, Pillai's Trace = .34, F = 32.4, df = (12,758), $p < 0.001$, indicating that the profile of the difference scores is significantly different from zero, i.e there is strong evidence of optimistic bias. *Post hoc* tests (using the Bonferroni correction) show there is a significant difference from zero for all risks apart from spam and information sold to advertisers.

Chart 5.37 & Chart 5.38 show optimistic bias by gender and age cohort.

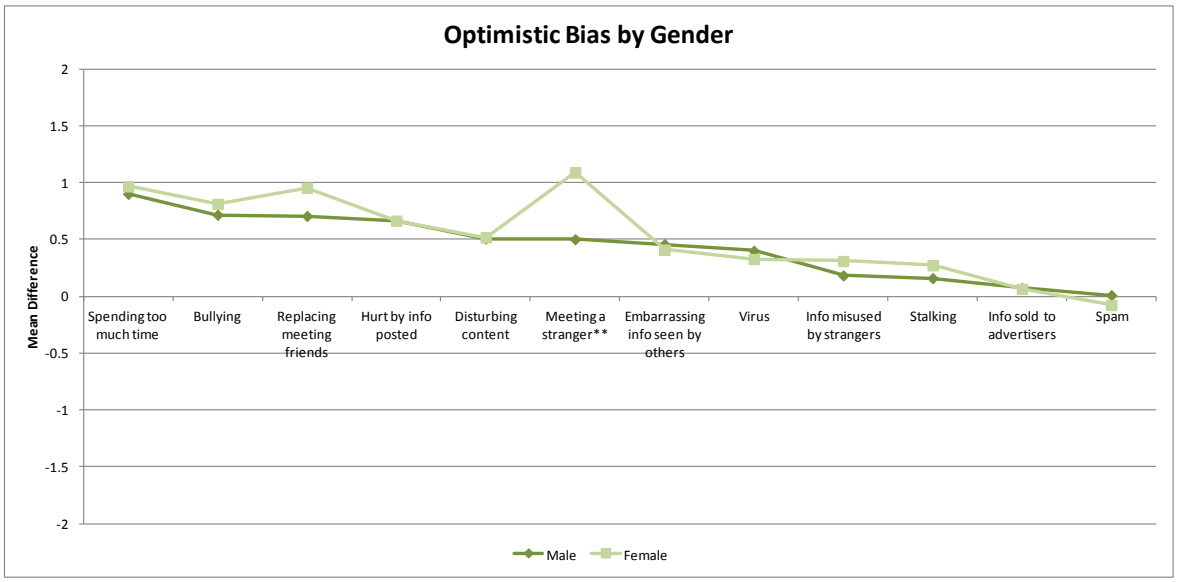


Chart 5.37 Optimistic Bias by Gender

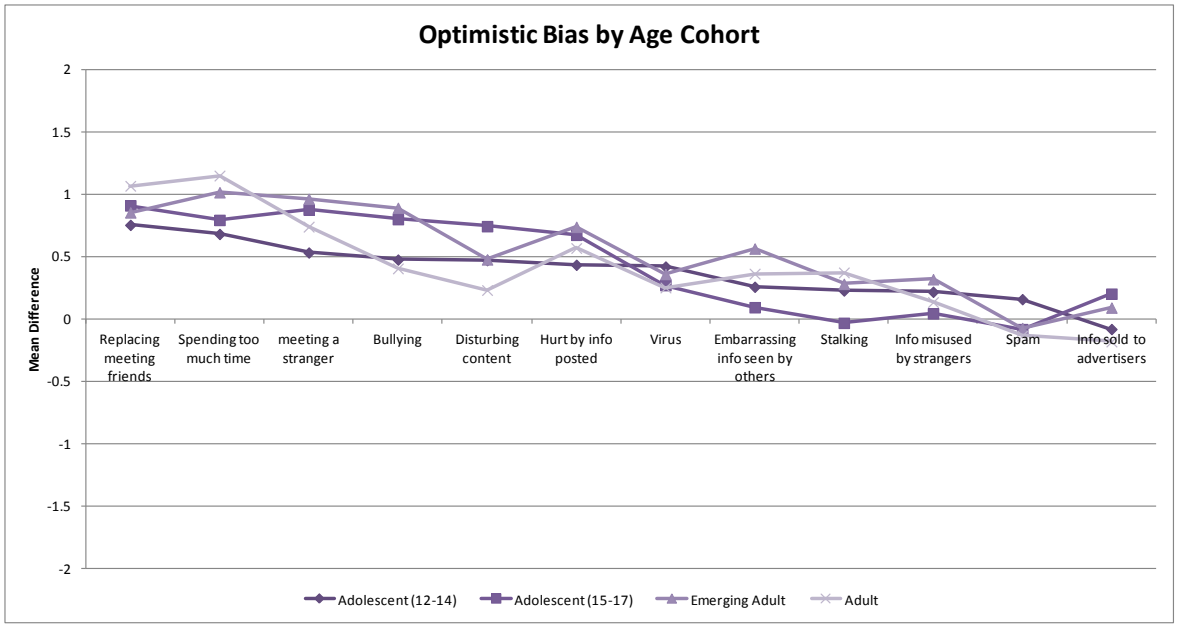


Chart 5.38 Optimistic Bias by Age Cohort

A MANOVA is used to compare optimistic bias scores across all twelve risks by age cohort and gender. The multivariate result is significant for gender, Pillai's Trace = .03, F = 1.79, df = (12,758), p = .05, indicating a difference in optimistic bias between males and females. *Post hoc* tests show there is a significant difference between males and females for only one risk, meeting a stranger, F = 15.06, df = (1,769), p < 0.001. The multivariate result is significant for age cohort, Pillai's Trace = .07, F = 1.49, df = (12,758), p = .03, indicating a difference in optimistic bias between age cohorts. None of the *post hoc* tests show a significant difference.

Unrealistic optimism is evident in the qualitative interviews with emerging adults. Most interviewees express that others in their peer group are at a greater risk, particularly for spam and phishing attacks, time wasting and having their personal information harvested. They see inexperienced computer users as being most at risk.

"I would like to think I would never fall for that. But my friends definitely do. I know one of them, it said go to this website and suddenly there is "do you wish to download this" and they said yeah! Such an idiot? If something ever pops up from a random website and asks do you wish to download this? You don't do that?" Male, Aged 22

"But you just have to be careful. You are just being stupid if you click on every single link. But obviously some people wouldn't be aware of it. I probably would be more aware then other people would be, but that is just to do with your computer knowledge too." Female, Aged 21.

5.13 Questionnaire Effect

Respondents are asked if completing the questionnaire has changed their opinions about the risks associated with SNSs, in particular has completing the questionnaire increased their awareness and concern about the risks associated with SNSs. Overall, 52% of respondents stated that completing the questionnaire has increased their awareness of the risks, and for 27% of respondents has made them more worried about the risks. Gender and age cohort differences are evident, see Chart 5.39 & Chart 5.40, with the effects being more pronounced for females and adolescents.

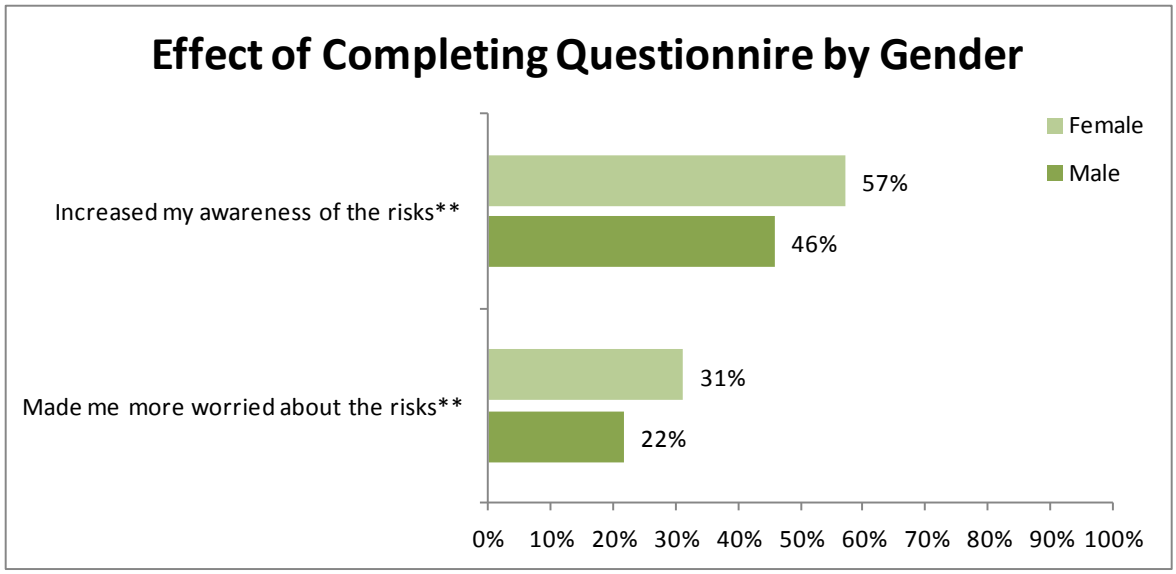


Chart 5.39 Effect of Completing Questionnaire by Gender

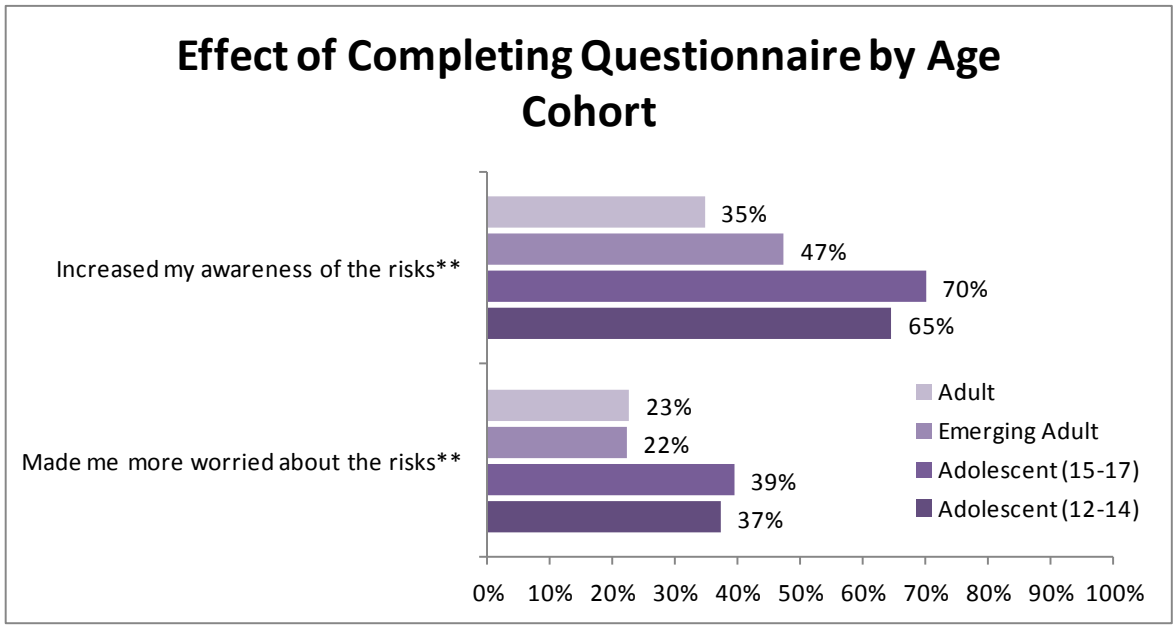


Chart 5.40 Effect of Completing Questionnaire by Age Cohort

5.14 Summary

This chapter presents the results of the survey of 551 adolescent respondents, 1,044 emerging adult respondents, 156 adult respondents and 15 complementary interviews with emerging adults and 4 focus groups with adolescents. This quantitative and qualitative analysis assesses risk perceptions associated with SNSs. This includes an investigation of the existence and importance of specific risk perceptions and other risk factors that contribute to risk perception. A logistic regression analysis is carried out to identify characteristics that are significant predictors of the likelihood of high personal risk perceptions. Respondents use and behaviour on SNSs is also examined. The mixture of both survey and interview data provide triangulation and add depth to the results.

In the following chapter the implications of these findings are discussed in terms of the research questions. In a broader sense, the discussion also provides an increased understanding of risk perception on SNSs and the crucial factors that can predict high risk perception on SNSs.

6. Discussion

6.1 Introduction

The primary focus of this research is to assess an individual's perception of risk associated with the use of social network sites, an understanding of risk perception is important as it provides explanations for people's actions. As far as it is known, this study is the first time that an extensive single study of age related risk perception on SNSs has been undertaken. The findings from this research have in some cases confirmed those found in other studies and in a number of instances contradict those of previous work. This study has also revealed a number of new findings about risk perception. This chapter discusses these findings. The theoretical and practical contribution of the thesis is examined.

6.2 Discussion of Findings

This section discusses the main findings of the research and compares and contrasts the findings to both the SNS and risk perception research literatures. The section starts by providing background information on respondents' use of SNSs, followed by a discussion of the findings related to risk perception. The SNS behaviours that make users more vulnerable to risk are examined. The section concludes by comparing the risk experiences of respondents with the findings of other studies that have been carried out in the area.

6.2.1 Use of SNSs

A high proportion of respondents (84.6%) are current users of SNSs. The highest proportion of SNSs users are in the older adolescent age cohort (91%), closely followed by the emerging adult cohort (86%) with the lowest proportion of current SNS users in the adult cohort (71%). Only 7% of respondents have never used SNSs. Similar to other studies (Livingstone *et al.*, 2010b, O'Neill *et al.*, 2011) this study found that adolescent's use of SNSs increases with age. Table 6.1 compares the findings of the Irish EU Kids Online study (O'Neill *et al.*, 2011) with the current study, both studies show similar proportions of SNS users in each age group.

Adolescent Age Group	EU Kids Online Study	Current Study
11-12 years	52%	56%
13-14 years	75%	83%
15-16 years	88%	90%

Table 6.1 Comparison of Proportions of SNS Users in Current Study to Irish EU Kids Online Study (O'Neill *et al.*, 2011).

Facebook is the predominant SNS used by respondents, although Bebo is also popular with the younger adolescent cohort. At the time of writing, Facebook membership is increasing and the age profile is widening (Socialbakers, 2011), it could be assumed that usage levels have further increased particularly in the adult cohort.

Like other studies (EUROBAROMETER, 2007a, Lenhart and Madden, 2007, WEBWISE, 2009, O'Neill *et al.*, 2011) this study found that more females (87%) than males (80%) are current users of SNSs.

Consistent with previous findings (boyd, 2007, Ellison *et al.*, 2007, Lenhart and Madden, 2007, OFCOM, 2008, Subrahmanyam *et al.*, 2008), respondents primarily use SNSs to keep in contact with existing friends, but some age cohort and gender differences are evident. Compared to emerging adults, older adolescents are 8.6 times more likely to have used SNSs to meet new friends, these results reflect the findings of other studies that suggest that younger SNS users collect friends and having the highest number of online friends is seen as highly desirable (OFCOM, 2008). Males are more likely than females to use SNSs to meet and find new friends and to help increase their popularity. Other studies have found similar gender differences in how SNSs are used, for example Lenhart and Madden (2007) found that boys were twice as likely as girls to use SNSs to flirt, whereas older girls tended to use SNSs to communicate with existing friends.

6.2.2 Discussion of Risk Perceptions

Risk perception is a multidimensional concept. The research literature has identified a number of different risk characteristics that contribute to risk perceptions. Many of the risk characteristics identified in the research literature are not of direct relevance to the type of risks that can be encountered on SNSs. For example the degree to which a risk invokes a feeling of dread is not relevant for IS/ICT risks, but the degree to which a risk is understood or known would be relevant for IS/ICT risks. A review of previous studies of risk perception (with an emphasis on ICT studies and adolescent studies) identified over 45

different risk characteristics. As described in Section 3.7, the risk characteristics examined in this study have been chosen based on their relevance to SNS risks and include personal risk (likelihood), concern about risk, awareness/knowledge of risk, severity/harm of risk and controllability of the risk.

Overall respondents' perceive themselves to be most likely to encounter spam and have embarrassing information seen by others on SNSs. This finding is not surprising as these risks are among the top three most commonly experienced risks on SNS and are experienced by over 40% of respondents in this study. However when the consequences of these risks are taken into account as shown in Chart 6.1, it can be seen that spam is not considered a serious threat and risk perceptions for spam are low. Risk perceptions are highest for having embarrassing information seen by others. Although respondents recognise the severity of the more serious threatening risks on SNSs, such as bullying, stalking, meeting a stranger and being hurt by information posted, they do not perceive that these negative events are likely to happen to them. It is surprising that risk perceptions are not higher for these more serious threatening risks. Optimistic bias provides a possible explanation. Optimistic bias is particularly high for the threatening risks of meeting a stranger, being cyberbullied and being hurt by information posted indicating that users perceive that these risks are significantly more likely to happen to others and not to them. A more detailed discussion of optimistic bias is provided in Section 6.2.4.

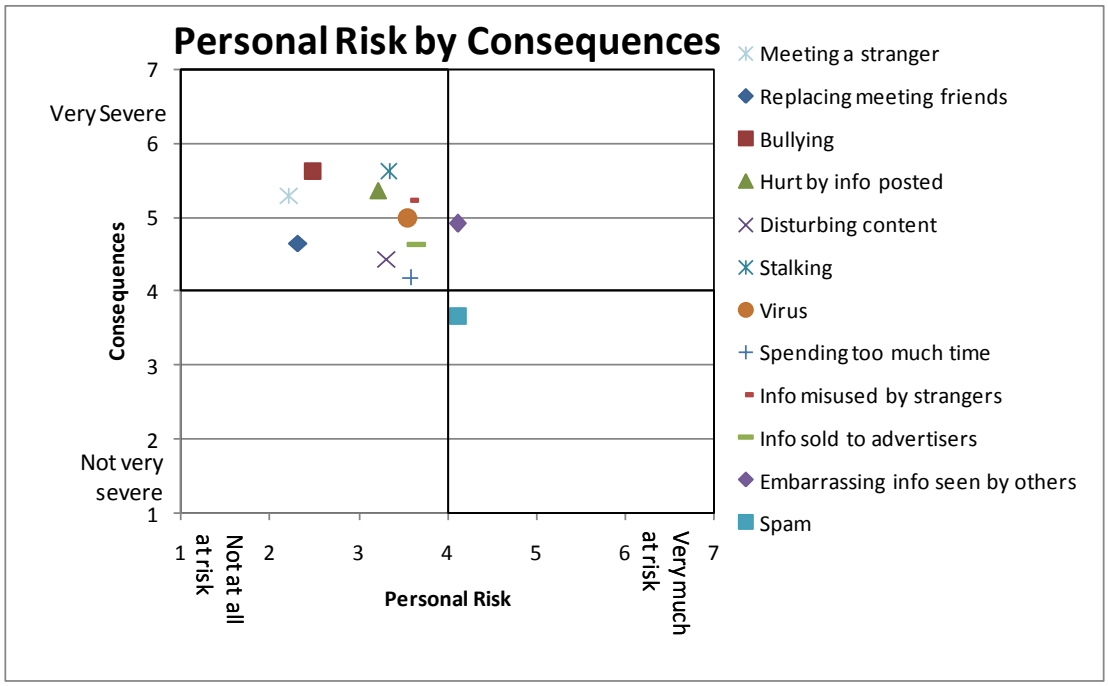


Chart 6.1 Perceived Personal Risk (Likelihood) by Perceived Consequences

The fact that risk perceptions are higher for embarrassing information being seen by others on SNSs is not surprising. 42% of respondents have experienced this problem; it is the type of negative event that users can relate to; users can see the direct personal effect, thus it is salient and emotive for users.

Chart 6.2, shows that respondents are most concerned about the reputational risks followed by the more serious threatening risks. Respondents are least concerned about the excessive use risks: displacing FtF time with existing friends and spending too much time on SNSs.

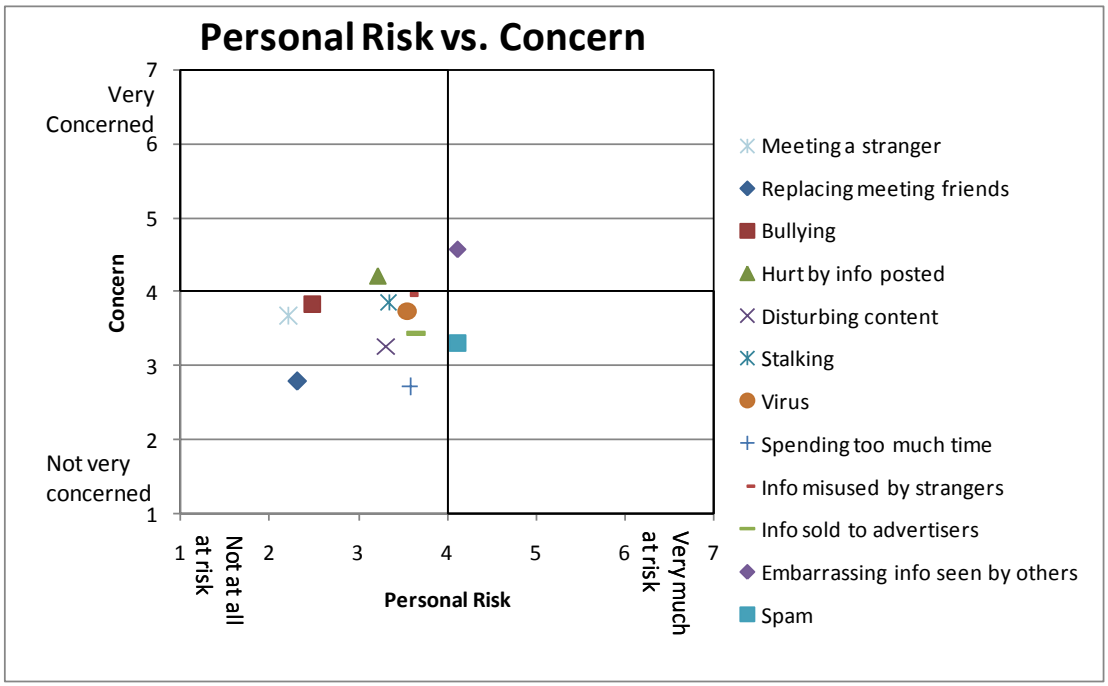


Chart 6.2 Perceived Personal Risk (Likelihood) by Perceived Concern

The fact that users are most concerned about the reputational risks, indicates users may be adopting an instinctive intuitive reaction to risk rather than making a deliberate and reasoned analysis of the risks, following the affect heuristic or a "*risk as feelings*" approach. Previous studies have examined reputational risks (in particular being hurt by information posted by others) as they relate to cyberbullying (O'Moore and Minton, 2010, Livingstone *et al.*, 2011a) and not as separate negative events. These reputational risks are not necessarily due to cyberbullying but can simply be due to others not being aware of the implications of what they post or even from postings being misinterpreted. Many users have rated these risks as having serious effects. Further studies are needed to assess the implications of these risks.

Respondents were asked to indicate whether they thought people their age know about the risks. The reputational risks are the most well known followed by the serious threatening risks of meeting a stranger and bullying. The least well known risks are information being sold to advertisers and viruses. Measuring knowledge in this way does give some indication of users' awareness of the risks, but it does not show whether users are fully aware of the consequences of the risks and if they know how to protect themselves from the risks. The qualitative interviews provide some further insights. Confirming the findings of the survey, many interviewees are not aware that viruses can be spread on SNSs and although interviewees are aware of advertising, they do not realise that others could be harvesting their personal information and building up profiles about them. Interviewees show little awareness that their personal information can be aggregated over time and combined with other online and offline sources to allow detailed profiles of them to be built. As has been found in previous research (Lampe *et al.*, 2006, Livingstone, 2008, Phippen *et al.*, 2009, Pike *et al.*, 2009, West *et al.*, 2009), interviewees do not fully appreciate the potential audience on SNSs and assume the audience is just their restricted friends group. Interviewees are not aware of how easily their data can be accessed and most are trusting of the SNSs. Many have not considered the business model behind SNSs. This lack of awareness is reflected in user's behaviour on SNSs and the measures they adopt to protect themselves on SNSs. Although most users restrict who can see their profile, they do not always fully utilise the privacy settings available to them on SNSs. The lack of knowledge about potential audiences may also explain why users continue to reveal substantial amounts of personal information on their SNS profile. These behaviours are discussed in further detail in Section 6.2.5.

Respondents were asked to indicate whether they thought people their age could control or stop the risks associated with SNSs, see Chart 6.3. As would be expected respondents feel they have most control over meeting a stranger, SNS use displacing FtF meetings with friends and spending too much time on SNSs. For the remaining risks, they feel less in control with between 27% – 40% of respondents feeling they had little control over these risks.

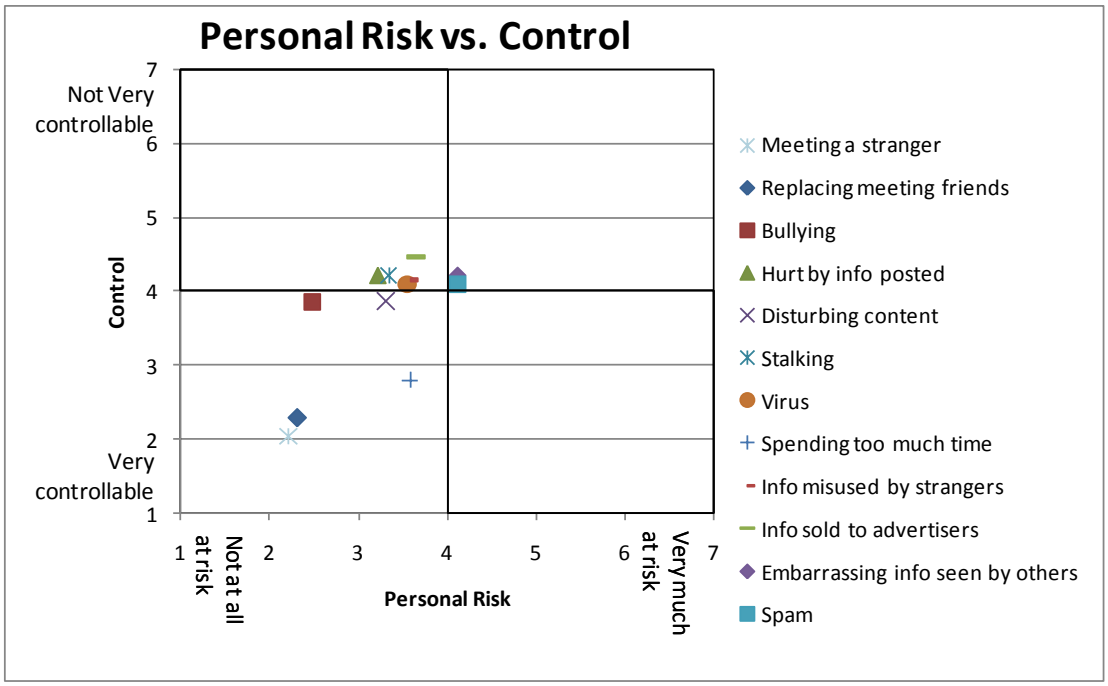


Chart 6.3 Perceived Personal Risk (Likelihood) by Perceived Control

Previous studies have shown that risk perception has an inverse relationship to age, where younger adolescents perceive greater risk than older adolescents and older adolescents perceive greater risk than young adults (Gullone and Moore, 2000, Gullone *et al.*, 2000, Millstein and Halpern-Felsher, 2002a). Confirming this finding, results of this study show that for most of the risks on SNSs, adolescents compared to the other age cohorts perceive themselves to be at a higher likelihood of experiencing the risk, express higher levels of concern, are more knowledgeable about the risks and perceive the consequences of the risks to be more severe. Adolescents showed significantly higher levels of awareness and concern for the serious threatening risks. This would be expected as the consequences of these risks are more serious for adolescents and safety awareness campaigns tend to be targeted at these risks. It is also possible that adolescents engage with new technologies more readily and tend to be early adopters and thus they often know more about these technologies (including the risks) than older age cohorts. Chart 6.4 compares the risk perceptions of adolescents and emerging adults and shows how the risk perception for the serious threatening risks of bullying and meeting a stranger differs between the two age cohorts.

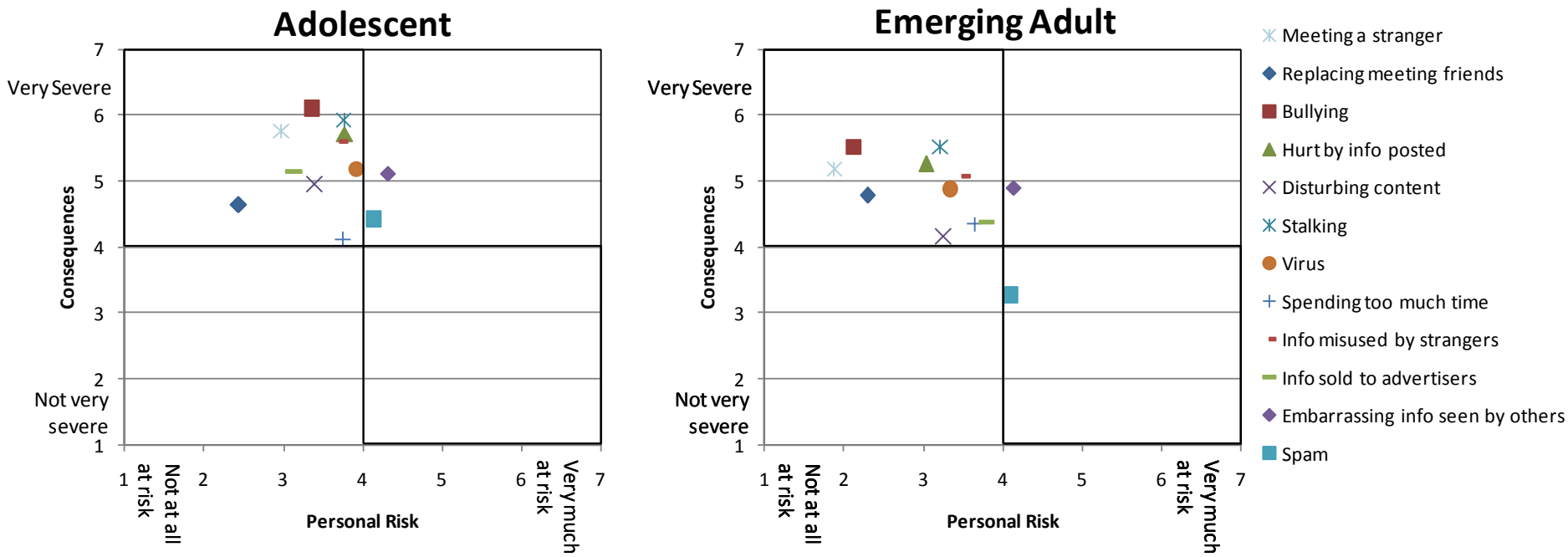


Chart 6.4 **Perceived Personal Risk (Likelihood) by Perceived Consequences for Adolescents and Emerging Adult Age Cohorts.**

Some other age cohort differences are evident. Emerging adults perceive they have significantly less control compared to the other age cohorts over embarrassing information being seen by others and being hurt by information that others post. Apart from the reputational risks, emerging adults show the lowest levels of concern about all other risks. Adults feel that they can better control the amount of time they spend online compared to the other age cohorts.

Risk perception research suggests that females tend to perceive themselves at greater risk than males (Flynn *et al.*, 1994, Parsons *et al.*, 1997, Byrnes *et al.*, 1999, Finucane *et al.*, 2000). In contrast, this study has found that although females perceive all of the risks as more serious than males there is no evidence to suggest that risk perceptions (personal likelihood of risk x consequences of risk) are higher for females. As stated by Byrnes (2003), this gender effect can depend on the hazard being examined, so it would appear that for this risk domain gender differences in risk perceptions are not apparent. However, some gender differences are evident for the perceived personal likelihood of risk. Males perceived themselves to be at a higher likelihood than females for meeting a stranger and having personal information sold to advertisers. Females perceived themselves to be at a higher likelihood of spending too much time on SNSs, having embarrassing information seen by others and getting a virus. It is possible that these differences in personal risk perceptions are related to prior experience of the risk and not to a gender effect, as more males than females have experienced meeting a stranger and having personal information sold to advertisers and more females than males have experienced spending too much time on SNSs and having embarrassing information seen by others.

As half of the respondents to the survey have experienced spending too much time on SNSs, it is surprising that respondents do not express higher levels of concern about this risk. This may be because user's perceived benefits of using SNSs outweigh the risk of spending too much time on SNSs, a common finding in risk perception research (Furby and Beyth-Marom, 1992, Benthin *et al.*, 1993, Lavery *et al.*, 1993, Siegel and Cousins, 1994, Benthin *et al.*, 1995, Gerrard *et al.*, 1996a, Moore and Gullone, 1996, Frewer *et al.*, 1998, Parsons *et al.*, 2000). However, the qualitative research suggests that spending too much time on SNSs is seen as a serious concern. Many of those interviewed suggest that spending too much time on SNSs is a serious problem for their peer group even going so far as to suggest, for some, it is close to an addiction. Further research is needed to examine if excessive use of SNSs is displacing time spent on other activities and to fully

assess if the benefits of SNSs outweigh the amount of time users spend on SNSs. This study also found that users are underestimating the amount of time they are spending on SNSs (see Section 6.2.5) and this too could be contributing to their lack of concern in this regard.

Summary

In summary although users show an awareness and a recognition of the risks on SNSs, most users show a lack of concern about the risks on SNSs and do not think that these negative events are likely to happen to them. It would be expected that users would be most concerned and have highest risk perceptions for the serious threatening risks such as cyberbullying and meeting a stranger, this is not the case and users express higher levels of concern and perceive greater risk for risks to their reputation. For most of the negative events on SNSs, adolescents compared to the other age groups perceive themselves to be at a higher risk, show higher levels of awareness, are more concerned and perceive the consequences of the risk to be higher. No gender effects are evident with regard to risk perceptions. The qualitative interviews and focus group discussions highlight some misconceptions with regard to these risks and in particular users lack of awareness of the audience on SNSs and how easily their personal information can be accessed.

6.2.3 Predicting High Personal Risk

It is useful to have an understanding of why some users see themselves as more likely to be at risk on SNSs. As discussed in Section 3.7, a number of factors have been highlighted that can influence perceived risk. The factors include the risk characteristics discussed above but also personal beliefs (such as an individual's disposition to trust and their level of privacy concern), contextual variables (such as intensity of SNS usage and the amount of personal information revealed on SNSs) and other variables including age cohort, gender, level of Internet experience, and prior experience of the event.

An analysis was carried out using binary logistic regression to identify which of these factors are significant predictors of the likelihood of high personal (i.e. likelihood) risk perception. Five risks are examined:

1. Excessive use risk: spending too much time on SNSs;
2. Threatening risk: being bullied or harassed;

3. Reputational risk: embarrassing information or photos being seen by people who you would prefer didn't see it;
4. Personal information risk: personal information being sold to advertisers;
5. Technical risk: receiving spam

Three factors are significant predictors of the likelihood of high personal (i.e. likelihood) risk perception for all of the five risks examined. The strongest predictor is prior experience. Although not displaying as strong an effect as prior experience, concern about risk and age are significant predictors for all five negative events.

Controlling for all other variables in the model, for all five risks, prior experience of risk is the most significant predictor of a respondent perceiving themselves to be at high risk. Depending on the risk, individuals that have personal experience of the risk are between 3 and 4.5 times as likely to perceive themselves at high personal risk compared to those that have not experienced the risk. For the excessive use risk of spending too much time on SNSs, there is an interaction between personal experience of the risks and age cohort. Emerging adults that have experienced spending too much time on SNSs are 3 times as likely to perceive themselves at high risk, adolescents that have experienced the risk are over 2 and half times as likely to perceive themselves at high risk and adults that have experienced the risk are over twice as likely to perceive themselves at high risk compared to those that have not experienced the risk. It is not surprising that prior experience is a strong predictor of personal risk perception and this finding lends support for the availability and representation heuristics (Tversky and Kahneman, 1974), see section 2.3.2, in that events that are more easily brought to mind are judged to be more likely and individual events or experiences can have a greater impact on an individual's perception of the risk.

Although it is recognised that prior experience is an important determinant of risk perception (Eiser, 2004, Breakwell, 2007), prior experience is not a factor that has been empirically tested in many studies and the few studies that have examined prior experience have not reached many coherent conclusions. Prior experience is not relevant or even measurable for studies that examine extreme hazards such as a fatal airplane crash etc., but for those studies that have examined ICT/IS risks, it is possible to and important to examine the impact of prior experience. In their study of information technology risks as seen by the public, Sjöberg and Fromm (2001) did examine prior experience of risks.

However, they combined their measure for prior experience with overall Internet experience to create a composite score for experience. It is therefore not possible to isolate what effects prior experience of negative IT events had on risk perception. Compared to the current study the prevalence of risks was much lower for example, only 3.5% of respondents had experienced getting a virus via the Internet and this could be a possible reason why the authors combined the measures. Campbell *et al.* (2007) found that negative personal experiences with Internet events were significantly correlated with optimistic bias, but they did not explicitly examine the correlation with risk perception. Other studies examining ICT/IS risk perceptions (Coles and Hodgkinson, 2008, Gabriel and Nyshadham, 2008) did not measure prior experience. This highlights a serious gap in previous studies of ICT/IS risks.

Previous studies have shown that risk perception has an inverse relationship to age, where younger adolescents perceive greater risk than older adolescents and older adolescents perceive greater risk than young adults (Gullone and Moore, 2000, Gullone *et al.*, 2000, Millstein and Halpern-Felsher, 2002a). This study compares adolescent, emerging adult and adult age cohorts. For all risks except the excessive use risk and controlling for all other variables in the model, adolescents are more likely than the emerging adult age cohort to perceive themselves at high personal risk, but there is no evidence to suggest that emerging adults are more likely than the adult cohort to perceive themselves at high risk. So this inverse relationship is evident between adolescents and emerging adults but not between emerging adults and adults. Further research is needed to confirm these findings, the lack of evidence of an inverse relationship between emerging adults and adults may be due to the small sample size and the representativeness of the adult cohort sample used in this study. As already stated, for the excessive use risk, there is an interaction between personal experience and age cohort. This makes it difficult to separate out the age effect.

According to the "*risk as feelings*" or affect hypothesis, feelings such as worry and concern about a risk can lead to increased risk perceptions (Zajonc, 1980, Rundmo, 2002, Tennfjord and Rundmo, 2007). Confirming these findings, concern or worry about risk is a significant predictor for the likelihood of high personal risk perception for all types of risk. As would be expected, the effect of concern/worry is highest for the threatening risk of being bullied or harassed.

Two other risk characteristics, knowledge and control, that have been suggested by the psychometric paradigm, show small effects on the likelihood of high personal risk perception and are only significant for some of the risks examined. The findings of this analysis suggest that users with high personal risk perception perceive the excessive use risk, the reputational risk and the technical risks to be less controllable. Although these findings are understandable for the reputational risk and technical risk, this appears counterintuitive for the excessive use risk of spending too much time on SNSs and it is surprising that this effect is not significant for the personal information risk. This suggests that this measure of control may not be adequately measuring user's perception of control. For example, it is possible that a user's locus of control is playing a part here. As suggested by Rotter (1966, 1990) individuals with an internal locus of control believe that they are in control of their environment and those with an external locus of control believe that events in their environment are outside their control. It is possible that those that perceive themselves at high personal risk tend to display an external locus of control and thus feel less able to control negative events on SNSs. This is an area that warrants further investigation.

The findings of this analysis show that an increased knowledge of risk is only a significant predictor for the excessive use risk of spending too much time on SNSs. Individuals that perceive themselves to be at a high risk of spending too much time on SNSs have an increased knowledge/awareness of this risk. It is surprising that knowledge of risk is not a significant predictor for the remaining risk categories and this has implications for the effectiveness of Internet safety awareness campaigns.

As would be expected individuals with higher levels of expressed online privacy concerns perceive themselves to be at high personal risk for personal information risks. Explaining why disposition to trust is a significant predictor for some variables and not for others is difficult. This is made more challenging as there is no evidence of significant relationships between high personal risk perception and disposition to trust in the univariate analysis. However, the analysis suggests that individuals with high personal risk perceptions express lower levels of trust for certain negative events on SNSs. The relationship between disposition to trust and risk perception is clear in the online shopping domain and this analysis suggests that disposition to trust may also be important for SNSs. Further research should be conducted to examine the relationship in more detail.

Gender is not a significant predictor for any of the risk categories. As stated in the previous section, this contradicts the findings of risk perception research that suggests females tend to perceive themselves at greater risk than males (Flynn *et al.*, 1994, Parsons *et al.*, 1997, Byrnes *et al.*, 1999, Finucane *et al.*, 2000). The univariate analysis shows there is a significant relationship between intensity of SNS use and the excessive use risk, with high personal risk perceptions increasing with usage level. This relationship is not evident in the logistic regression and further analysis suggests that this is because intensity of SNS use is highly correlated with prior experience and thus prior experience is explaining this effect in the multivariate analysis. The level of Internet experience is not a significant predictor of the likelihood that an individual would perceive themselves to be at high risk for any of the 5 risk categories. This suggests that those users with higher levels of computer experience do not necessarily see themselves to be at a higher risk. This finding is discussed in further detail in Section 6.2.5.

Summary

This logistic regression analysis shows that, depending on the negative event, different factors are significant predictors of a user perceiving themselves to be at high risk on SNSs. However, prior experience, concern about risk and age are relevant for all risk types. It is important to note that an analysis of this nature does not allow conclusions to be drawn with regard to which variable is causing changes to the other. For example, it is unclear whether having an increased concern about a risk is a cause or a consequence of a high risk perception.

6.2.4 Optimistic Bias

As discussed in section 2.4.4, optimistic bias is the tendency for individuals to report that they are less likely than others to experience negative events and are more likely than others to experience positive events. This study has focussed on optimistic bias with regard to negative rather than positive events on SNSs, as an optimistic bias for negative events has implications for risk perception and risky behaviour.

Apart from spam and information being sold to advertisers, respondents perceive that they are less likely than others in their peer group to experience negative events on SNSs. This optimistic bias is most pronounced for the excessive use risks of spending too much time on SNSs and SNSs replacing FtF meetings with friends, followed by the threatening risks

of meeting a stranger, being bullied and being hurt by information posted. These results generally support the findings of optimistic bias research (Weinstein, 1980, 1984, 1987) and suggest that comparative risk judgments (self versus others) are also evident in SNS environments. The implications of these high levels of optimistic bias with regard to risk perception have been discussed in Section 6.2.2.

Previous research has found that heavy Internet users demonstrate significantly more optimistic bias than light users of the Internet (Campbell *et al.*, 2007). To ascertain if a similar trend is evident on SNSs, a MANOVA is used to compare optimistic bias scores across all twelve risks by the SNS intensity score. The multivariate result is not significant for SNS intensity, indicating no difference in optimistic bias between high and low intensity users of SNSs. This discrepancy may be attributable to a difference in the measures used to assess heavy and light Internet users, Campbell *et al.* (2007) used a crude measure where heavy users were defined as users that use the Internet for more than an hour a day and light users used the Internet for less than 1 hour a day. A more detailed measure is used in this study.

6.2.5 Behaviour on SNSs

Although this study is primarily concerned with risk perception on SNSs, the study has highlighted a number of behaviours on SNSs that could make users more vulnerable to adverse events. Again some of these findings are consistent with previous research, but some of these findings are new. The problem behaviours highlighted include: users underestimate how long they spend on SNSs, users reveal substantial amounts of personal information, users are not fully aware how to protect themselves on SNSs and users depend on informal sources to gain awareness of risks. Each of these behaviours is discussed in this section.

A comparison of the findings from the quantitative and qualitative elements of the study show that users underestimate the amount of time they spend on SNSs. Results from the survey show that both the adolescent and the emerging adult cohorts access a SNS about once a day on average, the adult cohort, on average, access SNSs less often at a couple of times a week. The qualitative findings indicate that users underestimate the amount of time they spend on SNSs. The majority of those interviewed keep Facebook open in the background all the time they are on a computer, similar to an email application. In

addition, interviewees are increasingly accessing SNSs via their smart phones and smart devices. They also keep Facebook open when they are watching television. This makes it difficult for users to estimate accurately the amount of time they spend on SNSs as they constantly flick in and out of SNS. Recent research by Brasel and Gips (2011), which used eye-tracking cameras, shows that this "*media multitasking*" is distracting. They found that individuals switch their attention between the computer and the TV at a high rate, nearly once every 14 seconds, but most attention was concentrated on the computer. They found that users drastically underestimate how often they switch behaviour. The researchers suggest that individuals lack the ability to recall much of their media multitasking behaviour. This means that asking survey respondents to estimate the frequency and duration of time they spend on SNSs, a technique used in many studies (Acquisti and Gross, 2006, EUROBAROMETER, 2007a, Lenhart and Madden, 2007, Anchor, 2008b, OFCOM, 2008, Fogel and Nehmad, 2009, Young and Quan-Haase, 2009, Livingstone *et al.*, 2010b), is no longer an adequate measure of the amount of time users spend on SNSs. Alternative measurement options are discussed in Section 7.3. By using two methods, such as implemented in this study, it is possible to get a better understanding of the phenomena being examined. In the qualitative interviews it is possible to probe and attain a deeper understanding of the amount of time respondents spend and their behavioural patterns on SNSs. The measurements from the quantitative study are not without merit. The SNS intensity scale measurement although not ideal (as it is based on user estimates of time online) does allow comparisons of intensity of SNS use between groups. For example, this scale shows that females are more likely than males to be high intensity users of SNSs.

This study has found that SNS users are revealing substantial amounts of personal information, a consistent finding in previous studies (Gross and Acquisti, 2005, Acquisti and Gross, 2006, Anchor, 2008b, Hinduja and Patchin, 2008b, Tufekci, 2008, Christofides *et al.*, 2009, Fogel and Nehmad, 2009, WEBWISE, 2009, Young and Quan-Haase, 2009). However, compared to previous studies, this study shows that while respondents are exercising caution in revealing personal contact information (address and phone numbers) they still continue to reveal substantial amounts of other personal information. For example, 93% of respondents have a picture of themselves on their profile, 85% have revealed their full name, 71% display their age, 68% show their school/college or workplace and 62% their email address. Perhaps indicating the success of safety awareness campaigns targeted to children, adolescents are less likely than the other age

cohorts to place direct contact information on SNSs, but overall the adult age cohort is the most cautious in the amount of information they reveal. To further investigate the extent to which respondents reveal information on SNSs, an information revealed score adapted from Livingstone *et al.* (2011a) was created and applied to the data in this study. This shows that the older adolescent and emerging adult age cohorts reveal significantly more information than the younger adolescent and adult age cohorts. This score is measured against the intensity of SNS use scale and as would be expected shows that the amount of information revealed increases with intensity of use. Findings indicate that individuals that display higher levels of peer influence are more likely to reveal more information on SNSs and are more likely to use SNSs more intensively.

Some gender differences are evident in the information revealed. Females are more likely than males to place pictures online, but males are more likely to reveal contact information as has been found in previous studies (Gross and Acquisti, 2005, Tufekci, 2008, Fogel and Nehmad, 2009). Gross and Acquisti (2005) suggested that this was single males that were "*signalling*" their interest in making the maximum amount of contact information easily available. As details of relationship status are not collected in this study, it is not possible to verify if signalling is an explanation for males providing more personal contact details. As discussed in Section 3.4.2, a number of reasons have been suggested in the literature as to why users reveal considerable amounts of personal information about themselves, including signalling, peer pressure, lack of awareness of the risks, difficulties with privacy settings on SNSs, accepting the default settings etc. Although not investigated in depth in this study, the qualitative findings and open ended questions suggest that users are guided by the default settings and design of the SNS. Users when they first join SNSs accept the default privacy settings and fill in all the information categories provided on the SNS, in time they learn to restrict their settings and remove direct contact information.

A number of studies have investigated the relationship between a respondent's online privacy concerns, their privacy settings and information disclosure. Like previous studies (Acquisti and Gross, 2006, De Souza and Dick, 2009), this study found that users who express higher levels of privacy concern are more likely to restrict their privacy settings. This finding in itself is not surprising; however these privacy concerns do not extend to information disclosure. As with previous research (Acquisti and Gross, 2006, Tufekci, 2008, De Souza and Dick, 2009), this study found no relationship between a user's

expressed online privacy concern, their privacy settings and the quantity of personal information they disclose.

Clearly respondents to this study, at all age cohorts, are revealing substantial amounts of personal information. Even without direct contact information it is still possible to identify and locate users using the information they do provide, as many users provide images and give their place of work/college and school attended. Although many respondents do not currently display direct contact information, many respondents did display this information in the past. Archived and cached copies of these pages are often made and stored online. Users are often unaware that they can be identified through this aggregated data and that although they have removed data that copies of the data may reside elsewhere. As discussed in Section 6.2.2 users show a lack of awareness of how their personal information can be harvested.

An examination of the measures users adopt to protect themselves on SNSs highlights some areas of concern. In contrast to the findings of previous studies (Gross and Acquisti, 2005, Anchor, 2007, Dwyer, 2007, Hinduja and Patchin, 2008b, OFCOM, 2008), this study found an increase in the proportion of users (65%) that have restricted their SNS profile. This could indicate that recent awareness campaigns and press coverage about the privacy concerns with SNSs may be having an effect. However, it is a concern that compared to other age cohorts, a higher proportion of adolescents do not know if they have changed their privacy settings and a higher proportion of older adolescents have not changed their settings. From the interviews, it is evident that some adolescents find it hard to understand the privacy settings. The interviews show that many users (both adolescents and emerging adults) initially accept the default privacy settings set by the SNS. The default privacy settings on SNSs are not restrictive. On Facebook for example, for minors, the visibility of their information is limited to friends of friends and networks, for an adult the default privacy setting for certain types of information is set to "*everyone*". The interviews show that users tend to restrict their settings in reaction to a negative incident on their or a friends profile. As with previous studies (Lewis *et al.*, 2008, O'Neill *et al.*, 2011), this study found that females (72%) are more likely than males (55%) to have restricted their privacy settings.

Similar to the findings of previous studies that have examined IS/ICT risks (Furnell *et al.*, 2007), interviewees indicate that they gain their awareness of the risks from informal

sources such as their peer group, siblings and other family members or from personal experience rather than formal sources such as the media, awareness campaigns etc. Further analysis suggests that these informal sources may not be entirely reliable. Interviewees think that users with higher levels of computer experience (often themselves) are more knowledgeable about the risks. This study found, however, that there is no statistically significant relationship between knowledge of risk and Internet experience, indicating that those with a higher level of Internet experience do not necessarily display an increased knowledge of the risks. This would lend support to the argument proposed by Jackson *et al*. (2004a) and Collins and Mansell (2004) who contend that that more experienced users of the Internet tend to be overconfident and can become desensitised to Internet risks.

Summary

This study has highlighted a number of behaviours on SNSs that could make users more vulnerable to risk. Users are underestimating the amount of time they spend on SNSs and may be unaware of the distracting aspects of SNSs. Respondents continue to reveal substantial amounts of personal information, adolescents are less likely than the other age cohorts to reveal personal contact information, but overall older adolescents and emerging adults reveal significantly more information than the other age cohorts. More intensive users of SNSs reveal more information.

In contrast to some previous studies, this study has found that over 65% of respondents have restricted their privacy settings, indicating that SNS users may be becoming more aware and concerned about the privacy risks on SNSs. However, similar to the findings of other studies, this concern does not extend to restricting the amount of information respondents disclose. The qualitative interviews indicate that SNS users tend to be guided by the SNS company by initially accepting the default setting and by filling in the information categories provided on the SNS.

Users tend to learn about the risks on SNSs from informal rather than formal sources. These sources may not be reliable, especially if the informal sources used are experienced Internet users, as these users can be overconfident and desensitised to the risks on SNSs.

6.2.6 Respondents' Prior Experience of Negative Events on SNSs

The section compares the risk experiences of respondents to this study with other comparable studies that have been carried out in the area. Each of the twelve risks examined in the study are discussed below. The negative events are discussed under the headings of threatening risks, risks to personal information, reputational risks, technology risks and risks associated with excessive use of SNSs. There is a considerable amount of detail in this section, to aid interpretation a summary is provided at the end of this section, see Table 6.2.

Threatening Risks:

Bullying and Harassment

Two recent nationally representative studies of children and adolescents in Ireland have found divergent estimates of the incidents of online cyberbullying. O'Moore and Minton (2010) (n= 2,794, 12-16 year olds) found that around one in seven (14.2%, female=18.1%, male=12.3%) respondents reported having being cyberbullied over the previous few months. The Irish EU Kids Online study (O'Neill *et al.*, 2011) (n= 994, 9-16 year olds) found that only 4% of respondents experienced online cyberbullying. Both studies examined the incidence of cyberbullying on SNSs, with O'Moore and Minton (2010) reporting a rate of 12.3% and O'Neill *et al.* (2011) reporting a rate of only 3%. The findings of this study, lies between theses two rates with 8.5% of 12-16 year olds experiencing cyberbullying on SNSs. O'Moore and Minton (2010) provided a broad definition of cyberbullying on SNSs by asking respondents whether they had "nasty, aggressive, threatening or embarrassing things about you posted on SNSs". As they included embarrassing comments it is not surprising that their findings would be higher than the findings of the current study, which examined "cyberbullying and harassment". It is not clear why the Irish EU Kids Online study found lower proportions of bullying online, especially as a similar study carried out in the UK found online bullying rates of 8% (Livingstone *et al.*, 2010a).

The research literature has not reached a consensus on whether there is a gender effect in the victims of cyberbullying and this study did not find evidence of a gender effect. As the majority of studies to date have examined cyberbullying from an adolescent viewpoint, it is difficult to find comparable rates for emerging adults and adolescents, however this study

does highlight that cyberbullying and harassment is not a problem that is confined to adolescents and is experienced by emerging adults (6%) and to a lesser extent adults (3%).

Stalking

It is difficult to find comparable figures for the prevalence of cyberstalking, as previous studies have used differing definitions and sampling methods. Studies have reported cyberstalking rates between 3.7% and 14.5% (Spitzberg and Hoobler, 2002, Alexy *et al.*, 2005, Sheridan and Grant, 2007). The findings of this study indicate that 8.7% of respondents had experienced cyberstalking; this is in line with previous studies. Although other studies have found that the victims of cyberstalking tend to be female (D'Ovidio and Doyle, 2003, Sheridan and Grant, 2007, Maple *et al.*, 2011), the results of this study show that young adolescent (12-14) males were 3 times more likely to have experienced cyberstalking compared to young adolescent females and adult males were 5 times more likely have experienced cyberstalking compared to adult females. These results are surprising as the victims of offline stalking are predominately female (Tjaden and Thoennes, 1998) and it would be expected that the victims of cyberstalking would be similar. However, Alexa *et al.* (2005) also found that males were more likely to be cyberstalked. They suggest that this is because traditionally stalking studies have focused on female participants. The qualitative interviews point to another possible explanation. A number of interviewees saw stalking as nothing more than voyeurism or nosiness. It is possible that male respondents to the survey saw stalking in this way and that the female respondents saw it as a more serious threat.

Meeting in person a stranger that was initially met online

The findings of this study are consistent with the findings of the Irish EU Kids Online study (O'Neill *et al.*, 2011). The EU Kids online study found that 10% of 15-16 year olds of respondents have gone to face to face meetings; this study found that 13% of 15-17 year olds had FtF meetings with a stranger they had met online. A gender effect is evident in this study, males are twice as likely as females to have a FtF meeting with a stranger that they had met online. This effect is evident across all age cohorts. Previous studies of adolescents have not found evidence of this gender effect (Valkenburg *et al.*, 2006, Livingstone *et al.*, 2011a, O'Neill *et al.*, 2011). As males are more likely than females to use SNSs to meet new friends and are more likely to place contact information online, it is not unsurprising that they would actually follow through and meet in person a someone that they have initially met online. This is an area that warrants further investigation.

Accidentally Finding Disturbing Content

Studies indicate that between a quarter and a third of children/adolescent Internet users had seen sexual material that they had not searched for (Mitchell *et al.*, 2003, NCTE/SAFT, 2003, Wolak *et al.*, 2006, WEBWISE, 2009). This study found lower rates and that 20% of younger adolescent's and 24% of older adolescents have encountered disturbing content on SNSs. As this study is specifically addressing the risk on SNSs, it is not surprising that the rates reported by this study would be lower. Similar to previous studies no significant gender differences are found in the levels of unwanted exposure (Mitchell *et al.*, 2003).

Previous studies have primarily examined the experiences of children and adolescents so it is interesting to note that 15% of emerging adults and 13% of adults have encountered disturbing content on SNSs.

Personal Information Risks:

Personal Information Misused by Strangers

In one of the few studies that has examined personal information misuse, the EU Kids Online study (Livingstone *et al.*, 2011a) asked whether children had experience of: someone using their password to access their information or for impersonation; someone misusing personal information; or if they had been cheated out of money on the Internet. The Irish study (O'Neill *et al.*, 2011) found that 12% of children had experienced one or more of these personal data misuses, this is above the European average of 9% (Livingstone *et al.*, 2011a). In this study the type of personal data misuse is not differentiated, and specifically addresses experiences of these risks on SNSs. It is therefore not possible to make any direct comparisons. This study found that 9% of adolescents have experienced this risk on SNSs. 5% of emerging adults and 8% of adults have also experienced this risk.

Personal Information Sold to Advertisers

Overall, 9% of respondents have experience of their information being sold to advertisers on SNSs. Only 4% of adolescents have experienced this risk compared to 12% of emerging adults and 17% of adults. No comparable studies are available.

Technology Risks:

Spam

A considerable proportion of respondents (41%) have experience of spam on SNSs. More males (46%) than females (38%) have experience of spam and adults (57%) and emerging adults (45%) are more likely to experience spam compared to adolescents (32%). The adult rates can be compared to those reported by a Sophos (2011) survey of 1,273 respondents. They found that 67% of respondents had experience of spam on SNSs. The Sophos report does not provide details of the respondents to the survey or how they were sampled, but as Sophos is an anti-virus company targeted at the corporate market and further questions in the survey addressed employee's behaviour on SNSs it is quite likely that the respondents were business users, as compared to end users in this study. In contrast to the findings of this study, previous studies based on experiments have found that females are more likely than males to be victims of phishing attacks (Jagatic *et al.*, 2007, Bailey *et al.*, 2008) or have found no evidence of a gender effect (Kumaraguru *et al.*, 2009). It is not clear why a higher proportion of males have experience of spam compared to females. Some possible explanations are that: spammers are targeting males over females; female profiles tend to be more restricted so spammers are not gaining as much access to females; males reveal more contact information and so are easier to target and females may not be recognizing spam attacks on SNSs as spam attacks are increasingly coming from friends. Further investigation is needed to clarify this gender difference.

Viruses

Overall, 14% of respondents have got a virus on a SNS. Only 10% of emerging adults have experienced this risk compared to 20% of adolescents and 24% of adults. The adult rates can be compared to those reported by a Sophos (2011) report which recorded much higher incidence rate of malware (40%). In the absence of detail of how the Sophos study was carried out and given that the authors have a vested interest in this area, caution needs to be exercised in interpreting the results.

Excessive use of SNSs:

Spending too much time on SNS

Overall, half of respondents feel that they spend too much time on SNSs. Females (56%) are more likely than males (42%) to spend too much time on SNS. This finding is expected as the results have shown females are more intensive users of SNSs. Age cohort differences are also evident with emerging adults (56%) and older adolescents (48%) more

likely to spend too much time on SNSs compared with younger adolescents (37%) and adults (33%). Again the emerging adult and older adolescent age groups use SNSs more intensively.

Replacing the Need to Meet up with Existing Friends

The Irish EU Kids Online study (O'Neill *et al.*, 2011) examined whether excessive Internet use displaced children's social or personal needs. They found that 45% of respondents felt that they have spent less time than they should with friends, family or doing schoolwork. A direct comparison is not possible as this study only addresses displacement of time with friends. This study found that 11.5% of adolescents feel that using SNSs replaces the need to meet up with friends. Similar rates are found for emerging adults, but only 4% of adults have experience of this risk.

Reputational Risks:

Being Hurt by Information Posted

Overall, 16% of respondents have been hurt by information that has been posted about them on SNSs. Older adolescents (23%) are the most likely to be hurt and adults (3%) the least likely to be hurt. Other studies have examined being hurt by information posted in conjunction with cyberbullying so it is not possible to make direct comparisons.

Embarrassing Information or Photos Seen by Others

Overall, 42% of respondents have had embarrassing information or photos seen by people they would prefer didn't see them. Females (50%) are more likely than males (30%) to have experience of this risk. This could be explained by the fact that more females place photos online or it could be that females are more sensitive to risks of this nature. Age cohort differences are also evident with emerging adults (48%) and older adolescents (42%) more likely to have experienced this compared to younger adolescents (31%) and adults (24%).

Threatening Risks	Findings Present Study	Findings Previous Studies	Comment
Bullying and Harassment			
Experience of Risk: Adolescent	8.5% (12-16 year olds)	Rates between 3% and 12.3%	Adolescent rates between bounds of previous studies.
Emerging Adult	6%	No comparable studies	
Adult	3%	No comparable studies	
Other findings	No gender effect	No consensus on gender effect	Similar to previous studies.
Cyberstalking			
Experience of Risk: Overall	8.7%	Rates between 3.7% and 14.5%	Current findings between bounds of previous studies.
Other findings	Victims tend to be male	Victims tend to be female but one study has found similar results	Result is surprising as victims of stalking are predominately female.
Meeting a Stranger			
Experience of Risk: Adolescent	13% (15-17 year olds)	10%	Similar to previous studies.
Emerging Adult	8%	No comparable studies	
Adult	10%	No comparable studies	
Other findings	Males more likely than females to meet a stranger	No gender differences	In contrast to previous studies, requires further investigation.
Disturbing Content			
Experience of Risk: Adolescent	22%	Rates between 25% and 33%	Similar to previous studies.
Emerging Adult	15%	No comparable studies	
Adult	13%	No comparable studies	
Other findings	No gender differences	No gender differences	Similar to previous studies.
Personal Information Risks			
Information Misused by Strangers			
Experience of Risk: Adolescent	9%	12%	Comparable study has combined a number of personal information risks, including impersonation and fraud, so results are not directly comparable
Emerging Adult	5%	No comparable studies	
Adult	8%	No comparable studies	
Information Sold to Advertisers			
Experience of Risk: Adolescent	9%	No comparable studies	
Emerging Adult	5%		
Adult	8%		

Technical Risks	Findings Present Study	Findings Previous Studies	Comment
Spam			
Experience of Risk: Adolescent Emerging Adult Adult	32% 45% 57%	No comparable studies No comparable studies 65%	Caution needs to be exercised in comparing results as comparable study is US based anti-virus software company
Other findings	More males than females have experienced spam	Females more likely to be the victims of spam	Not clear why higher proportion of males have experienced spam – requires further research
Viruses			
Experience of Risk: Adolescent Emerging Adult Adult	20% 10% 24%	No comparable studies No comparable studies 40%	Caution needs to be exercised in comparing results as comparable study is US based anti-virus software company
Excessive Use Risks			
Spending too much time on SNSs			
Experience of Risk: Adolescent Emerging Adult Adult	42% 56% 33%	No comparable studies	More prevalent for older adolescents (49%) than younger adolescents (37%)
Other findings	Females more likely to have experienced this risk	No comparable studies	As would be expected, females are more intensive users of SNSs
Replacing FtF meetings with friends			
Experience of Risk: Adolescent Emerging Adult Adult	11.5% 11.5% 4%	No comparable studies	
Reputational Risks			
Being hurt by information posted			
Experience of Risk: Adolescent Emerging Adult Adult	19.5% 16% 3%	No comparable studies	Other studies have examined this in conjunction with cyberbullying. More prevalent for older adolescents than younger adolescents.
Embarrassing information seen by others			
Experience of Risk: Adolescent Emerging Adult Adult	36% 48% 24%	No comparable studies	More prevalent for older adolescents (42%) than younger adolescents (31%)
Other findings	Females more likely to have experienced this risk	No comparable studies	Not clear why higher proportion of females have experienced this risk – requires further research

Table 6.2 Summary Prior Experience of Negative Events on SNSs

Summary

In this section the levels of prior experience of negative events on SNSs are compared to pervious studies in the area. Caution needs to be exercised in comparing studies, as differences in how variables are defined and measured, culture, age groups studied, sample sizes and methodology used and timing of studies can make comparisons difficult. Where possible the results of this study have been compared to studies that have been carried out at a similar timescale, on similar populations and on similar age groups. A comparison of the results show that the rates found for cyberbullying, cyberstalking, meeting in person a stranger that was initially met online, encountering disturbing content and personal information being misused by strangers are in line with those found in the previous studies.

To date, most studies have addressed the prevalence of these risks for children and adolescents. This study differs as it examines the prevalence of risks over a number of age cohorts and highlights that many of these risks have been experienced by emerging adults and adults. As shown in Sections 5.4.5 & 6.2.2, compared to adolescents, emerging adults and adults do perceive the impact of many of these risks as being less severe, but they still recognise that there are serious consequences to their age group from many of these risks. As the age profile on SNSs is widening, it is important that further research is carried out to fully assess the negative impact of these risks on these older age groups.

Some interesting and contradictory findings have been highlighted in this section. Contrary to expectations and the findings of previous studies, the results of this study show that males are more likely than females to be victims of cyberstalking and males are more likely than females to have a FtF meeting with a stranger that they have initially met online.

For the technical risks of spam and viruses the only comparable studies are those carried out by commercial anti-virus software vendors. Results of this study indicate lower rates for these risks. This discrepancy may be due to the fact that users are not recognising these attacks on SNSs, but caution has to be exercised in accepting the rates published by commercial anti-virus software vendors. These companies have a vested interest in publicising attacks of this nature. The findings of this study indicate that males have experienced more spam attacks than females. It is not clear why such a gender disparity exists, possible explanations are that spammers are targeting males over females; female profiles tend to be more restricted so spammers are not gaining as much access to females

or that males are better at recognising spam attacks. Further investigation is needed to clarify this gender difference.

For the excessive use risks and reputational risks, few comparable studies are available. As these risks are some of the most commonly experienced risks on SNSs, it is important that further studies evaluate the displacement effect of excessive use risks and the level of harm and effects on well-being from reputational risks.

6.3 Summary of Findings

While there have been numerous studies over the past number of years into users' use of and behaviour on SNSs as far as it is known, no studies to date have examined users' risk perception on SNSs. Understanding risk perception is important as it can explain why people chose to act in particular ways. This study is the first time that an extensive study of age related risk perception on SNSs has been undertaken. The findings from this research have in some cases confirmed those found in other studies and in a number of instances contradicted those found in previous work. The differences from previous research findings and the possible explanations for them have been discussed in the course of this chapter. This study has also revealed a number of new findings about risk perception and SNSs and has contributed to knowledge of this area. Some of these findings are intuitive; others are not. This section briefly reviews these findings.

This research examines why some users perceive themselves to be at high personal risk on SNSs and others do not. A model was derived to test what factors contribute to high levels of perceived personal risk, see Section 3.7, Figure 3.6. This model was tested on five negative events that can occur on SNSs: spending too much time on SNSs; being bullied or harassed; embarrassing information or photos being by people who you would prefer didn't see it; personal information being sold to advertisers and receiving spam. Following detailed analysis a modified model is proposed, as shown in Figure 6.1.

Three factors are significant predictors of the likelihood of high personal (i.e. likelihood) risk perceptions across all of the five risks examined, prior experience of the risk, concern about the risk and age group. The most significant predictor of high personal risk (i.e. likelihood) perception for all of the negative events is prior experience. With regard to age

group, adolescents are more likely than emerging adults to see themselves at high personal risk for all the negative events except excessive use of SNSs. Increased concern/worry about a risk is a significant predictor of high personal risk for all the negative events, but the predictive value of concern is not as strong as prior experience.

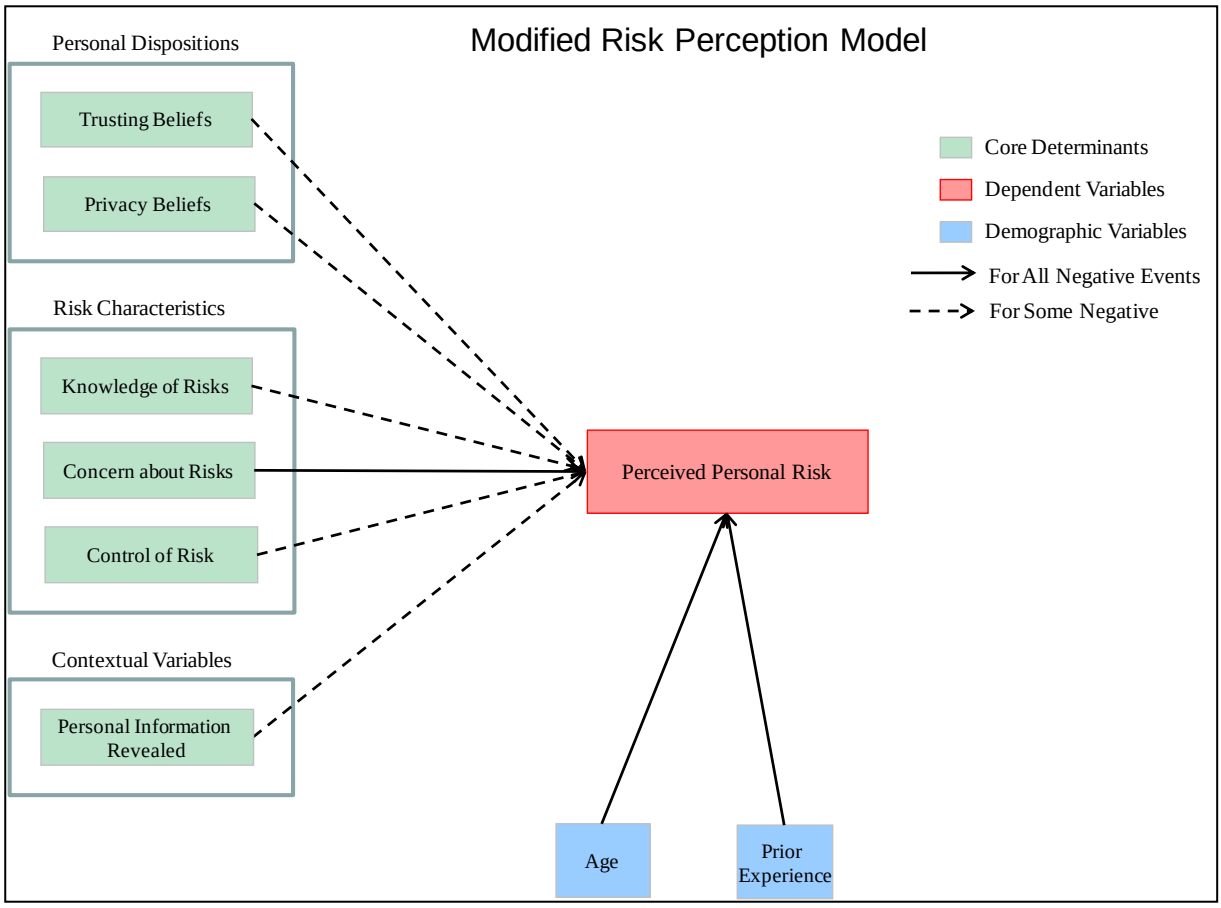


Figure 6.1 Modified Risk Perception Model

Although suggested as significant predictors of risk perception by the psychometric paradigm, both knowledge of risk and controllability of risk show small effects on the likelihood of high personal risk perceptions. These effects are evident for some risk categories but not for others. For the controllability of risk, some of the findings appear counterintuitive and it may be that other psychological aspects of control, such as locus of control, could provide a better explanation for the results found. Knowledge of risk is only a significant predictor of personal risk perceptions for the excessive use risk.

As is expected, individuals with higher levels of online privacy concerns perceive themselves to be at high personal risk for the personal information risk. The predictive significance of disposition to trust is more tenuous. Contrary to previous risk perception studies, gender is not a significant predictor for any of the risk categories. Level of

Internet experience, intensity of SNS use and the quantity of personal information revealed are not significant predictors of high personal risk perceptions.

With regard to the perception of risk on SNSs, this study has found that although users are aware of and recognise the severity of the risks on SNSs, they are unconcerned about most of these risks and do not perceive that these negative events are likely to happen to them. Contrary to expectations risk perceptions are not high for the more serious threatening risks on SNSs such as cyberbullying, and meeting a stranger. The perceived likelihood of these risks is low and optimistic bias was particularly high for many of the threatening risks. The fact that users perceive that threatening risks are significantly more likely to happen to others and not to themselves provides a possible explanation for why risk perceptions are not higher for these risks. The research suggests that individuals may be adopting an instinctive intuitive reaction to risk rather than making a reasoned analysis of the risks, following the affect heuristic or a "*risk as feelings*" approach.

Some age effects are evident with regard to risk perceptions on SNSs. Again some of these are counterintuitive. Whilst one might expect risk perceptions to increase with age, the findings suggest that, compared to the other age cohorts, adolescents feel they are more likely to be at risk on SNSs. They also express higher levels of risk awareness and higher levels of concern about the risks. This could indicate that Internet safety awareness campaigns targeted at adolescents are having an effect. It is also possible that adolescents engage with new technologies more readily and tend to be early adopters, they often know more about these technologies (including the risks) than older age cohorts. The fact that adolescents compared to the older age cohorts have higher levels of risk perception may appear counterintuitive, but previous studies indicate that there is an inverse relationship between risk perception and age.

Although there is a high level of awareness of the majority of risks on SNSs, the quantitative and qualitative analyses show some risks are less well known, in particular getting viruses on SNS and that personal information can be harvested. Users show little awareness that their personal information can be aggregated over time and combined with other online and offline sources to allow detailed profiles of them to be built. This threat is exacerbated because most users are unaware of the potential audience on SNSs, how easily their data can be accessed and the business model behind SNSs. This lack of awareness is reflected in users' behaviour on SNSs in that users continue to reveal substantial amounts of personal information on their SNS profile.

6.4 Contribution

6.4.1 Theoretical

This section outlines the contribution to theory made by this research. This research has addressed a number of deficiencies in the current literature and research to date. In so doing, it proposes a more holistic and comprehensive model of risk perceptions in SNS than has hitherto been available. While there is further research to be done to refine this model, it represents a considerable advance on existing models and theories and provides a number of significant new insights.

The deficiencies in the literature which have been discussed in chapters 2 & 3 are briefly reiterated in order to demonstrate the research contribution.

A number of deficiencies have been identified in the literature. These include:

- There is no single, universally accepted paradigm for assessing risk perception. As a result there is a lack of coherence in the literature;
- Studies of risk perception in the information systems literature generally fail to address the complexity of risk perception;
- There has been a lack of SNS studies that examine the effects of risks on users and the factors that can contribute to high risk perception;
- There has been a lack of SNS risk research on older age cohorts and age comparative studies;
- The risk agenda has been set by researchers rather than by users;
- Studies to date have not addressed the wide variety of risks that can be encountered on SNSs;

<u>There is no single, universally accepted paradigm for assessing risk perception</u>

The literature demonstrates that risk perception is a complex and multidimensional concept that not only involves people beliefs, judgement and feelings about risk, but also their cultural and social dispositions towards risk. The field of risk perception research is marked by considerable theoretical and methodological differences. The two most influential areas of risk perception research have been the psychometric paradigm (Fischhoff *et al.*, 1978, Slovic *et al.*, 1984) and Cultural Theory (Douglas and Wildavsky,

1982). There is currently no theory that integrates or attempts to integrate these. This research has therefore been directed at the interaction between the psychological and social cultural paradigms in an attempt to bridge the paradigmatic gap. The psychometric approach has been criticised because it does not address the fact that risk can be socially constructed (Rogers, 1997, Lupton, 1999). This has led leading exponents of the psychometric approach to begin to take account of social, political and cultural factors such as gender, race, emotions, control, and trust in shaping risk perception. As stated by (Renn, 2008) to understand risk perception it is necessary to study its psychological, social and cultural components and their mutual interactions. This research contributes to the field by proposing a model that examines many of the risk characteristics suggested by the psychometric paradigm, but includes other biological, psychological and social factors that have been shown to influence risk perception. These factors were identified by examining the extant literature relating to risk perception with a particular emphasis placed on research related to adolescents and emerging adults, IS/ICT risks and Internet shopping. Further factors were identified by examining the SNS literature. The choice of factors has been discussed in detail in Section 3.7. The resultant refined model, provides a holistic framework for assessing perceived risk.

Studies of risk perception in the IS literature generally fail to address the complexity of risk perception

As discussed in chapter 2, there is a limited body of research examining risk perception with relation to IS/ICT risks. The studies have examined a diverse range of IS/ICT risks from a number of different angles and thus there is little commonality in the findings with regard to risk perception, but the research does show that a number of risk perception theories, including the psychometric paradigm, Cultural Theory and SARF, can be successfully applied in the IS/ICT domain (e.g. Bener, 2000, MacGregor, 2003, Coles and Hodgkinson, 2008).

While the risk characteristics examined vary between studies, some gaps are evident. Many of the IS/ICT studies have not taken into account prior experience of a risk (Coles and Hodgkinson, 2008, Gabriel and Nyshadham, 2008) and those that have accounted for prior experience have come to no conclusions with regard to its relationship to risk perception (Sjöberg and Fromm, 2001, Campbell *et al.*, 2007). This gap is also evident in the extant risk perception literature. Although it is clear that prior experience of a negative event is an important determinant of risk perception (Eiser, 2004), to date few studies have

examined the relationship between experience of a risk and general risk perceptions and of the studies that do, these studies provide few coherent conclusions (Breakwell, 2007).

A sizeable body of research exists in the e-commerce literature relating to Internet shopping that has examined risk perception in more detail and how it affects online purchasing behaviour (For e.g: Jarvenpaa *et al.*, 2000, McKnight *et al.*, 2002, Gefen *et al.*, 2003, Pavlou, 2003). However, many of these studies can be criticised because perceived risk has been treated as a one-dimensional construct despite the fact that a large body of literature indicates that risk perception is a complex, multidimensional construct.

Many of the studies examining risk perceptions with relation to IS/ICT risks and also in the online shopping literature have not addressed the psychological and social aspects of risk perception. This is an important consideration as information systems are essentially social systems (Adams and Sasse, 1999, Gonzalez and Sawicka, 2002, Backhouse *et al.*, 2004, Besnard and Arief, 2004, Dourish *et al.*, 2004, Cranor, 2008).

This research addresses these deficiencies by not only assessing the cognitive and affective dimensions of risk perception but also by examining how age, gender, prior experience of negative event, disposition to trust, online privacy concern and other contextual variables such as Internet experience, intensity of SNS use and amount of information revealed can influence risk perception. Examining risk perception in this way provides a holistic and improved understanding of the risk environment and this is further enriched by the inclusion of qualitative research. The test results of the study were used to refine the initial model and the resulting model provides a preliminary framework that captures the factors that influence risk perception on SNSs. This framework increases our knowledge and understanding of the factors that predict high personal risk perceptions on SNSs. This can inform not only further studies of SNS risks, but also studies of IS/ICT risks and e-commerce research.

<u>There has been a lack of SNS studies that examine the effects of risks on users and the factors that can contribute to high risk perception</u>

Research examining risks on SNSs has examined the prevalence of these negative events, but has made little progress in researching the relationship between risk and harm (Staksrud and Livingstone, 2008). This study addresses this deficiency by examining users risk perception on SNSs. This provides not only an improved understanding of the

perceived personal risk (i.e. likelihood) of negative events on SNSs, but also the perceived consequences of the risk. The survey also measures users expressed levels of concern about negative events on SNSs and this provides further insight in this regard. This study, as far as it is known, is the first study to examine risk perceptions of negative events on SNSs. This contributes to knowledge in this area by determining the structure of risk perceptions on SNSs and by examining the factors that contribute to high risk perception on SNSs.

There has been a lack of SNS risk research on older age cohorts and age comparative studies

Many of the risks encountered on SNSs can pose threats for adults, but are considered of more concern for children as they may not have yet developed adequate coping mechanisms to deal with these threats. Most of the previous studies examining SNSs risks have been carried out on children and adolescents, so it is not known how risks on SNSs may affect older age groups. This study is, as far as it is known, the first to comprehensively examine different age cohorts views and perceptions of the risks associated with SNS use. This provides an important contribution to the understanding of risks on SNSs and allows a detailed examination of how risks are perceived by different age cohorts, but also allows comparisons between age groups and presents further new findings with regard to how risk perceptions change across age groups.

The risk agenda has been set by researchers rather than by users

A criticism of previous risk perception studies (Moore and Gullone, 1996, Millstein and Halpern-Felsher, 2002a) and studies of online risks carried out on children and adolescents (Livingstone and Haddon, 2008) is that the risks studied have been determined by the researchers or by adult society. This can mean that the risks studied may not necessarily reflect users' concerns. This study has addressed these limitations by bringing together a wide range of different categories of risk that can be experienced on SNSs and including negative events identified by the users themselves. This provides a better understanding of the risks that are of particular concern to users.

Studies to date have not addressed the wide variety of risks that can be encountered on SNSs

Up to now, the risk agenda has been largely driven by researchers and areas of public concern. Consequently research has tended to focus on the more threatening risks such as

cyberbullying, encountering pornography, paedophiles, stranger contact and so on. As a result there is little available research on commercial risks, personal information risks, reputational risks or the impact of excessive use of SNSs. This research addresses this gap by examining a wide-ranging list of negative events that can happen on SNSs. This not only provides a comprehensive assessment of the risks on SNSs but allows for a ranking of negative events.

Other theoretical contributions

The following are theoretical contributions made by this research which were not identified as deficiencies in the literature:

1. Although most recent studies in risk perception have diversified to include biological, psychological and social risk factors, for many studies the risk factors seem to be included on an *ad hoc* basis. There is evidently a need for an all encompassing theoretical framework that includes all the factors that might influence an individuals' risk perceptions. This research contributes to developing this framework. To develop the initial test framework in a holistic manner, a number of literatures were consulted. This framework was tested on a number of test populations and this led to further refinements. The resultant framework helps in informing research about the elements that contribute to risk perception for SNS risks and ICT/IS risk environments.

2. Although the principal aim of this research is to address risk perceptions on SNSs, the study also examined user's use and behaviour on SNSs. Although some previous studies have examined age differences with relation to SNS use and behaviour (OFCOM, 2008, Brandtzæg *et al.*, 2010, Nosko *et al.*, 2010, EUROBAROMETER, 2011, Pollet *et al.*, 2011), none of the studies have examined age related differences in a comprehensive manner and compared, as this study does, adolescents, emerging adults and adults.

3. The study also examines optimistic bias, i.e. to what extent users think that others are more likely than themselves to experience negative events on SNSs. In contrast to previous studies, this research examines whether optimistic bias is higher for certain negative events that can be encountered on SNSs.

6.4.2 Practical

There is a number of difficulties in addressing risk and privacy concerns on SNSs. The obvious practical question is how can such concerns be addressed and the risks of using SNSs reduced? As the likelihood of experiencing a negative event on SNSs increases with use, one option is to limit access to SNSs. This is not a realistic solution as limiting access also reduces the many benefits that users gain from using SNSs. Many if not most users in first world countries today have unlimited access to the Internet at home, at work or in college and increasingly through smart phones. The nature of SNSs creates further difficulties. The aim of SNSs sites is to create a culture of openness and transparency and this can create formidable challenges for users who are trying to protect their privacy. Rather than restricting use of SNSs, the focus should be on educating users about the risk and privacy implications of using SNSs and providing users with adequate mechanisms to cope with these risks and also by providing suitable privacy protection mechanisms on SNSs.

User education has been a key element in helping users (both adults and children) recognise and avoid online risks. In the UK, there is a Get Safe Online initiative (http://www.getsafeonline.org/). This is a joint initiative between the UK Government, law enforcement, leading businesses and the public sector, which provides computer users and small businesses with free, independent, user-friendly advice that will allow them to use the Internet confidently, safely and securely. A similar initiative is the Make IT Secure initiative in Ireland (http://www.makeitsecure.org/en/index.html). However there have also been many campaigns aimed at young people and their parents, to educate them on how to protect themselves in these online environments. The EU's Safer Internet Programme aims at creating a safer online environment for young people and helps fund awareness initiatives in member states, e.g. the Safer Internet Ireland Project. The EU has also worked towards improving legislation to protect children online.

There have also been some multi-stakeholder and cross industry dialogues within the EU aimed at improving establishing good practices for SNSs. These have led to guidelines such as the Safer Social Networking Principles for the EU (2009). These guidelines provided recommendations for social networking service providers to enhance the safety of children and young people using their services. In an evaluation of how these guidelines

have been implemented, Staksrud and Lobe (2010) highlight that these guidelines have had some success, but there remain areas for improvement.

The findings of this research provide a number of suggestions for raising awareness about the risks on SNSs, in particular highlighting risk areas and misconceptions that need to be addressed, highlighting target groups and the form of the awareness message.

Implications for Safety Awareness Initiatives

The findings of this study highlight a number of areas where there is a lack of awareness, misunderstandings or misconceptions that need to be addressed:

- While previous awareness campaigns have concentrated on raising awareness of the serious threatening risks on SNSs, there is a broad range of other risks that can be encountered on SNSs including personal information risks, technical risks, excessive use risks and reputational risks. This study highlights the prevalence and users' concern about other risk areas that can be encountered on SNSs. Safety awareness initiatives need to be extended to address these additional risk areas.
- Many respondents to this study were unaware that viruses and malware can be transmitted via SNSs. Users need to be made aware of this possibility and that fraudsters are using many social engineering techniques, including spoofed messages appearing to be from friends, to get users to click on links to malware/viruses.
- Although users continue to reveal substantial amounts of personal information on SNSs, many are not fully aware of the personal information risks associated with SNS use. Users need to be educated as to how easily their personal information can be harvested, how profiles can be built of users and how data can be aggregated over time. Users need to understand the permanence of data on the Internet and that data cannot be completely deleted as it may be stored elsewhere and indefinitely. Related to this is the possible audience for this information which is potentially anyone, anytime, anywhere including future employers and state agencies. User show a lack of awareness of the business motivations behind SNSs, they are unaware of the commercial value of the personal information they reveal, especially when it is aggregated over time. It is important that users are made aware of what personal information is held about them, how this personal information is used and who it is shared with.

- The findings of this study show that adolescents are less likely than the older age cohorts to have restricted their privacy settings and that many users and in particular adolescents find it difficult to manage privacy settings on SNSs. Although SNS companies clearly have a role in making their privacy settings easy and intuitive to use, commercial logic suggests that SNS companies are unlikely to emphasise protecting data as strongly as sharing personal information. This means that there is a continuing role for safety awareness initiatives to educate users on how to protect themselves on SNSs, which need to be targeted at younger users.
- This study has found that users are underestimating the amount of time they spend on SNSs and show a lack of concern about the time they are spending online. Users need to be informed of the time wasting aspects of these technologies and how using SNSs may be displacing time spent studying and in other productive activities (including exercise). Users need to be given guidance on how to manage the time they spend online.

This study highlights some issues with regard to the targets of safety awareness initiatives:

- This study highlights that the prevalence of risk and risky behaviours on SNSs is evident at all age groups. To date, most safety awareness campaigns have been targeted at younger users. This research suggests that that safety awareness initiatives need to be targeted at older age groups, although this is predicated on further research being carried out to assess the impact of these negative events on older age groups.
- The research also shows that certain risks are more prevalent in certain age groups and this insight can be used for more effectively targeted awareness campaigns, for example older users are more likely to be the victims of spam and personal information attacks.

This research highlights some important considerations in how safety messages are transmitted to users:

- Users are more likely to perceive themselves at high risk of a negative event on SNSs if they have personally experienced the negative event. It is usually as a result of experiencing a negative event that users change their behaviour on SNSs. This creates difficulties for safety awareness initiatives as they need to make risks

appear as real risks that are taken seriously by users who have not yet encountered actual privacy violations. A careful balance has to be achieved as overemphasising the likelihood of negative events can be counterproductive as users will become aware that most of their experiences on SNSs do not lead to negative outcomes. As suggested by Millstein and Halpern-Felsher (2002b) safety awareness initiatives need to find ways to translate small probabilities into real possibilities without raising anxiety to unproductive levels.

- This study highlights a further difficulty. Many users think that they are less likely than others to encounter risk on SNSs. This creates difficulties for awareness initiatives as users with a strong optimistic bias may think that the message is not directed at them, but at others. To overcome these difficulties safety awareness initiatives have to make the risks encountered on SNSs salient, personal and real for users.
- As this study has found that the affective/emotional characteristics of risk increase the likelihood that users perceive themselves at high risk on SNSs, is important that safety initiatives target the emotional meaning and impact of negative events on SNSs in order to achieve maximum effectiveness.

A further question arises as to how safety awareness messages should be disseminated to users? It has been suggested by some researchers (Mitchell and Ybarra, 2009) and also by a number of interviewees in this study that using SNSs would be an effective way to disseminate safety awareness messages. It is suggested that users are more likely to relate to these messages on a personal level as they come from the technology they are using. (Millstein and Halpern-Felsher, 2002b) have suggested utilising the social normative component in safety awareness initiatives for adolescents because of the strong effect of peer influence in adolescence. As peer influence is a strong component in SNSs and this study has shown that many users gain their awareness of the risks from informal sources such as peers, this suggestion has clearly some merit. However this study has found that these informal sources may not be entirely reliable and that even more experienced users of the Internet are not necessarily more aware of the risks on SNSs. Before disseminating messages on SNSs or using peers as a medium for safety awareness initiatives, it is important that there be reliable sources of information available regarding the risks on SNSs. There are clear advantages in disseminating a message on SNSs as the message is spread quickly and the reach is vast. This advantage is also the main disadvantage particularly if the message is incorrect, tampered with, or misinterpreted. As shown by the

social amplification of risk framework (SARF), see Section 2.3.5, the impacts of an adverse event can have large ripple effects and this will be especially amplified on SNSs. Clearly there are advantages in using SNSs or peers to disseminate safety awareness messages but caution needs to be exercised and further research is needed to assess the most effective way to circulate messages.

It is not easy to effectively get messages across to SNSs users that result in them taking the message seriously, that they feel is personally relevant to them and that result in users adapting their behaviour. It is therefore important that awareness initiatives are monitored to ensure that they are translated into risk perceptions or modifications of risky behaviour. A further concern is that the SNS landscape is evolving, the SNSs and technology environment is continuously changing, adding new functionalities which in turn can result in the risk landscape changing. As criminals and fraudsters continue to move to this medium new risks will continue to emerge. This too poses a challenge for awareness initiatives that constantly have to be updated to reflect the changing risk landscape.

A wide range of stakeholders have a role to play in managing and informing users of the potential risks on SNSs, including: governments and regulators; SNS organisations and schools, colleges and employers and parents. The following section describes the implications of the research findings for each of these stakeholder areas.

Implications for Governments and Regulators

It is not clear that SNS users are acting rationally when it comes to personal privacy (Acquisti, 2004). This lack of rationality is evident in this study, as some users express high levels of online privacy concern, but continue to reveal large amounts of personal information. It is also not clear that increasing awareness of this issue would necessarily change user's behaviour and it may be that regulation is needed to protect user's privacy and to restrict data collection in the first place. Although users willingly provide this personal information, the findings of this study show that users are not fully aware of the implications of sharing such large amounts of information and indeed the long term implications of revealing this information are as yet unknown. It is also questionable whether single commercial organisations such as Facebook should be allowed hold such large repositories of personal information. Ultimately control of this personal information should be in hands of the user, but this too will require regulation.

Implications for SNS Organisations and Technology

This research shows that many users, particularly younger users, have difficulty with the privacy settings on SNSs. Many users also accept the SNS default settings which are not generally set to be restrictive. Ideally SNS organisations should design privacy protection features that are easy and intuitive to use and ensure that the default privacy settings offer maximum protection for users. Some innovative measures have been suggested, for example Kelley *et al.* (2009), suggest the use of standardised "*privacy nutrition labels*" similar to nutritional labels on food. These labels can show SNS users, in a visual way, areas of concern with regard to their privacy practices. Other researchers have examined how simplified encryption techniques could be employed amongst groups of users on SNSs, thus allowing users to continue to use the functionality of SNSs, but giving users increased control over who has access to their communications and personal information (e.g. Guha *et al.*, 2008).

However, it is in the commercial interest of SNSs to encourage data sharing rather than discourage sharing so it is unlikely that they will implement measures such as these unless required by law to do so.

Implications for schools, colleges and workplaces

Schools, colleges and work organisations need to be aware of the risks that SNSs pose to their students and employees, but that they can also cause serious damage to the reputation of the organisation. These organisations also have a role in informing their users about these risks.

Summary and Discussion

Users need to be made aware of the saliency of the risks that can be encountered on SNSs, safety awareness initiatives need to address the emotive response to risk, make the risks real and make users aware that can be personally at risk. This will not be easy to achieve and it is likely that awareness initiatives alone may not be able to fully address the privacy problems and other risks associated with SNS use. A combination of technology improvements, awareness and regulative policies may be needed to protect users on SNSs. Initially research should be directed towards evaluating the effectiveness of awareness initiatives and if these initiatives are not proving successful, the regulatory and technical options need to be investigated.

A full discussion of the privacy implications of SNSs is beyond the scope of this thesis, but some observations about privacy are warranted. Clearly SNSs are not only changing how users communicate, but also what they share online and there is the potential that this could change how people view privacy. Society can choose to accept this and acknowledge that personal privacy is no longer a salient issue. People will have to be happy to live out their lives in the public gaze, with no secrets. As the Internet never forgets and what you said as a teenager or in the heat of the moment could potentially haunt you the rest of your live, it will be necessary for as suggested by Mayer-Schönberger (2011) for society to become more forgiving or adopt some element of forgetting. This will not be easy to achieve and will require a change in behavioural norms. In the meantime individuals will be judged by what they post and what is posted about them online. Society on the other hand can choose to protect personal privacy. It is of particular concern that large commercial organisations such as Facebook and Google can hold such large repositories of personal information about users. This study shows that users show a lack of awareness of the business aspect of these companies and underestimate the commercial value of the personal information they reveal on SNSs. Users place a considerable amount of trust in these companies. Users need to be better informed of what data is held about them, who has access to it and what it is used for. As stated by Schneier (2010) the only solution may be to develop broad legislation protecting personal privacy by giving people control over their personal data. Society is at an important crossroads in this regard, as we continue to live more and more of our lives online, it will be interesting to see which road society will take. Research of this nature can help inform this debate, as this is a rapidly changing environment clearly further research is needed in this area. Areas for future research are highlighted in the next chapter.

7. Chapter 7

7.1 Conclusions

Since the mid 2000s the growth of SNSs has been remarkable. SNSs sites offer many benefits to users, but there are risks in using these sites. To date most studies have examined the prevalence and impact of these risks for adolescents and to lesser extent emerging adults, as these age groups were seen as the primary users of SNSs. However, recent evidence shows that the growth in the numbers using SNSs is continuing with particular growth in the older age groups. As far as it is known, this is the first study of its kind to examine risk prevalence on SNSs across a number of age groups, including adults. It is also the first study to examine users' perceptions of these risks.

This study adopts a two-phase explanatory mixed methods design. The first phase of the study uses surveys of 551 adolescents, 1044 emerging adults and 156 adults to obtain statistical, quantitative results. The second phase of the study follows up with 15 semi-structured interviews (emerging adults) and four focus group discussions (adolescents) to explore these results in more depth.

Some of the findings confirm the findings of previous research. For example this study found that users primarily use SNSs to keep in contact with existing friends. Although many users express concern about their privacy on SNSs, users, especially older adolescents and emerging adults continue to reveal substantial amounts of personal information on SNSs. The prevalence of risk found in this study is similar to that in previous studies.

Other findings are new and highlight some concerns about how users perceive risk on SNSs. The research reveals some ironies; although users are aware of the risks on SNSs and acknowledge the severity of the risks, they are not concerned about these risks and do not perceive themselves to be at risk. Furthermore they view their peer group to be at greater risk than they are. For most of the negative events on SNSs, adolescents compared to the other age groups perceive themselves to be at a higher risk, show higher levels of awareness, are more concerned and perceive the consequences of the risk to be higher.

Prior experience, concern about risk and age are all significant predictors of a user perceiving him or herself to be at high personal risk on SNSs.

This study addresses a number of gaps in the extant literature and the research findings provide both a theoretical and a practical contribution. The results of the research include a preliminary framework that captures the factors that influence risk perception on SNSs. The findings of this research can inform not only further studies of SNS risks but also studies of other IS/ICT risks.

7.2 Limitations

As in all research of this nature, there are limitations to the study and the need and opportunities for further research.

This study has addressed some of the limitations of the psychometric paradigm by testing a risk perception model that extends beyond the psychometric paradigm to include other variables such as age, gender, disposition to trust, online privacy concerns and other contextual variables. However, the risk perception measures adopted in this study are based on self expressions of affective feelings and cognitions and not on actual behaviour. This study has not examined how these risk perceptions have modified behaviours on SNSs. It has not explored, for example if a user perceived him or herself to be at high risk of (say) cyberbullying on SNSs, how their behaviour on SNSs might have changed over time, if at all? It is important to recognise that the risk perception measures and other measures such as disposition to trust, online privacy concern etc. used in this study assume that risk, privacy concerns etc. can be subjectively defined by individuals.

In order to address the research questions posed by this research, a key consideration was that the study needed to be carried out on a number of age groups, specifically adolescents, emerging adults and adults. Due to feasibility and practical considerations, a choice was made to access adolescents through schools, emerging adults through a university and adults through workplaces. For ease of access, the study was limited to an urban area. Further external limitations arise from the fact that, in several cases where potential samples of schools and workplaces were identified, the schools and companies refused to give access to their pupils/employees. It is not claimed that samples in this study are a fully random representation of the entire Irish online population. Rather they were chosen

with the understanding that they would be most likely to provide the required information for this study. However they do represent a reasonably wide spectrum of the relevant populations. In addition, this study investigates risk perceptions of SNSs at a particular moment in time. As with any Internet technology, SNSs evolve over time and SNS use and the risk landscape on SNSs is constantly changing and evolving. Due to these limitations caution needs to be exercised in generalising the findings of this study to all current Internet users in Ireland. However the basic functionality of SNSs has not changed and this study is valuable in offering insights into risk perceptions on SNSs and how they differ across age groups. The findings would also be useful as a historical data point in a longitudinal analysis.

Due to the cross sectional nature of the data, it is not possible to explore causality between variables. For example, it is unclear whether having an increased concern about a risk is a cause or a consequence of a high risk perception. This combined with the limitations highlighted above point to the need for longitudinal studies to explore how risk perception may change over time and the factors that contribute to this change. In particular it would be interesting to study whether older and younger adults differ in their risk perceptions.

A further limitation relates to the fact that there may be other factors that contribute to risk perception that have not been identified by this study. For example, the findings of this analysis suggest that users with high personal risk perception perceive the excessive use risk of spending too much time on SNSs to be less controllable. This finding appears counterintuitive and suggests that this measure of control may not be adequately measuring users' perceptions of control. A possible explanation could be that those that perceive themselves at high personal risk tend to display an external locus of control and thus feel less able to control negative events on SNSs. Those with an external locus of control believe that events in their environment are outside their control.

All research methods have advantages and disadvantages, in this study surveys were used as a means of assessing risk perceptions for large sample groups, however surveys only provide a surface level of description and rely on self-reported measures which can introduce error into findings. To counteract these limitations semi-structured interviews and focus groups were used to provide a deeper level of analysis and explanation. This combination of methods helps to mitigate weaknesses in individual methodologies; however some methodological limitations are evident in this study.

Some of the measures used in this study are limited in their scope. For example: in this study prior experience was measured as a dichotomous yes/no variable and other aspects of prior experience such as frequency of prior experience; intensity of prior experience, timing of prior experience, harm from prior experience etc. were not examined. As the primary aim of this study was to identify the factors that contribute to risk perception, a decision was made to measure more factors at a higher level of granularity rather than include detailed measurements of individual factors.

A number of different scales has been used in the IS literature to measure peer and social influence, for example (Davis, 1989a, Ajzen, 1991, Moore and Benbasat, 1991, Thompson *et al.*, 1991, Taylor and Todd, 1995a, Taylor and Todd, 1995b). A choice was made to use the Taylor and Todd (1995b) scale in this study. Although Taylor and Todd recorded a reliability coefficient of 0.92 for this scale, the overall reliability coefficient recorded for the scale in this study was 0.41. The scale proved unreliable across all age cohorts. It is difficult to explain this finding as numerous IS studies have successfully used this scale to assess peer influence (for e.g. Bhattacherjee, 2000, Hung *et al.*, 2003, Shen *et al.*, 2006, Tan *et al.*, 2007, To *et al.*, 2008) and the scale items appear to logically measure the same construct. Further analysis is needed to examine the problems experienced with this scale. For analysis purposes a single item measurement was used for peer influence.

7.3 Future Work

This dissertation provides a strong theoretical basis for future research. The findings with relation to risk perception of negative events on SNSs and the resultant model of the factors that influence high personal risk perception advances our knowledge of how risk is perceived on SNSs. However further empirical validation is necessary to confirm the findings of this study. Further testing of this model is required in other countries in order to establish whether it is culture independent, i.e. robust regardless of culture. The model needs to be tested on a wider range of ages, in particular younger and older Internet users.

SNS's, like much else on the Internet, continue to evolve not only in functionality but in how they are used. Research in this field becomes quickly out of date. During the course of this study, new functionalities and new risks possibilities have emerged with SNSs. The use of apps has increased on SNSs, allowing users to log into third party sites using their

profile information and thus sharing their information with these third party sites. SNSs continue to incorporate functionality that encourages users to share increasing amounts of personal information. For example Facebook recently launched Timeline, which Mark Zuckerburg explained, is "*the story of your life*". Timeline allows users to present "*all your stories, all your apps, and a new way to express who you are*" (Terdiman, 2011). The use of smart phones as a medium for accessing SNSs has created further risks for users, for example, Facebook automatically posted mobile numbers of users who used their smart phone to access Facebook to their main Facebook profile.

Time sensitivity is thus an issue for research in this field, as the technologies and user practices all continue to change. In addition, individual's perceptions of risks are by no means constant, but can change in different social settings and in relation to new knowledge experiences. Clearly the findings must be regularly updated and this points, as suggested in Section 7.2, to the need for longitudinal studies to examine how the risk landscape and risk perceptions are changing over time. Longitudinal studies are also needed to determine causality: for example if the perceptions associated with negative events on SNSs occur prior to the experience of the negative event.

There is a need for studies that examine the relationship between risk perception and risk behaviour. Safety awareness initiatives can be used to get users to recognise and acknowledge their own vulnerability to negative outcomes; however, as stated in Section 6.4.2, it is important that longitudinal studies are used to evaluate the effectiveness of these initiatives. These evaluations should not rely only on self-reported measures, but examine actual behaviours on SNSs. It would be useful to carry out longitudinal studies that follow younger users before they begin to engage with SNSs and observe how their risk perceptions and actual behaviour on SNSs vary over time. A study of this nature could be carried out as part of larger national longitudinal studies of children, such as the Growing Up In Ireland study (http://www.growingup.ie). There are ethical considerations in monitoring actual behaviour on SNSs, in particular when participants are not informed. There is a danger too, if participants are informed, that they may modify their behaviour.

This study has examined risk perception from an individual perspective rather than a social perspective. Cultural Theory (Douglas and Wildavsky, 1982) recognises that risk judgements are not formed independently of social context. Social context is an important element of SNS use. As stated by Amichai Hamburger and Vinitzky (2010), people

function in social groups that have expectations as to how SNSs are used and this in turn can create pressure on individuals in what they display and how they behave on SNSs. It would be useful to understand if and how community members and groups influence how individuals regard risk on SNSs. Cultural Theory has proven difficult to test empirically, one alternative may be to use an approach based on a network theory of contagion (Burt, 1987) as empirically tested by Scherer and Cho (2003). This theory has emerged from social network studies and suggests that it is individuals and their relations with social networks that should be the units of analysis. The theory suggests that individuals adopt the attitudes or behaviours of others in their social network and this forms a cultural system of norms, expectations, knowledge and behavioural support (Monge and Contractor 2000). There are clear benefits in examining risk perception on SNSs from this perspective.

This research has focussed on SNSs, but other Web 2.0 technologies such as blogging, tweeting, instant messaging and other technologies such as texting all contribute to the amount of personal information revealed. The aggregation of information revealed across all Internet technologies increases the level of risk. It is important to examine the cumulative effects of these different technologies, not only in the amount of information revealed, but also in how they may increase user's vulnerability to other online risks.

This study provides a rich dataset that allows further analysis to be carried out. For example further analyses could include:

1. Examining correlations between experiences of negative events, for example if a user experiences a certain risk are they likely to experience others?
2. Examining correlations between risk perceptions of negative events;
3. Examining the profile of those that perceive themselves at low risk;
4. Comparing the risk perception profile of those with prior experience of risk against those with no prior experience;
5. Examining whether friends' experience of risk affects personal risk perceptions.

During the course of this research some other factors emerged as significant and worthy of further consideration. As stated in the previous section, locus of control may influence user's perceptions of how controllable risks are on SNSs. Other personality dispositions such as sensation seeking, level of extroversion/introversion and risk aversion may also effect risk perception on SNSs. Further empirical analysis is needed to examine the effects of these different factors.

This research highlights the need for improved measurement tools for assessing time spent on SNSs, see Section 6.2.5. The majority of studies estimate time spent on SNSs by asking survey respondents to estimate the frequency and duration of time they spend on SNSs. This study has found that this is not an adequate measure of the amount of time users spend on SNSs. An alternative approach is observation. The benefits of this include accuracy and detailed behavioural descriptions. The downside is the method is time consuming for the researcher. The digital log of time spent in applications can also provide the researcher with a more accurate measurement of user behaviour. This too has drawbacks as the presence of an observer even in the form of a digital log has the potential to alter the behaviour of the subject and may not be an accurate reflection of use when several applications and windows are open concurrently. The best solution, though not necessarily the most practical solution, would be to use eye tracking technology. Future studies need to assess the most effective measurement tools for assessing time spent on the Internet.

As this study has identified prior experience and age as significant predictors of a user perceiving him or herself to be at high personal risk on SNSs, future studies could examine these factors in more detail. With regard to prior experience, studies should examine the frequency of prior experience; the intensity of prior experience, the timing of prior experience and the harm from prior experience. Some researchers suggest that when assessing risk perceptions measures of psychosocial maturity should be used in addition with age to assess developmental differences (Cauffman and Steinberg, 2000, Curry and Youngblade, 2006). Future studies, particularly of children and adolescents should consider measuring psychological maturity. Psychosocial maturity can be measured using the Psychosocial Maturity Inventory, PSMI Form D (Greenberger *et al.*, 1975).

It was noted at the outset that SNSs have seen a phenomenal growth since the mid 2000s. Initially users on SNSs were predominately younger users, but the age profile has changed and SNSs are now popular with all age groups. Understanding how users at all age levels perceive risk on SNSs is important not only for researchers, but also for governments and regulators; SNS companies; schools; colleges; employers; parents and of course the users themselves. This dissertation has sought to advance this understanding by examining how users perceive risks on SNSs and the factors that influence risk perception.

BIBLIOGRAPHY

Acquisti, A. 2004. Privacy in electronic commerce and the economics of immediate gratification. *Proceedings of the 5th ACM conference on Electronic commerce.* New York, NY, USA: ACM.

Acquisti, A. & Gross, R. 2006. Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. *Privacy Enhancing Technologies.*

Acquisti, A. & Grossklags, J. 2005. Privacy and Rationality in Individual Decision Making. *IEEE Security and Privacy,* 3,1, 26-33.

Adams, A. & Sasse, M. A. 1999. Users Are Not The Enemy. *Communications of the ACM,* 42,12, 40-46.

Agar, M. & MacDonald, J. 1995. Focus groups and ethnography. *Human Organization,* 54,1, 78.

Ajzen, I. 1985. From intentions to actions: a theory of planned behavior. *In:* Kuhl, J. & Beckman, J. (eds.) *Control: From cognition to behaviors.* New York: Springer-Verlag.

Ajzen, I. 1991. The theory of planned behavior. *Organizational Behavior and Human Decision Processes,* 50,2, 179-211.

Alao, A. O., Soderberg, M., Pohl, E. L. & Alao, A. L. 2006. Cybersuicide: Review of the Role of the Internet on Suicide. *CyberPsychology & Behavior,* 9,4, 489-493.

Alberts, C. & Dorofee, A. 2002. *Managing Information Security Risks, The OCTAVE^{SM} Approach,* Boston, Addison-Wesley.

Alexy, E. M., Burgess, A. W., Baker, T. & Smoyak, S. A. 2005. Perceptions of Cyberstalking Among College Students. *Brief Treat Crisis Intervention,* 5,3, 279-289.

Alhakami, A. S. & Slovic, P. 1994. A Psychological Study of the Inverse Relationship Between Perceived Risk and Perceived Benefit. *Risk Analysis,* 14,6, 1085-1096.

Allen, M., D'Alessio, D. & Brezgel, K. 1995. A Meta-Analysis Summarizing the Effects of Pornography II Aggression After Exposure. *Human Communication Research,* 22,2, 258-283.

Amichai-Hamburger, Y. & Ben-Artzi, E. 2003. Loneliness and Internet use. *Computers in Human Behavior,* 19,1, 71-80.

Amichai-Hamburger, Y. & Vinitzky, G. 2010. Social network use and personality. *Computers in Human Behavior,* 26,6, 1289-1295.

Amichai-Hamburger, Y., Wainapel, G. & Fox, S. 2002. "On the Internet No One Knows I'm an Introvert": Extroversion, Neuroticism, and Internet Interaction. *CyberPsychology & Behavior,* 5,2, 125-128.

Anchor 2007. Anchor Watch Your Space 2007 Survey. Anchor Youth Centre and NCTE.

Anchor 2008a. 2008 Watch Your Space - Survey of Irish Teenagers Use of Social Networking Websites. National Centre for Technology in Education.

Anchor 2008b. Anchor Watch Your Space 2008 Survey. Anchor Youth Centre and NCTE.

Anderson, K. J. 2001. Internet Use Among College Students: An Exploratory Study. *JOURNAL OF AMERICAN COLLEGE HEALTH,* 50,1, 21-26.

Apple, A. L. & Messner, B. A. 2001. Paranoia and paradox: The apocalyptic rhetoric of Christian identity. *Western Journal of Communication,* 65,2, 206-227.

Armstrong, L., Phillips, J. G. & Saling, L. L. 2000. Potential determinants of heavier internet usage. *International Journal of Human-Computer Studies,* 53,4, 537-550.

Arnett, J. 1991. Still crazy after all these years: Reckless behavior among young adults aged 23-27. *Personality and Individual Differences,* 12,12, 1305-1313.

Arnett, J. 1992. Reckless behavior in adolescence: A developmental perspective. *Developmental Review,* 12,4, 339-373.

Arnett, J. 1994. Are college students adults? Their conceptions of the transition to adulthood. *Journal of Adult Development,* 1,4, 213-224.
Arnett, J. J. 1996. Sensation seeking, aggressiveness, and adolescent reckless behavior. *Personality and Individual Differences,* 20,6, 693-702.
Arnett, J. J. 2000a. Emerging adulthood: A theory of development from the late teens through the twenties. *American Psychologist,* 55,5, 469-480.
Arnett, J. J. 2000b. Optimistic bias in adolescent and adult smokers and nonsmokers. *Addictive Behaviors,* 25,4, 625-632.
Arnett, J. J. 2004. *Emerging adulthood : the winding road from the late teens through the twenties,* New York; Oxford, Oxford University Press.
Arnett, J. J., Offer, D. & Fine, M. A. 1997. Reckless driving in adolescence: 'State' and 'trait' factors. *Accident Analysis & Prevention,* 29,1, 57-63.
Ashton, R. H. & Kramer, S. S. 1980. Students As Surrogates in Behavioral Accounting Research: Some Evidence. *Journal of Accounting Research,* 18,1, 1-15.
Associated_Press & MTV 2009. AP-MTV Digital Abuse Study - Executive Summary. Associated Press and MTV.
Authority, H. E. 2009. *Undergraduate Enrolments - Full time and part time enrolments by gender, institution, and field of study 2008/2009* [Online]. Higher Education Authority. Available: http://www.hea.ie/en/node/288 [Accessed 24th August 2010 2010].
Avison, D. & Myers, M. 2005. Qualitative Research. *In:* Avison, D. & Pries-Heje, J. (eds.) *Research in information systems.* Oxford: Butterworth-Heinemann.
Avison, D. E., Dwivedi, Y. K., Fitzgerald, G. & Powell, P. 2008. The beginnings of a new era: time to reflect on 17 years of the ISJ. *Information Systems Journal,* 18,1, 5-21.
Back, L. 2002. Aryans reading Adorno: cyber-culture and twenty-firstcentury racism. *Ethnic and Racial Studies,* 25,4, 628-651.
Back, M. D., Stopfer, J. M., Vazire, S., Gaddis, S., Schmukle, S. C., Egloff, B. & Gosling, S. D. 2010. Facebook Profiles Reflect Actual Personality, Not Self-Idealization. *Psychological Science,* 21,3, 372-374.
Backhouse, J., Bener, A. B., Chauvidul, N., Wamala, F. & Willison, R. 2004. Risk managment in cyberspace. *Foresight Cyber Trust and Crime Prevention Project.* UK Office of Science and Technology.
Backstrom, L., Dwork, C. & Kleinberg, J. 2007. Wherefore art thou r3579x?: anonymized social networks, hidden patterns, and structural steganography. *Proceedings of the 16th international conference on World Wide Web.* Banff, Alberta, Canada: ACM.
Backstrom, L., Huttenlocher, D., Kleinberg, J. & Lan, X. 2006. Group formation in large social networks: membership, growth, and evolution. *Proceedings of the 12th ACM SIGKDD international conference on Knowledge discovery and data mining.* Philadelphia, PA, USA: ACM.
Bailey, J. L., Mitchell, R. B. & Jensen, B. K. 2008. Analysis of Student Vulnerabilities to Phishing. *In:* 14th Americas Conference on Information Systems, 14-17 August 2008 2008 Toronto Canads. Paper 271.
Bakardjieva, M. 2005. *Internet Society: The Internet in Everyday Life,* London, Sage.
Baker, D. & Fortune, S. 2008. Understanding self-harm and suicide websites - A qualitative interview study of young adult website users. *Crisis-The Journal of Crisis Intervention and Suicide Prevention,* 29,3, 118-122.
Baker, R. K. & White, K. M. 2010. Predicting adolescents' use of social networking sites from an extended theory of planned behaviour perspective. *Computers in Human Behavior,* 26,6, 1591-1597.
Balduzzi, M., Platzer, C., Holz, T., Kirda, E., Balzarotti, D. & Kruegel, C. 2010. Abusing Social Networks for Automated User Profiling. *In:* Jha, S., Sommer, R. & Kreibich, C. (eds.) *Recent Advances in Intrusion Detection.* Springer Berlin / Heidelberg.

Bandura, A. 1986. *Social foundations of thought and action : a social cognitive theory*, Englewood Cliffs ; London, Prentice-Hall.
Bandyopadhyay, K., Mykytyn, P. P. & Mykytyn, K. 1999. A framework for integrated risk management in information technology. *Management Decision*, 37,5, 437-444.
Banville, C. & Landry, M. 1989. Can the field of MIS be disciplined? *Communications of the ACM*, 32,1, 48 - 60.
Barabási, A.-L. 2003. Linked: The New Science of Networks. *American Journal of Physics*, 71,4, 409-410.
Barak, A. 2005. Sexual Harassment on the Internet. *Social Science Computer Review*, 23,1, 77-92.
Barak, A. 2007. Emotional support and suicide prevention through the Internet: A field project report. *Computers in Human Behavior*, 23,2, 971-984.
Bardone-Cone, A. M. & Cass, K. M. 2007. What does viewing a pro-anorexia website do? an experimental examination of website exposure and moderating effects. *International Journal of Eating Disorders*, 40,6, 537-548.
Barker, V. 2009. Older Adolescents' Motivations for Social Network Site Use: The Influence of Gender, Group Identity, and Collective Self-Esteem. *CyberPsychology & Behavior*, 12,2, 209-213.
Barki, H., Rivard, S. & Talbot, J. 2001. An Integrative Contingency Model of Software Project Risk Management. *Journal of Management Information Systems*, 17,4, 37-69.
Barnes, G. M. & Farrell, M. P. 1992. Parental Support and Control as Predictors of Adolescent Drinking, Delinquency, and Related Problem Behaviors. *Journal of Marriage and the Family*, 54,4, 763-776.
Barnett, E. 2011. '$100bn' Facebook; Social network site poised to become bigger than Amazon. *The Daily Telegraph* May 4, 2011 Wednesday, p.5.
Baumeister, L. M., Flores, E. & Marin, B. V. 1995. Sex information given to Latina adolescents by parents. *Health Educ. Res.*, 10,2, 233-239.
Baumrind, D. 1987. A developmental perspective on adolescent risk taking in contemporary America. *New Directions for Child and Adolescent Development*, 1987,37, 93-125.
BBC. 2008. *Stab death suspect's web message* [Online]. Available: http://news.bbc.co.uk/2/hi/uk_news/england/nottinghamshire/7637644.stm [Accessed 27th September 2008].
BBC. 2004. *Passwords revealed by sweet deal* [Online]. Available: http://news.bbc.co.uk/2/hi/technology/3639679.stm [Accessed 17th September 2008 2008].
Beatson, S., Hosty, G. S. & SmithThompson, S. 2000. Suicide and the internet. *Psychiatric Bulletin*, 24,11, 434.
Beck, K. H., Shattuck, T., Haynie, D., Crump, A. D. & Simons-Morton, B. 1999. Associations between parent awareness, monitoring, enforcement and adolescent involvement with alcohol. *Health Educ. Res.*, 14,6, 765-775.
Beck, U. 1992. *Risk society: towards a new modernity. [translated from German by Mark Ritter]*, London, Sage.
Becker, K. & Schmidt, M. 2004. Internet chat rooms and suicide. *Journal of the American Academy of Child and Adolescent Psychiatry*, 43,3, 246-247.
Beckles, C. 1997. Black Struggles in Cyberspace: Cyber-Segregation and Cyber-Nazis. *Western Journal of Black Studies*, 21,1, 12-19.
Beer, D. 2008. Social network(ing) sites... revisiting the story so far: A response to danah boyd & Nicole Ellison. *Journal of Computer-Mediated Communication*, 13,2, 516-529.

Bell, V. 2007. Online information, extreme communities and internet therapy: Is the internet good for our mental health? *Journal of Mental Health,* 16,4, 445-457.

Ben-Ari, O. T. 2004. Risk Taking in Adolescence. *In:* Greenberg, J., Koole, S. L. & Pyszczynski, T. A. (eds.) *Handbook of Experimental Existential Psychology.* New York; London: Guilford Press.

Benbasat, I. & Weber, R. 1996. Research Commentary: Rethinking "Diversity" in Information Systems Research. *Information Systems Research,* 7,4, 389-399.

Benbasat, I. & Zmud, R. W. 2003. The identity crisis within the IS discipline: Defining and communicating the discipline's core properties. *MIS Quarterly,* 27,2, 183-194.

Bener, A. B. 2000. *Risk perception, trust and credibility: A case in internet banking.* PhD, London School of Economics and Political Science.

Benson, J. K. 1983. Paradigm and praxis in organizational analysis. *In:* Cummings, L. L. & Staw, B. M. (eds.) *Research in organizational behavior.* New York: JAI Press.

Benthin, A., Slovic, P., Moran, P., Severson, H., Mertz, C. K. & Gerrard, M. 1995. Adolescent health-threatening and health-enhancing behaviors: A study of word association and imagery. *Journal of Adolescent Health,* 17,3, 143-152.

Benthin, A., Slovic, P. & Severson , H. 1993. A Psychometric study of adolescent risk perception. *Journal of Adolescence,* 16,2, 153-168.

Beran, T. & Li, Q. 2005. Cyber-harassment: a study of a new method for an old behavior. *Journal of Educational Computing Research,* 32,3, 265-277.

Bertrim, B. 2005. It's How You Play the Games. *Marketing Magazine.*

Besnard, D. & Arief, B. 2004. Computer security impaired by legitimate users. *Computers & Security,* 23,3, 253-264.

Bessière, K., Kiesler, S., Kraut, R. & Boneva, B. S. 2008. Effects of Internet Use and Social Resources on Changes in Depression. *Information, Communication & Society,* 11,1, 47 - 70.

Beyth-Marom, R., Austin, L., Fischhoff, B., Palmgren, C. & Jacobs-Quadrel, M. 1993. Perceived consequences of risky behaviors: Adults and adolescents. *Developmental Psychology,* 29,3, 549-563.

Bhatnagar, A., Misra, S. & Rao, H. R. 2000. On risk, Convenience and Internet Shopping Behaviour. *Communications of the ACM,* 43,11, 98-105.

Bhattacherjee, A. 2000. Acceptance of e-commerce services: the case of electronic brokerages. *Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on,* 30,4, 411-420.

Biddle, L., Donovan, J., Hawton, K., Kapur, N. & Gunnell, D. 2008. Suicide and the internet. *British Medical Journal,* 336,7648, 800-802.

Biglan, A. & Cody, C. 2003. Preventing Multiple Problem Behaviors in Adolescence. *In:* Romer, D. (ed.) *Reducing Adolescent Risk: Towards an Integrated Approach.* Thousand Oaks, CA: Sage Publications.

Bilge, L., Strufe, T., Balzarotti, D. & Kirda, E. 2009. All your contacts are belong to us: automated identity theft attacks on social networks. *Proceedings of the 18th international conference on World wide web.* Madrid, Spain: ACM.

Blake, S. M., Simkin, L., Ledsky, R., Perkins, C. & Calabrese, J. M. 2001. Effects of a Parent-Child Communications Intervention on Young Adolescents' Risk for Early Onset of Sexual Intercourse. *Family Planning Perspectives,* 33,2, 52-61.

Blazak, R. 2001. White Boys to Terrorist Men: Target Recruitment of Nazi Skinheads. *American Behavioral Scientist,* 44,6, 982-1000.

Boehm, B. W. 1991. Software risk management: principles and practices. *Software, IEEE,* 8,1, 32-41.

Boholm, Å. 1998. Comparative studies of risk perception: a review of twenty years of research. *Journal of Risk Research,* 1,2, 135-163.

Bonneau, J., Anderson, J. & Danezis, G. 2009. Prying Data out of a Social Network. *In:* Social Network Analysis and Mining, 2009. ASONAM '09. International Conference on Advances in, 20-22 July 2009 2009. 249-254.

Bonneau, J. & Preibusch, S. 2010. The Privacy Jungle:On the Market for Data Protection in Social Networks. *In:* Moore, T., Pym, D. & Ioannidis, C. (eds.) *Economics of Information Security and Privacy*. Springer US.

Borawski, E. A., Ievers-Landis, C. E., Lovegreen, L. D. & Trapl, E. S. 2003. Parental monitoring, negotiated unsupervised time, and parental trust: the role of perceived parenting practices in adolescent health risk behaviors. *Journal of Adolescent Health*, 33,2, 60-70.

Borzekowski, D. L. G., Schenk, S., Wilson, J. L. & Peebles, R. 2010. e-Ana and e-Mia: A Content Analysis of Pro-Eating Disorder Web Sites. *Am J Public Health*, 100,8, 1526-1534.

Bosma, H. A. & Kunnen, E. S. 2001. Determinants and Mechanisms in Ego Identity Development: A Review and Synthesis. *Developmental Review*, 21,1, 39-66.

Bostdorff, D. M. 2004. The internet rhetoric of the Ku Klux Klan: A case study in web site community building run amok. *Communication Studies*, 55,2, 340-361.

Bostrom, A., Morgan, G. M., Fischhoff, B. & Read, D. 1994. What Do People Know About Global Climate Change? 1. Mental Models. *Risk Analysis*, 14,6, 959-970.

Boverie, P. E. & Scheuffele, D. J. 1994. Multimethodological approach to examining risk-taking. *Current Psychology*, 13,4, 289 - 302.

Bowling, N. A. & Beehr, T. A. 2006. Workplace harassment from the victim's perspective: A theoretical model and meta-analysis. *Journal of Applied Psychology*, 91,5, 998-1012.

boyd, d. 2004. Friendster and publicly articulated social networking. *CHI '04 extended abstracts on Human factors in computing systems.* Vienna, Austria: ACM.

boyd, d. & Hargittai, E. 2010. Facebook privacy settings: Who cares? *First Monday (Online)*, 15,8, 23.

boyd, d. M. 2007. Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life. *In:* Buckingham, D. (ed.) *Youth, Identity, and Digital Media Volume.* Cambridge, MA: MIT Press.

boyd, d. m. & Ellison, N. B. 2007. Social Network Sites: Definition, History, and Scholarship *Journal of Computer-Mediated Communication*, 13,1, 210-230.

Boyer, T. W. 2006. The development of risk-taking: A multi-perspective review. *Developmental Review*, 26,3, 291-345.

Bradley, G. & Wildman, K. 2002. Psychosocial Predictors of Emerging Adults' Risk and Reckless Behaviors. *Journal of Youth and Adolescence*, 31,4, 253-265.

Bramwell, S. & Mussen, D. 2003. Boy text bullied to death. *Sunday Star Times*, November 30 2003, p.A1.

Brandtzæg, P. B., Lüders, M. & Skjetne, J. H. 2010. Too Many Facebook "Friends"? Content Sharing and Sociability Versus the Need for Privacy in Social Network Sites. *International Journal of Human-Computer Interaction*, 26,11, 1006 - 1030.

Brasel, A. S. & Gips, J. 2011. Media Multitasking Behavior: Concurrent Television and Computer Usage. *Cyberpsychology, Behavior, and Social Networking*, Not available-, ahead of print.

Breakwell, G. M. 1996. Risk Estimation and Sexual Behaviour. *Journal of Health Psychology*, 1,1, 79-91.

Breakwell, G. M. 2007. *The psychology of risk*, Cambridge, Cambridge University Press.

Brennan, M. & CEOP 2006. Understanding Online Social Network Services and Risks to Youth - Stakeholder Perspectives. Child Exploitation and Online Protection Centre (CEOP).

Brenner, V. 1997. Psychology of computer use: XLVII. parameters of Internet use, abuse and addiction: the first 90 days of the Internet Usage Survey. *Psychological Reports,* 80,3, 879-882.

Brewer, N. T., Chapman, G. B., Gibbons, F. X., Gerrard, M., McCaul, K. D. & Weinstein, N. D. 2007. Meta-analysis of the relationship between risk perception and health behavior: The example of vaccination. *Health Psychology,* 26,2, 136-145.

Briand, L. C., El Emam, K. & Bomarius, F. 1998. COBRA: A Hybrid Method for Software Cost Estimation, Bechmarking, and Risk Assessment. *In:* 20th International Conference on Software Engineering (ICSE'98), 1998 Kyoto, Japan. IEEE Computer Society, 390.

Brockhaus, R. H. 1975. I-E Locus of Control Scores as Predictors of Entrepreneurial Intentions. *Academy of Management Proceedings*, 433-435.

Bronfenbrenner, U. 1979. *The ecology of human development : experiments by nature and design,* Cambridge, Mass., Harvard University Press.

Buchanan, T. 2000. Potential of the Internet for Personality Research. *In:* Birnbaum, M. H. (ed.) *Psychological Experiments on the Internet.* San Diego, CA: Academic Press.

Buchanan, T., Paine, C., Joinson, A. N. & Reips, U.-D. 2007. Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology,* 58,2, 157-165.

Burgoon, J. K., Parrott, R., Le Poire, B. A., Kelley, D. L., Walther, J. B. & Perry, D. 1989. Maintaining and Restoring Privacy through Communication in Different Types of Relationships. *Journal of Social and Personal Relationships,* 6,2, 131-158.

Burns, W. J., Slovic, P., Kasperson, R., Kasperson, J., Renn, O. & Emani, S. 1993. Incorporating Structural Models into Research on the Social Amplification of Risk: Implications for Theory Construction and Decision Making. *Risk Analysis*, 13,6, 611-624.

Burrell, G. & Morgan, G. 1979. *Sociological Paradigms and Organisational Analysis,* London, Heinemann Books.

Burt, R. S. 1987. Social Contagion and Innovation: Cohesion Versus Structural Equivalence. *The American Journal of Sociology,* 92,6, 1287-1335.

Bynner, J. 2005. Rethinking the Youth Phase of the Life-course: The Case for Emerging Adulthood? *Journal of Youth Studies,* 8,4, 367-384.

Byrne, D. N. 2008. The Future of (the) 'Race': Identity, Discourse, and the Rise of Computer-mediated Public Spheres. *In:* Everett, A. (ed.) *Learning Race and Ethnicity: Youth and Digital Media.* Cambridge, MA: The MIT Press.

Byrnes, J. P. 2003. Changing Views on the Nature and Prevention of Adolescent Risk Taking. *In:* Romer, D. (ed.) *Reducing Adolescent Risk: Towards an Integrated Approach.* Thousand Oaks, CA: Sage Publications.

Byrnes, J. P., Miller, D. C. & Schafer, W. D. 1999. Gender differences in risk taking: A meta-analysis. *Psychological Bulletin,* 125,3, 367-383.

Calder, A. 2006. *Information Security based on ISO 27001/ISO 17799, A Management Guide,* Zaltbommel, Van Haren Publishing.

Campbell, D. T. & Fiske, D. W. 1959. Convergent and discriminant validation by the multitrait-multimethod matrix. *Psychological Bulletin,* 56,2, 81-105.

Campbell, J., Greenauer, N., Macaluso, K. & End, C. 2007. Unrealistic optimism in internet events. *Computers in Human Behavior,* 23,3, 1273-1284.

Cannell, C. & Kahn, R. 1968. Interviewing. *In:* Lindzey, G. & Aronson, E. (eds.) *The Handbook of Social Psychology.* Reading MA: Addison-Wesley.

Cao, F. & Su, L. 2007. Internet addiction among Chinese adolescents: prevalence and psychological features. *Child: Care, Health & Development,* 33,3, 275-281.

Carlsson, S. A. 2003. Advancing Information Systems Evaluation (Research): A Critical Realist Approach. *Electronic Journal of Information Systems Evaluation,* 6,2, 11-20.

Carlstrom, L. K., Woodward, J. A. & Palmer, C. G. S. 2000. Evaluating the Simplified Conjoint Expected Risk Model: Comparing the Use of Objective and Subjective Information. *Risk Analysis,* 20,3, 385-392.

Carter, H. 2011. Juror jailed for internet chats with defendant. *The Guardian*, June 17, 2011 Friday, p.6.

Cauffman, E. & Steinberg, L. 2000. (Im)maturity of judgment in adolescence: why adolescents may be less culpable than adults. *Behavioral Sciences & the Law,* 18,6, 741-760.

Cecez-Kecmanovic, D., Klein, H. K. & Brooke, C. 2008. Exploring the critical agenda in information systems research. *Information Systems Journal,* 18,2, 123-135.

Ceyhan, A. A. 2008. Predictors of Problematic Internet Use on Turkish University Students. *CyberPsychology & Behavior,* 11,3, 363-366.

Charlton, J. P. 2002. A factor-analytic investigation of computer 'addiction' and engagement. *British Journal of Psychology,* 93,3, 329.

Chassin, L., Pitts, S. C. & Prost, J. 2002. Binge drinking trajectories from adolescence to emerging adulthood in a high-risk sample: Predictors and substance abuse outcomes. *Journal of Consulting and Clinical Psychology,* 70,1, 67-78.

Chassin, L., Presson, C. & Sherman, S. 1989. "Constructive" vs. "Destructive" deviance in adolescent health-related behaviors. *Journal of Youth and Adolescence,* 18,3, 245-262.

Chau, D. H., Pandit, S., Wang, S. & Faloutsos, C. 2007. Parallel crawling for online social networks. *Proceedings of the 16th international conference on World Wide Web.* Banff, Alberta, Canada: ACM.

Chellappa, R. K. & Sin, R. G. 2005. Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma. *Information Technology and Management,* 6,2, 181-202.

Chen, W. & Hirschheim, R. 2004. A paradigmatic and methodological examination of information systems research from 1991 to 2001. *Information Systems Journal,* 14,3, 197-235.

Chesley, E. B., Alberts, J. D., Klein, J. D. & Kreipe, R. E. 2003. Pro or con? Anorexia nervosa and the internet. *Journal of Adolescent Health,* 32,2, 123-124.

Chou, C., Condron, L. & Belland, J. C. 2005. A Review of the Research on Internet Addiction. *Educational Psychology Review,* 17,4, 363-388.

Chou, C. & Hsiao, M.-C. 2000. Internet addiction, usage, gratification, and pleasure experience: the Taiwan college students' case. *Computers & Education,* 35,1, 65-80.

Christian, L. M., Dillman, D. A. & Smyth, J. D. 2007. Helping Respondents Get It Right the First Time: The Influence of Words, Symbols, and Graphics in Web Surveys. *Public Opin Q,* nfl039.

Christian, L. M., Parsons, N. L. & Dillman, D. A. 2009. Designing Scalar Questions for Web Surveys. *Sociological Methods & Research,* 393-425.

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

Chua, W. F. 1986. Radical Developments in Accounting Thought. *The Accounting Review,* 61,4, 601.

Ciborra, C. 2001. *From control to drift: the dynamic of corporate information infrastructures,* Oxford, Oxford University Press.

Cohen, L., Manion, L. & Morrison, K. 2007. *Research methods in education,* London, Routledge.
Cohen, N. S. & Shade, L. R. 2008. Gendering Facebook: Privacy and commodification. *Feminist Media Studies,* 8,2, 210-214.
Cohen, P., Kasen, S., Chen, H., Hartmark, C. & Gordon, K. 2003. Variations in patterns of developmental transmissions in the emerging adulthood period. *Developmental Psychology,* 39,4, 657-669.
Cohn, L. D., Macfarlane, S., Yanez, C. & Imai, W. K. 1995. Risk-perception: Differences between adolescents and adults. *Health Psychology,* 14,3, 217-222.
Coles, R. & Hodgkinson, G. P. 2008. A Psychometric Study of Information Technology Risks in the Workplace. *Risk Analysis,* 28,1, 81-93.
Collin, B. 1997. The Future of Cyberterrorism. *Crime and Justice International,* 13,2, 15-18.
Collins, B. & Mansell, R. 2004. Cyber Trust and Crime Prevention: A Synthesis of the State-of-the-Art Science Reviews. *Foresight Cyber Trust and Crime Prevention Project.* UK Office of Science and Technology.
Comte, A. 1875. The positive philosophy. *In:* Thompson, K. & Tunstall, J. (eds.) *Sociological Perspectives.* Harmondworth: Penguin.
Connolly, R. & Bannister, F. 2007. Consumer trust in Internet shopping in Ireland: Towards the development of a more effective trust measurement instrument. *Journal of Information Technology,* 22,2, 102-118.
Conti, G. & Sobiesk, E. 2007. An honest man has nothing to fear: user perceptions on web-based information disclosure. *Proceedings of the 3rd symposium on Usable privacy and security.* Pittsburgh, Pennsylvania: ACM.
Conway, L. 2008. Virgin Atlantic sacks 13 staff for calling its flyers 'chavs'; Facebook blog insulted passengers and claimed aircraft had cockroaches (London) *The Independent,* November 1, 2008, p.10.
Conway, M. 2006. Terrorism and the Internet: New Media-New Threat? *Parliamentary Affairs,* 59,2, 283-298.
Correa, T., Hinsley, A. W. & de Zúñiga, H. G. 2010. Who interacts on the Web?: The intersection of users' personality and social media use. *Computers in Human Behavior,* 26,2, 247-253.
Cosoi, C. 2011. The evolving threat of social media. *Computer Fraud & Security,* 2011,6, 14-16.
Costa, P. T. & McCrae, R. R. 1992. *Revised NEO Personality Inventory (NEOPI-R) and NEO Five-Factor Inventory (NEO-FFI) Professional Manual.,* Odessa, FL, Psychological Assessment Resources.
Couper, M. P. 2008. *Designing effective Web surveys,* Cambridge, Cambridge University Press.
Cox, D. F. 1967. *Risk Taking and Information Handling in Consumer Behavior,* Boston, MA, Harvard University Press.
Cox, D. F. & Rich, S. U. 1964. Perceived Risk and Consumer Decision-Making - The Case of the Telephone Shopping. *Journal of Marketing Research (JMR),* 1,4, 32-39.
Cox, P., Niewöhner, J., Pidgeon, N., Gerrard, S., Fischhoff, B. & Riley, D. 2003. The Use of Mental Models in Chemical Risk Protection: Developing a Generic Workplace Methodology. *Risk Analysis,* 23,2, 311-324.
Cox_Communications 2009. Teen online & wireless safety survey: Cyberbullying, sexting and parental controls. Atlanta GA: Cox Communications - in Partnership with the National Center for Missing & Exploited Children® (NCMEC) and John Walsh.
Cranor, L. F. 2008. A Framework for Reasoning About the Human in the Loop. Carnegie Mellon CyLab.

Cranor, L. F., Reagle, J. & Ackerman, M. S. 2000. Beyond Concern: Understanding Net Users' Attitudes about Online Privacy. *In:* Vogelsang, I. & Compaine, B. M. (eds.) *The Internet Upheaval: Raising Questions, Seeking Answers in Communications Policy.* Cambridge MA: MIT Press.

Creswell, J. W. 2009. *Research Design: Qualitative, Quantitative and Mixed Methods Approaches,* Thousand Oaks, CA, Sage.

Creswell, J. W. & Miller, D. L. 2000. Determining Validity in Qualitative Inquiry. *Theory Into Practice,* 39,3, 124 - 130.

Creswell, J. W. & Plano Clark, V. L. 2007. *Designing and Conducting Mixed Methods Research,* Thousand Oaks, CA, Sage.

Creswell, J. W., Plano Clark, V. L., Guttman, M. L. & Hanson, W. E. 2003. Advanced mixed methods research designs. *In:* Tashakkori, A. & Teddlie, C. (eds.) *Handbook of mixed methods in social and behavioral research.* Thousand Oaks, CA: Sage.

Csipke, E. & Horne, O. 2007. Pro-eating disorder websites: users' opinions. *European Eating Disorders Review,* 15,3, 196-206.

Culnan, M. & Armstrong, P. K. 1999. Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science,* 10,1, 104-115.

Cummings, J. N., Sproull, L. & Kiesler, S. B. 2002. Beyond hearing: Where the real-world and online support meet. *Group Dynamics: Theory, Research, and Practice,* 6,1, 78-88.

Cunningham, S. M. 1967. The Major Dimensions of Perceived Risk. *In:* Cox, D. F. (ed.) *Risk Taking and Information Handling in Consumer Behavior.* Boston: Harvard University Press.

Curry, L. A. & Youngblade, L. M. 2006. Negative affect, risk perception, and adolescent risk behavior. *Journal of Applied Developmental Psychology,* 27,5, 468-485.

D'Ovidio, R. & Doyle, J. 2003. A Study on Cyberstalking Understanding Investigative Hurdles. *FBI Law Enforcement Bulletin,* 72,3, 10-17.

Dake, K. 1991. Orienting Dispositions in the Perception of Risk, An Analysis of Contemporary Worldviews and Cultural Biases. *Journal of Cross-Cultural Psychology,* 22,1, 61-82.

Datcu, S. 2010. Social Networking and the Illusion of Anonymity. *Privacy Experiments Series.* BitDefender.

Davies, A. R. 1999. Where do we go from here? Environmental focus groups and planning policy formation. *Local Environment,* 4,3, 295.

Davis, C. & Bauserman, R. 1993. Exposure to sexually explicit materials: An attitude change perspective. *Annual Review of Sex Research,* 4,4, 121-209.

Davis, F. D. 1989a. Perceived Usefulness, Perceived Ease Of Use, And User Accep. *MIS Quarterly,* 13,3, 319.

Davis, F. D. 1989b. Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly,* 13,3, 319-340.

Davison, K. P., Pennebaker, J. W. & Dickerson, S. S. 2000. Who talks? The social psychology of illness support groups. *American Psychologist,* 55,2, 205-217.

Davison, W. P. 1983. The Third-Person Effect in Communication. *Public Opinion Quarterly,* 47,1, 1-15.

de Leeuw, E. D., Hox, J. J. & Dillman, D. A. (eds.) 2008. *International handbook of survey methodology,* London: Taylor & Francis Group.

De Souza, Z. & Dick, G. N. 2009. Disclosure of information by children in social networking--Not just a case of "you show me yours and I'll show you mine". *International Journal of Information Management,* 29,4, 255-261.

Debatin, B., Lovejoy, J. P., Horn, A.-K. & Hughes, B. N. 2009. Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences. *Journal of Computer-Mediated Communication,* 15,1, 83-108.

Deboelpaep, R. & EPTA 2006. Cyberbullying among youngsters in Flanders. EPTA European Parliamentary Technology Assessment.

DeCew, J. W. 1997. *In pursuit of privacy : law, ethics, and the rise of technology,* Ithaca, N.Y. ; London Cornell University Press.

Dehue, F., Bolman, C. & Völlink, T. 2008. Cyberbullying: Youngsters' Experiences and Parental Perception. *CyberPsychology & Behavior,* 11,2, 217-223.

Denning, D. E. 1999. *Information Warfare and Security,* Addison Wesley.

Denning, D. E. 2001. Activism, Hacktivism and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. *In:* Arquilla, J. & Ronfeldt, D. F. (eds.) *Networks and Netwars: The Future of Terror, Crime, and Militancy.* Santa Monica, CA: Rand Corporation.

Denzin, N. K. 1970. *The research act in sociology : a theoretical introduction to sociological methods* London, Butterworths.

Desjarlais, M. & Willoughby, T. 2010. A longitudinal study of the relation between adolescent boys and girls' computer use with friends and friendship quality: Support for the social compensation or the rich-get-richer hypothesis? *Computers in Human Behavior,* 26,5, 896-905.

Devine, D., Long, P. & Forehand, R. 1993. A prospective study of adolescent sexual activity: Description, correlates, and predictors. *Advances in Behaviour Research and Therapy,* 15,3, 185-209.

Dewispelare, A. R., Herren, L. T. & Clemen, R. T. 1995. The use of probability elicitation in the high-level nuclear waste regulation program. *International Journal of Forecasting,* 11,1, 5-24.

DiClemente, R. J., Hansen, W. B. & Ponton, L. E. (eds.) 1996. *Handbook of Adolescent Health Risk Behavior,* New York: Plenum.

Dillman, D. A., Smyth, J. D. & Christian, L. M. 2009. *Internet, Mail and Mixed-Mode Surveys, The Tailored Design Method,* Hoboken, New Jersey, John Wiley and Sons Inc.

Dinev, T. & Hart, P. 2004. Internet privacy concerns and their antecedents - measurement validity and a regression model. *Behaviour & Information Technology,* 23,6, 413-422.

Dishion, T. J. & McMahon, R. J. 1998. Parental Monitoring and the Prevention of Child and Adolescent Problem Behavior: A Conceptual and Empirical Formulation. *Clinical Child & Family Psychology Review,* 1,1, 61-75.

Dominos_Pizza. Jan 25, 2007. *Domino's Revealed as Creator of Popular Internet Videos* [Online]. Press Release. Available: http://www.prnewswire.com/cgi-bin/stories.pl?ACCT=109&STORY=/www/story/01-25-2007/0004512862&EDATE= [Accessed 18/08/2008].

Donath, J. 2008. Signals in Social Supernets. *Journal of Computer-Mediated Communication,* 13,1, 231-251.

Donath, J. & boyd, d. 2004. Public Displays of Connection. *BT Technology Journal,* 22,4, 71.

Donohew, L., Zimmerman, R., Cupp, P. S., Novak, S., Colon, S. & Abell, R. 2000. Sensation seeking, impulsive decision-making, and risky sex: implications for risk-taking and design of interventions. *Personality and Individual Differences,* 28,6, 1079-1091.

Donovan, J. E., Jessor, R. & Costa, F. M. 1988. Syndrome of problem behavior in adolescence: A replication. *Journal of Consulting and Clinical Psychology,* 56,5, 762-765.

Dorogovtsev, S. N. & Mendes, J. F. F. 2002. Evaluation of networks. *Advances in Physics,* 51,4, 1079-1188

Douglas, K. M. 2007. Psychology, discrimination and hate groups online. *In:* Joinson, A. N., Mckenna, K., Reips, U.-D. & Postmes, T. (eds.) *Oxford handbook of Internet Psychology.* Oxford: Oxford University Press.

Douglas, K. M., Mcgarty, C., Bliuc, A.-M. & Lala, G. 2005. Understanding Cyberhate. *Social Science Computer Review,* 23,1, 68-76.

Douglas, M. 2003. Risk and blame: essays in cultural theory. *Mary Douglas collected works.* London: Routledge.

Douglas, M. & Wildavsky, A. 1982. *Risk and culture : an essay on the selection of technical and environmental dangers* Berkeley, University of California Press.

Douglass, C. B. 2005. *Barren states : the population "implosion" in Europe,* Oxford; New York, N.Y., Berg.

Dourish, P., Grinter, R. E., Delgado de la Flor, J. & Joseph, M. 2004. Security in the wild: user strategies for managing security as an everyday, practical problem *Personal and Ubiquitous Computing,* 8,6, 391-401.

Dowland, P. S., Furnell, S. M., Illingworth, H. M. & Reynolds, P. L. 1999. Computer crime and abuse: A survey of public attitudes and awareness. *Computers & Security,* 18,8, 715-726.

Draper, E. 1993. Review: Risk, Society and Social Theory. *Contemporary Sociology,* 22,5, 641-644.

Driscoll, C. 2008. This is not a Blog: Gender, intimacy, and community. *Feminist Media Studies,* 8,2, 198-212.

Dwyer, C. 2007. Digital Relationships in the "MySpace" Generation: Results From a Qualitative Study. *In:* 40th Annual Hawaii International Conference on System Sciences (HICSS'07), 2007 Hawaii. 19c.

Dwyer, C., Hiltz, S. R. & Passerini, K. 2007. Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. *In:* Americas Conference on Information Systems (AMCIS),, August 09-12, 2007 2007 Keystone, Colorado, USA.

Earp, J. B. & Baumer, D. 2003. Innovative Web Use to Learn About Consumer Behaviour and Online Privacy. *Communications of the ACM,* 46,4, 81-83.

Easterby-Smith, M., Thorpe, R. & Lowe, A. 2002. *Management Research: An Introduction,* Sage.

Einarsen, S. & Skogstad, A. 1996. Bullying at work: Epidemiological findings in public and private organizations. *European Journal of Work and Organizational Psychology,* 5,2, 185 - 201.

Eiser, J. R. 2004. Public Perceptions of Risk. *Foresight Review.* Report prepared for Foresight Office of Science and Technology.

Elkind, D. 1967. Egocentrism in adolescence. *Child Dev,* 38,4, 1025-34.

Elliot, S. & Avison, D. 2005. Discipline of Information Systems. *In:* Avison, D. & Pries-Heje, J. (eds.) *Research in information systems.* Oxford: Butterworth-Heinemann.

Ellison, L. & Akdeniz, Y. 1998. Cyber-stalking: the Regulation of Harassment on the Internet. *Criminal Law Review, December Special Edition: Crime, Criminal Justice and the Internet,* 29-48.

Ellison, N. B., Lampe, C. & Steinfield, C. 2009. Social network sites and society: current trends and future possibilities. *interactions,* 16,1, 6-9.

Ellison, N. B., Steinfield, C. & Lampe, C. 2007. The Benefits of Facebook "Friends:" Social Capital and College Students' Use of Online Social Network Sites. *Journal of Computer-Mediated Communication,* 12,4, 1143 - 1492.

Elmer-Dewitt, P., Cole, W. & Quittner, J. 1995. On a screen near you: Cyberporn. *Time,* 146,1, 38.

Engländer, T., Farago, K., Slovic, P. & Fischhoff, B. 1986. A comparative analysis of risk perception in Hungary and the United States. *Social Behaviour,* 1,1, 55-66.
Erdur-Baker, Ö. 2010. Cyberbullying and its correlation to traditional bullying, gender and frequent and risky usage of internet-mediated communication tools. *New Media & Society,* 12,1, 109-125.
Erikson, E. H. 1968. *Identity: youth and crisis,* London, Faber and Faber Ltd.
Ernst&Young 2010. 13th Annual Global Information Security Survey - Borderless Security. Ernst & Young.
EU 2009. Safer Social Networking Principles for the EU.
EUROBAROMETER 2007a. Safer Internet for Children, Qualitative Study in 29 European Countries - National Analysis:Ireland. EUROPEAN COMMISSION - Directorate-General Information Society and Media.
EUROBAROMETER 2007b. Safer Internet for Children, Qualitative Study in 29 European Countries - Summary Report. EUROPEAN COMMISSION - Directorate-General Information Society and Media.
EUROBAROMETER 2011. Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union. Conducted by TNS Opinion & Social at the request of Directorate-General Justice, Information Society & Media and Joint Research Centre.
Eysenbach, G. & Köhler, C. 2002. How do consumers search for and appraise health information on the world wide web? Qualitative study using focus groups, usability tests, and in-depth interviews. *British Medical Journal,* 324,7337, 573-577.
Facebook. 2011. *Facebook's Privacy Policy* [Online]. Available: http://www.new.facebook.com/home.php#/policy.php?ref=pf [Accessed 16th June 2011].
Fay, B. 1987. An Alternative View: Interpretive Social Science. *In:* Gibbons, M. T. (ed.) *Interpreting Politics.* New York: New York University Press.
Featherman, M. S. & Pavlou, P. A. 2003. Predicting e-services adoption: a perceived risk facets perspective. *International Journal of Human-Computer Studies,* 59,4, 451-474.
Fenton-O'Creevy, M., Nicholson, N., Soane, E. & Willman, P. 2003. Trading on illusions: Unrealistic perceptions of control and trading performance. *Journal of Occupational and Organizational Psychology,* 76,1, 53-68.
Fine, J. 2009. OfficeMax's Wacky Marketing Strategy. January 29, 2009.
Finucane, M., Alhakami, A. S., Slovic, P. & Johnson, S. M. 1999. The affect heuristic in judgements of risks and benefits. *Journal of Behavioral Decision Making,* 13,1, 1-17.
Finucane, M. L., Slovic, P., Mertz, C. K., Flynn, J. & Satterfield, T. A. 2000. Gender, race, and perceived risk: the 'white male' effect. *Health, Risk & Society,* 2,2, 159-172.
Fischhoff, B., Slovic, P. & Lichtenstein, S. 1979. Weighing the Risks: Which Risks Are Acceptable? *Environment,* 2,4, 17-20, 32-38.
Fischhoff, B., Slovic, P. & Lichtenstein, S. 1982. Lay Foibles and Expert Fables in Judgments about Risk. *The American Statistician,* 36,No. 3, Part 2: Proceedings of the Sixth Symposium on Statistics and the Environment., 240-255.
Fischhoff, B., Slovic, P., Lichtenstein, S., Read, S. & Combs, B. 1978. How Safe is Safe Enough? A Psychometric Study of Attitudes Toward Technological Risks and Benefits. *Policy Sciences,* 9, 127-52.
Fishbein, M. & Ajzen, I. 1975. *Belief, attitude, intention and behavior : an introduction to theory and research,* Reading, Mass. ; London [etc.], Addison-Wesley.
Fletcher, D. 2010. How Facebook is Redefining Privacy. *Time Magazine.* Time Inc.
Flick, U. 2006. *An introduction to qualitative research,* London, SAGE.

Flood, M. 2007. Exposure to pornography among youth in Australia. *Journal of Sociology,* 43,1, 45-60.
Flynn, J., Burns, W. J., Mertz, C. K. & Slovic, P. 1992. Trust as a Determinant of Opposition to a High-Level Radioactive Waste Repository: Analysis of a Structural Model. *Risk Analysis,* 12,3, 417-429.
Flynn, J., Slovic, P. & Mertz, C. K. 1994. Gender, Race, and Perception of Environmental Health Risks. *Risk Analysis,* 14,6, 1101-1108.
Fogel, J. & Nehmad, E. 2009. Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior,* 25,1, 153-160.
Fogg, B. J. 2008. Mass interpersonal persuasion: An early view of a new phenomenon. *In:* Third International Conference on Persuasive Technology, Persuasive 2008, 2008 Berlin. Springer.
Fontana, A. & Frey, J. H. 1994. Interviewing: The art of science. *In:* Denzin, N. K. & Lincoln, Y. S. (eds.) *Handbook of qualitative research.* Thousand Oaks, CA, US: Sage Publications.
Fontevecchia, A. 2011. Zynga Reveals Profit And Revenues As It Looks To Raise $500 Million. *Moral Hazard* [Online]. Available from: http://blogs.forbes.com/afontevecchia/2011/03/02/zynga-reveals-profit-and-revenues-as-it-looks-to-raise-500-million/ [Accessed 23 June 2011].
Forlani, D. & Mullins, J. W. 2000. Perceived risks and choices in entrepreneurs' new venture decisions *Journal of Business Venturing,* 15,4, 305-322
Forsythe, S. M. & Shi, B. 2003. Consumer patronage and risk perceptions in Internet shopping. *Journal of Business Research,* 56,11, 867-875.
Fox, N., Ward, K. & O'Rourke, A. 2005. Pro-anorexia, weight-loss drugs and the internet: an 'anti-recovery' explanatory model of anorexia. *Sociology of Health & Illness,* 27,7, 944-971.
Fox, S. & Sydnes, J. 2009. The social life of health information. Washington, DC: Pew Internet and American Life Project.
Frankfort-Nachmias, C. & Nachmias, D. 1996. *Research methods in the social sciences,* London, Edward Arnold.
Frewer, L. J., Howard, C. & Shepherd, R. 1998. Understanding public attitudes to technology. *Journal of Risk Research,* 1,3, 221-235.
Furby, L. & Beyth-Marom, R. 1992. Risk taking in adolescence: A decision-making perspective. *Developmental Review,* 12,1, 1-44.
Furby, L., Slovic, P., Fischhoff, B. & Gregory, R. 1988. Public perceptions of electric power transmission lines. *Journal of Environmental Psychology,* 8,1, 19-43.
Furnell, S. & Botha, R. A. 2011. Social networks - access all areas? *Computer Fraud & Security,* 2011,5, 14-19.
Furnell, S. M., Bryant, P. & Phippen, A. D. 2007. Assessing the security perceptions of personal Internet users. *Computers & Security,* 26,5, 410-417.
Furnell, S. M. & Warren, M. J. 1999. Computer hacking and cyber terrorism: the real threats in the new millennium? *Computers & Security,* 18,1, 28-34.
Gabriel, I. J. & Nyshadham, E. 2008. A Cognitive Map of People's Online Risk Perceptions and Attitudes: An Empirical Study. *In:* Hawaii International Conference on System Sciences, Proceedings of the 41st Annual, 2008. 274-274.
Gafford, J. 2007. *Guerilla Marketing on Myspace: Smart Do-it-yourself Online Marketing* [Online]. Available: http://www.articlesbase.com/marketing-articles/guerilla-marketing-on-myspace-smart-doityourself-online-marketing-100878.html [Accessed 17th September 2008].
Gajjala, R. 2007. Shifting Frames: Race, Ethnicity and Intercultural Communication in Online Social Networking and Virtual Work. *In:* Hinner, M. B. (ed.) *The Role of*

Communication in Business Transactions and Relationships. New York: Peter Lang.

Galliers, R. D. 1992. Choosing Information Systems Research Approaches. *In:* Galliers, R. D. (ed.) *Information Systems Research: Issues, Methods and Practical Guidelines.* Oxford: Blackwell Scientific Publications.

Galliers, R. D. 2003. Change as Crisis or Growth? Toward a Trans-disciplinary View of Information Systems as a Field of Study: A Response to Benbasat and Zmud's Call for Returning to the IT Artifact. *Journal of the Association for Information Systems,* 4, 337-351.

Galliers, R. D. & Meadows, M. 2003. A Discipline Divided: Globalization and Parochialism in Information Systems Research. *Communications of AIS,* 2003,11, 108-116.

Ganzach, Y. 2000. Judging Risk and Return of Financial Assets. *Organizational Behavior and Human Decision Processes,* 83,2, 353-370.

Gardner, M. & Steinberg, L. 2005. Peer Influence on Risk Taking, Risk Preference, and Risky Decision Making in Adolescence and Adulthood: An Experimental Study. *Developmental Psychology,* 41,4, 625-635.

Gefen, D. 2000. E-Commerce: the role of familiarity and trust. *Omega: The International Journal of Management Science,* 28,6, 725-737.

Gefen, D., Srinivasan Rao, V. & Tractinsky, N. 2003. The conceptualization of trust, risk and their electronic commerce: the need for clarifications. *In:* 36th Annual Hawaii International Conference on Systems Sciences (HICSS '03), 6-9 Jan. 2003 2003 Hawaii. 10.

Geidner, N., Flook, C. & Bell, M. 2007. Masculinity and online social networks: Male self-identification on Facebook. com. *Eastern Communication Association 98th Annual Meeting.* Providence RI.

Gerber, M. & von Solms, R. 2001. From Risk Analysis to Security Requirements. *Computers & Security,* 20,7, 577-584.

Gerber, M. & von Solms, R. 2005. Management of risk in the information age. *Computers & Security,* 24,1, 16-30.

Gerrard, M., Gibbons, F. X., Benthin, A. C. & Hessling, R. M. 1996a. A longitudinal study of the reciprocal nature of risk behaviors and cognitions in adolescents: What you do shapes what you think, and vice versa. *Health Psychology,* 15,5, 344-354.

Gerrard, M., Gibbons, F. X. & Bushman, B. J. 1996b. Relation between perceived vulnerability to HIV and precautionary sexual behavior. *Psychological Bulletin,* 119,3, 390-409.

Gerstenfeld, P. B., Grant, D. R. & Chiang, C.-P. 2003. Hate Online: A Content Analysis of Extremist Internet Sites. *Analyses of Social Issues and Public Policy,* 3,1, 29-44.

Gibson, F. 2007. Conducting focus groups with children and young people: strategies for success. *Journal of Research in Nursing,* 12,5, 473-483.

Giddens, A. 1991. *Modernity and Self-Identity,* Polity Press.

Gigerenzer, G., Hertwig, R., van den Broek, E., Fasolo, B. & Katsikopoulus, K. V. 2005. "A 30% Chance of Rain Tomorrow": How Does the Public Understand Probabilistic Weather Forecasts? *Risk Analysis,* 25,3, 623-629.

Gladwell, M. 2010. Small Change, Why the revolution will not be tweeted. *New Yorker Magazine.* New York: Conde Nast.

Glaser, B. G. & Strauss, A. L. 1967. *The Discovery of Grounded Theory; Strategies for Qualitative Research.,* New York, Aldine Publishing.

Goffman, E. 1959. *The Presentation of Self in Everyday Life,* New York, Doubleday.

Goldberg, J. & Fischhoff, B. 2000. The long-term risks in the short-term benefits: Perceptions of potentially addictive activities. *Health Psychology,* 19,3, 299-303.

Goldberg, J. H., Halpern-Felsher, B. L. & Millstein, S. G. 2002. Beyond invulnerability: The importance of benefits in adolescents' decision to drink alcohol. *Health Psychology,* 21,5, 477-484.

Goldstein, S. B., Dudley, E. A., Erickson, C. M. & Richer, N. L. 2002. Personality traits and computer anxiety as predictors of Y2K anxiety. *Computers in Human Behavior,* 18,3, 271-284.

Goles, T. & Hirschheim, R. 2000. The paradigm is dead, the paradigm is dead...long live the paradigm: the legacy of Burrell and Morgan. *Omega,* 28,3, 249-268.

Gonzalez, J. J. & Sawicka, A. 2002. A Framework for Human Factors in Information Security. *WSEAS International Conference on Information Security, Rio de Janeiro, 2002.* Brazil: WSEAS.

Goodings, L., Locke, A. & Brown, S. D. 2007. Social networking technology: place and identity in mediated communities. *Journal of Community & Applied Social Psychology,* 17,6, 463-476.

Goodman, S. E., Kirk, J. C. & Kirk, M. H. 2007. Cyberspace as a medium for terrorists. *Technological Forecasting and Social Change,* 74,2, 193-210.

Gorzig, A. 2011. Who bullies and who is bullied online? LSE, London: EU Kids Online.

Gosling, S. D., Gaddis, S. & Vazire, S. 2007. Personality Impressions Based on Facebook Profiles. *In:* International Conference on Weblogs and Social Media, March 26-28, 2007 2007 Boulder, Colorado, USA.

Gosling, S. D., Vazire, S., Srivastava, S. & John, O. P. 2004. Should We Trust Web-Based Studies? A Comparative Analysis of Six Preconceptions About Internet Questionnaires. *American Psychologist,* 59,2, 93-104.

Gould, M., Jamieson, P. & Romer, D. 2003. Media Contagion and Suicide Among the Young. *American Behavioral Scientist,* 46,9, 1269-1284.

Gould, M. S., Munfakh, J. L. H., Lubell, K., Kleinman, M. & Parker, S. 2002. Seeking Help From the Internet During Adolescence. *Journal of Amer Academy of Child & Adolescent Psychiatry,* 41,10, 1182-1189.

Grabner-Kräuter, S. & Kaluscha, E. A. 2003. Empirical research in on-line trust: a review and critical assessment. *International Journal of Human-Computer Studies,* 58,6, 783-812.

Granovetter, M. S. 1973. The Strength of Weak Ties. *The American Journal of Sociology,* 78,6, 1360-1380.

Granovetter, M. S. 1983. The Strength of Weak Ties: A Network Theory Revisited. *Sociological Theory,* 1, 201-233.

Grazioli, S. & Jarvenpaa, S. L. 2000. Perils of Internet fraud: an empirical investigation of deception and trust with experienced Internet consumers. *Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on,* 30,4, 395-410.

Greenberger, E., Josselson, R., Knerr, C. & Knerr, B. 1975. The measurement and structure of psychosocial maturity. *Journal of Youth and Adolescence,* 4,2, 127-143.

Greene, J. C. & Caracelli, V. J. 2003. Making paradigmatic sense of mixed-method practice. *In:* Tashakkori, A. & Teddlie, C. (eds.) *Handbook of mixed methods in social and behavioral research.* Thousand Oaks, CA: Sage.

Greene, J. C., Caracelli, V. J. & Graham, W. F. 1989. Toward a Conceptual Framework for Mixed-Method Evaluation Designs. *Educational Evaluation and Policy Analysis,* 11,3, 255-274.

Greene, K., Krcmar, M., Walters, L. H., Rubin, D. L., Jerold & Hale, L. 2000. Targeting adolescent risk-taking behaviors: the contributions of egocentrism and sensation-seeking. *Journal of Adolescence,* 23,4, 439-461.

Greenfield, D. N. 1999. Psychological Characteristics of Compulsive Internet Use: A Preliminary Analysis. *CyberPsychology & Behavior,* 2,5, 403-412.

Griffiths, M. 1998. Internet addiction: Does it really exist? *In:* Gackenbach, J. (ed.) *Psychology and the internet: Intrapersonal, interpersonal and transpersonal applications.* New York: Academic Press.

Griffiths, M. 2000a. Does Internet and Computer "Addiction" Exist? Some Case Study Evidence. *CyberPsychology & Behavior,* 3,2, 211-218.

Griffiths, M. 2000b. Excessive Internet Use: Implications for Sexual Behavior. *CyberPsychology & Behavior,* 3,4, 537-552.

Griffiths, M. 2000c. Internet Addiction - Time to be Taken Seriously? *Addiction Research,* 8,5, 413-418.

Gross, E. F. 2004. Adolescent Internet use: What we expect, what teens report. *Journal of Applied Developmental Psychology,* 25,6, 633-649.

Gross, E. F., Juvonen, J. & Gable, S. L. 2002. Internet Use and Well-Being in Adolescence. *Journal of Social Issues,* 58,1, 75.

Gross, R. & Acquisti, A. 2005. Information Revelation and Privacy in Online Social Networks. *ACM Workshop on Privacy in the Electronic Society (WPES).* Alexandria, Virginia,: ACM.

Grossman, L. 2006. Time's Person of the Year: You. *Time Magazine.* Time Inc.

Groves, R. M., Fowler, F. J. J., Couper, M. P., Lepkowski, J. M., Singer, E. & Tourangeau, R. 2004. *Survey methodology,* Hoboken, NJ, J. Wiley.

Guadagno, R. E., Okdie, B. M. & Eno, C. A. 2008. Who blogs? Personality predictors of blogging. *Computers in Human Behavior,* 24,5, 1993-2004.

Guba, E. G. 1990. The Paradigm dialog. *In,* 1990 1990 Newbury Park, Calif.: Sage Publications.

Guba, E. G. & Lincoln, Y. S. 1994. Competing paradigms in qualitative research. *In:* Denzin, N. K. & Lincoln, Y. S. (eds.) *Handbook of Qualitative Research.* Thousand Oaks: Sage.

Guba, E. G. & Lincoln, Y. S. 2005. Paradigmatic Controversies, Contradictions and Emerging Confluences. *In:* Denzin, N. K. & Lincoln, Y. S. (eds.) *The SAGE Handbook of Qualitative Research.* Thousand Oaks: Sage.

Guha, S., Tang, K. & Francis, P. 2008. NOYB: privacy in online social networks. *Proceedings of the first workshop on Online social networks.* Seattle, WA, USA: ACM.

Gullone, E. & Moore, S. 2000. Adolescent risk-taking and the five-factor model of personality. *Journal of Adolescence,* 23,4, 393-407.

Gullone, E., Moore, S., Moss, S. & Boyd, C. 2000. The Adolescent Risk-Taking Questionnaire Development and Psychometric Evaluation. *Journal of Adolescent Research,* 15,2, 231-250.

Gustafson, P. E. 1998. Gender Differences in Risk Perception: Theoretical and Methodological Perspectives. *Risk Analysis,* 18,6, 805-811.

Gutteling, J. M. & Kuttschreuter, M. t. 2002. The role of expertise in risk communication: laypeople's and expert's perception of the millennium bug risk in The Netherlands. *Journal of Risk Research,* 5,1, 35-47.

Haas, S. M., Irr, M. E., Jennings, N. A. & Wagner, L. M. 2011. Communicating thin: A grounded model of Online Negative Enabling Support Groups in the pro-anorexia movement. *New Media & Society,* 13,1, 40-57.

Halliday, J. 2011. David Cameron considers banning suspected rioters from social media. *Guardian Newspaper,* Thursday 11 August 2011.

Halpern-Felsher, B. L. & Cauffman, E. 2001. Costs and benefits of a decision: Decision-making competence in adolescents and adults. *Journal of Applied Developmental Psychology,* 22,3, 257-273.

Halpern-Felsher, B. L., Millstein, S. G., Ellen, J. M., Adler, N. E., Tschann, J. M. & Biehl, M. 2001. The role of behavioral experience in judging risks. *Health Psychology,* 20,2, 120-126.

Hammond, R. 2003. *Identity Theft How to Protect Your Most Valuable Asset,* Franklin Lakes, NJ, Career Press.

Hampson, S. E., Severson, H. H., Burns, W. J., Slovic, P. & Fisher, K. J. 2001. Risk perception, personality factors and alcohol use among adolescents. *Personality and Individual Differences,* 30,1, 167-181.

Han, P. & Maclaurin, A. 2002. Do consumers really care about online privacy? *Marketing Management,* 11,1, 35-39.

Hansen, W. B. & Malotte, C. K. 1986. Perceived personal immunity: The development of beliefs about susceptibility to the consequences of smoking. *Preventive Medicine,* 15,4, 363-372.

Hargittai, E. 2007. Whose Space? Differences Among Users and Non-Users of Social Network Sites. *Journal of Computer-Mediated Communication,* 13,1, 276-297.

Hargittai, E. & Hsieh, Y.-l. P. 2010. Predictors and Consequences of Differentiated Practices on Social Network Sites. *Information, Communication & Society,* 13,4, 515-536.

Harman, J. P., Hansen, C. E., Cochran, M. E. & Lindsey, C. R. 2005. Liar, Liar: Internet Faking but Not Frequency of Use Affects Social Skills, Self-Esteem, Social Anxiety, and Aggression. *CyberPsychology & Behavior,* 8,1, 1-6.

Harper, K., Sperry, S. & Thompson, J. K. 2008. Viewership of pro-eating disorder websites: Association with body image and eating disturbances. *International Journal of Eating Disorders,* 41,1, 92-95.

Harridge-March, S. 2006. Can the building of trust overcome consumer perceived risk online? *Marketing Intelligence & Planning,* 24,7, 746 - 761.

Harris_&_Associates & Westin, A. F. 1998. E-Commerce and Privacy: What Net Users Want. Hackensack, NJ: Sponsored by Price Waterhouse and Privacy & American Business, Privacy & American Business.

Hasebrink, U., Livingstone, S. & Haddon, L. 2008. Comparing children's online opportunities and risks across Europe: Cross-national comparisons for EU Kids Online, (Deliverable D3.2). London: EU Kids Online.

Helweg-Larsen, M. & Shepperd, J. A. 2001. Do Moderators of the Optimistic Bias Affect Personal or Target Risk Estimates? A Review of the Literature. *Personality and Social Psychology Review,* 5,1, 74-95.

Henke, L. L. & Fontenot, G. 2007. Children And Internet Use: Perceptions Of Advertising, Privacy, And Functional Displacement. *Journal of Business & Economics Research,* 5,11, 59-65.

Heydebrand, W. V. 1983. Organization and praxis. *In:* G., M. (ed.) *Beyond method.* Beverly Hills, CA: Sage Publications.

Hill, R. A. & Dunbar, R. I. M. 2003. Social Network Size in Humans. *Human Nature,* 14,1, 53-72.

Hinduja, S. & Patchin, J. W. 2008a. Cyberbullying: An Exploratory Analysis of Factors Related to Offending and Victimization. *Deviant Behavior,* 29,2, 129-156.

Hinduja, S. & Patchin, J. W. 2008b. Personal information of adolescents on the Internet: A quantitative content analysis of MySpace. *Journal of Adolescence,* 31,1, 125-146.

Hirschheim, R. 1992. Information Systems Epistemology: An Historical Perspective. *In:* Galliers, R. D. (ed.) *Information Systems Research: Issues, Methods and Practical Guidelines.* Oxford: Blackwell Scientific Publications.

Hirschheim, R. & Klein, H. 1994. Realizing Emancipatory Principles in Information Systems Development: The Case for ETHICS10. *MIS Quarterly,* 18,1, 83-109.

Hogg, T. & Adamic, L. 2004. Enhancing reputation mechanisms via online social networks. *Proceedings of the 5th ACM conference on Electronic commerce.* New York, NY, USA: ACM.

Holtgrave, D. R. & Weber, E. U. 1993. Dimensions of Risk Perception for Financial and Health Risks. *Risk Analysis,* 13,5, 553-558.

Hopper, T. & Powell, A. 1985. Making sense of research into the organizational and social aspects of management accounting: a review of its underlying assumptions. *Journal of Management Studies,* 22,5, 429-465.

Horswill, M. S. & McKenna, F. P. 1999. The Effect of Perceived Control on Risk Taking. *Journal of Applied Social Psychology,* 29,2, 377-391.

Hosmer, L. T. 1995. Trust: The Connecting Link between Organizational Theory and Philosophical Ethics. *The Academy of Management Review,,* 20,2, 379-403.

Hsee, C. & Kunreuther, H. C. 2000. The Affection Effect in Insurance Decisions. *Journal of Risk and Uncertainty,* 20,2, 141-159.

Hsu, W. H., Lancaster, J., Paradesi, M. S. R. & Weninger, T. 2007. Structural Link Analysis from User Profiles and Friends Networks: A Feature Construction Approach. *In:* ICWSM' 2007 March 2007 2007 Boulder, Colorado, USA.

Huang, D.-L., Rau, P.-L. P. & Salvendy, G. 2007. A Survey of Factors Influencing People's Perception of Information Security. *In:* Jacko, J. (ed.) *Human-Computer Interaction. HCI Applications and Services.* Berlin/ Heidelberg: Springer

Hung, S.-Y., Ku, C.-Y. & Chang, C.-M. 2003. Critical factors of WAP services adoption: an empirical study. *Electronic Commerce Research and Applications,* 2,1, 42-60.

Hunter, P. 2008. Social networking: the focus for new threats -- and old ones. *Computer Fraud & Security,* 2008,7, 17-18.

Hussain, Z. & Griffiths, M. D. 2008. Gender Swapping and Socializing in Cyberspace: An Exploratory Study. *CyberPsychology & Behavior,* 11,1, 47-53.

Hussong, A. M., Hicks, R. E., Levy, S. A. & Curran, P. J. 2001. Specifying the relations between affect and heavy alcohol use among young adults. *Journal of Abnormal Psychology,* 110,3, 449-461.

Hycner, R. H. 1985. Some Guidelines for the Phenomenological Analysis of Interview Data. *Human Studies,* 8,3, 279-303.

Igra, V. & Irwin, C. E. 1996. Theories of adolescent risk-taking behavior. *In:* Diclemente, R. J., Hansen, W. B. & Poton, L. E. (eds.) *Handbook of Adolescent Health Risk Behavior.* New York: Plenum Press.

Jackson, D. N., Hourany, L. & Vidmar, N. J. 1972. A four-dimensional interpretation of risk taking. *Journal of Personality and Social Psychology,* 40,3, 483-501.

Jackson, J., Allum, N. & Gaskell, G. 2004a. Perceptions of risk in cyberspace. *Foresight Cyber Trust and Crime Prevention Project.* UK Office of Science and Technology.

Jackson, L. A., von Eye, A., Barbatsis, G., Biocca, F., Fitzgerald, H. E. & Zhao, Y. 2004b. The impact of Internet use on the other side of the digital divide. *Communications of the ACM,* 47,7, 43-47.

Jackson, L. A., Yong, Z., Kolenic Iii, A., Fitzgerald, H. E., Harold, R. & Von Eye, A. 2008. Race, Gender, and Information Technology Use: The New Digital Divide. *CyberPsychology & Behavior,* 11,4, 437-442.

Jacoby, J. & Kaplan, L. B. 1972. The components of perceived risk. *In:* Venkatesan, M., ed. 3rd Annual Conference of the Association for Consumer Research, 1972 College Park, MD. Association for Consumer Research, 382-392.

Jagatic, T. N., Johnson, N. A., Jakobsson, M. & Menczer, F. 2007. Social phishing. *Commun. ACM,* 50,10, 94-100.

Jarvenpaa, S. L., Tractinsky, N. & Saarinen, L. 1999. Consumer Trust in an Internet Store: A Cross-Cultural Validation. *Journal of Computer-Mediated Communication,* 5,2.

Jarvenpaa, S. L., Tractinsky, N. & Vitale, M. 2000. Consumer trust in an Internet Store. *Information Technology and Management,* 1,1, 45-71.

Jessor, R. 1984. Adolescent development and behavioural health. *In:* Matarazzo, J. D., Weiss, C. M., Herd, J. A., Miller, N. E. & Weiss, S. M. (eds.) *Behavioral health : a handbook of health enhancement and disease prevention.* New York: Wiley.

Jessor, R. 1987. Problem-Behavior Theory, Psychosocial Development, and Adolescent Problem Drinking. *British Journal of Addiction,* 82,4, 331-342.

Jessor, R. 1991. Risk behavior in adolescence: A psychosocial framework for understanding and action. *Journal of Adolescent Health,* 12,8, 597-605.

Jessor, R. & Jessor, S. L. 1977. *Problem behavior and psychosocial development : a longitudinal study of youth,* New York, Academic Press.

Jobber, D. & Fahy, J. 2002. *Foundations of marketing,* London, McGraw-Hill.

Johnson, B. 2010. Privacy no longer a social norm, says Facebook founder. *The Guardian,* Monday 11 January 2010.

Johnson, B. & Christensen, L. 2008. *Educational research : quantitative, qualitative, and mixed approaches,* London, Sage.

Johnson, E. J. & Tversky, A. 1983. Affect, Generalization, and the Perception of Risk.: STANFORD UNIV CA DEPT OF PSYCHOLOGY.

Johnson, E. J. & Tversky, A. 1984. Representations of perceptions of risks. *Journal of Experimental Psychology: General,* 113,1, 55-70.

Johnson, J. A. 2005. Ascertaining the validity of individual protocols from Web-based personality inventories. *Journal of Research in Personality,* 39,1, 103-129.

Johnson, R. B. & Onwuegbuzie, A. J. 2004. Mixed Methods Research: A Research Paradigm Whose Time Has Come. *Educational Researcher,* 33,7, 14-26.

Johnson, R. B., Onwuegbuzie, A. J. & Turner, L. A. 2007. Toward a Definition of Mixed Methods Research. *Journal of Mixed Methods Research,* 1,2, 112-133.

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

Jones, H. & Soltren, J. H. 2005. Facebook: Threats to Privacy. *Ethics and the Law on the Electronic Frontier Course.* Boston: Massachusetts Institute of Technology.

Juarascio, A. S., Shoaib, A. & Timko, C. A. 2010. Pro-Eating Disorder Communities on Social Networking Sites: A Content Analysis. *Eating Disorders,* 18,5, 393-407.

Jump, K. 2005. A new kind of fame - MU student garners a record 75,000 Facebook friends. *The Columbian Missourian,* Thursday, September 1, 2005.

Jung, C. G. 1923. *Psychological types : or, The psychology of individuation,* London, Routledge & Kegan Paul.

Kahneman, D., Slovic, P. & Tversky, A. (eds.) 1982. *Judgement under uncertainty: heuristics and biases,* Cambridge: Cambridge University Press.

Kahneman, D. & Tversky, A. 1979. Prospect Theory: an analysis of decision under risk. *Econometrica (pre-1986),* 47,2, 263-291.

Kanfer, F. H. 1970. Self-regulation: Research, issues and speculations. *In:* Neuringer, C. & Michael, J. L. (eds.) *Behavior Modification in Clinical Psychology.* New York Appleton-Century-Crofts.

Kaplan, L. B., Szybillo, G. J. & Jacoby, J. 1974. Components of perceived risk in product purchase: A cross-validation. *Journal of Applied Psychology,* 59,3, 287-291.

Karpinski, A. C. & Duberstein, A. 2009. A description of Facebook use and academic performance among undergraduate and graduate students. *Poster presented at the meeting of the American Educational Research Association.* San Diego, CA.

Kasperson, R. E. 1992. The social amplification of risk: progress in developing and integrative framework of risk. *In:* Krimsky, S. & Golding, D. (eds.) *Social Theories of Risk.* Westport, CT: Praeger.

Kasperson, R. E. & Kasperson, J. X. 1996. The social amplification and attenuation of risk. *The Annals of the American Academy of Political and Social Science,* 545, 95-105.
Kasperson, R. E., Renn, O., Slovic, P., Brown, H. S., Emel, J., Goble, R., Kasperson, J. X. & Ratick, S. 1988. The Social Amplification of Risk: a conceptual framework. *Risk Analysis,* 8,2, 177-187.
Kavanaugh, A., Carroll, J. M., Rosson, M. B., Zin, T. T. & Reese, D. D. 2005. Community Networks: Where Offline Communities Meet Online. *Journal of Computer-Mediated Communication,* 10,4.
Keaney, A. 2009. Identity theft and privacy - consumer awareness in Ireland. *International Journal of Networking and Virtual Organisations,* 6,6, 620 - 633.
Keaney, A. & Remenyi, D. 2004. Spamming and Scamming- the real picture! *Irish Journal of Management,* 25,1, 23 - 40.
Keil, M., Cule, P., Lyytinen, K. & Schmidt, R. 1998. A Framework for Identifying Software Project Risks. *Communications of the ACM,* 4,11, 76-83.
Keil, M., Wallace, L., Turk, D., Dixon-Randall, G. & Nulden, U. 2000. An investigation of risk perception and risk propensity on the decision to continue a software development project. *Journal of Systems and Software,* 53,2, 145-157.
Keith, S. & Martin, M. E. 2005. Cyber-Bullying: Creating a Culture of Respect in a Cyber world. *Reclaiming Children & Youth,* 13,4, 224-228.
Kelley, P. G., Bresee, J., Cranor, L. F. & Reeder, R. W. 2009. A "nutrition label" for privacy. *Proceedings of the 5th Symposium on Usable Privacy and Security.* Mountain View, California: ACM.
Kemerer, C. F. & Sosa, G. L. 1991. Systems development risks in strategic information systems. *Information and Software Technology,* 33,3, 212-223.
Kennedy, C., Kools, S. & Krueger, R. 2001. Methodological Considerations in Children's Focus Groups. . 50,3, 184-187.
Keown, C. F. 1989. Risk Perceptions of Hong Kongese vs. Americans. *Risk Analysis,* 9,3, 401-405.
Kierkegaard, S. 2008. Cybering, online grooming and ageplay. *Computer Law & Security Report,* 24,1, 41-55.
Kiesler, S., Siegel, J. & McGuire, T. W. 1984. Social psychological aspects of computer-mediated communication. *American Psychologist,* 39,10, 1123-1134.
Kiesler, S. & Sproull, L. 1992. Group decision making and communication technology. *Organizational Behavior and Human Decision Processes,* 52,1, 96-123.
Kim, K. & Prabhakar, B. 2000. Initial trust, perceived risk, and the adoption of internet banking. *Proceedings of the twenty first international conference on Information systems.* Brisbane, Queensland, Australia: Association for Information Systems.
Kirkpatrick, D. 2010. *The Facebook Effect,* Virgin Books.
Kirschner, P. A. & Karpinski, A. C. 2010. Facebook® and academic performance. *Computers in Human Behavior,* 26,6, 1237-1245.
Kolek, E. A. & Saunders, D. 2008. Online Disclosure: An Empirical Investigation of Undergraduate Facebook Profiles. *NASPA Journal (Online),* 41,1, 1-25.
Koop, C. E. 1987. Report of the Surgeon General's Workshop on Pornography and Public Health. *American Psychologist,* 42,10, 944-945.
Kortum, P., Edwards, C. & Richards-Kortum, R. 2008. The Impact of Inaccurate Internet Health Information in a Secondary School Learning Environment. *Journal of Medical Internet Research,* 10,2.
Korzyk, A. 2002. *A conceptual design model for integrative information systems security.* PhD, Virginia Commonwealth University.
Krantz, J. H. & Dalal, R. 2000. Validity of Web-based Psychological Research. *In:* Birnbaum, M. H. (ed.) *Psychological Experiments on the Internet.* San Diego, CA: Academic Press.

Kraut, R., Kiesler, S., Boneva, B., Cummings, J., Helgeson, V. & Crawford, A. 2002. Internet Paradox Revisited. *Journal of Social Issues,* 58,1, 49.

Kraut, R., Patterson, M., Lundmark, V., Kiesler, S., Mukophadhyay, T. & Scherlis, W. 1998. Internet paradox: A social technology that reduces social involvement and psychological well-being? *American Psychologist,* 53,9, 1017-1031.

Krebs, V. E. 2002. Mapping networks of terrorist cells. *Connections,* 24,3, 43-52.

Krimsky, S. & Golding, D. (eds.) 1992. *Social Theories of Risk*: Praeger Paperback.

Krishnamurthy, B. & Wills, C. E. 2008. Characterizing privacy in online social networks. *Proceedings of the first workshop on Online social networks.* Seattle, WA, USA: ACM.

Krosnick, J. A. & Fabrigar, L. R. 1997. Designing rating scales for effective measurement in surveys. *In:* Lyberg, L. E. A. (ed.) *Survey Measurement and Process Quality* New York: Wiley.

Krueger, R. A. & Casey, M. A. 2000. *Focus Groups: A Practical Guide for Applied Research,* Thousand Oaks, Calif, London, Sage Publications.

Kuhn, T. S. 1970. *The structure of scientific revolutions,* Chicago, University of Chicago Press.

Kujath, C. L. 2011. Facebook and MySpace: Complement or Substitute for Face-to-Face Interaction? *CyberPsychology, Behavior & Social Networking,* 14,1/2, 75-78.

Kumar, R., Novak, J. & Tomkins, A. 2006. Structure and evolution of online social networks. *Proceedings of the 12th ACM SIGKDD international conference on Knowledge discovery and data mining.* Philadelphia, PA, USA: ACM.

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A. & Pham, T. 2009. School of phish: a real-world evaluation of anti-phishing training. *Proceedings of the 5th Symposium on Usable Privacy and Security.* Mountain View, California: ACM.

Kuttschreuter, M. & Gutteling, J. M. 2004. Time will tell: changes in risk perception and the processing of risk information about the Y2K-risk. *Computers in Human Behavior,* 20,6, 801-821.

Kvale, S. & Brinkmann, S. 2009. *InterViews : learning the craft of qualitative research interviewing,* Los Angeles, Sage Publications.

Lampe, C., Ellison, N. & Steinfield, 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.* Banff, Alberta, Canada: ACM.

Lampe, C., Ellison, N. B. & Steinfield, C. 2008. Changes in use and perception of facebook. *Proceedings of the 2008 ACM conference on Computer supported cooperative work.* San Diego, CA, USA: ACM.

Lampe, C. A. C., Ellison, N. & Steinfield, C. 2007. A familiar face(book): profile elements as signals in an online social network. *In:* Proceedings of ACM CHI 2007 Conference on Human Factors in Computing Systems 2007. ACM Press, 435-444.

Landry, M. & Banville, C. 1992. A disciplined methodological pluralism for mis research. *Accounting, Management and Information Technologies,* 2,2, 77-97.

Langer, E. J. 1975. The illusion of control. *Journal of Personality and Social Psychology,* 32,2, 311-328.

Langford, I., Georgiou, S., Bateman, I. J., Day, R. J. & Turner, R. K. 2000. Public Perceptions of Health Risks from Polluted Coastal Bathing Waters: A Mixed Methodological Analysis Using Cultural Theory *Risk Analysis,* 20,5, 691-704.

Langford, I., Marris, C., McDonald, A.-L., Goldstein, H., Rasbash, J. & O'Riordan, T. 1999. Simultaneous Analysis of Individual and Aggregate Responses in Psychometric Data Using Multilevel Modeling *Risk Analysis,* 19,4, 675-683.

LaRose, R., Kim, J. H. & Peng, W. 2010. Social Networking: Addictive, Compulsive, Problematic, or Just Another Media Habit? *In:* Pappacharissi, Z. (ed.) *A Networked Self: Identity, Community, and Culture on Social Network Sites.* NY: Routledge.

LaRose, R., Mastro, D. & Eastin, M. S. 2001. Understanding Internet Usage. *Social Science Computer Review,* 19,4, 395-413.

Lavery, B., Siegel, A. W., Cousins, J. H. & Rubovits, D. S. 1993. Adolescent Risk-Taking: An Analysis of Problem Behaviors in Problem Children. *Journal of Experimental Child Psychology,* 55,2, 277-294.

Lee, A. S. 2001. Editor's comments. *MIS Quarterly,* 25,1, III - VII.

Lee, A. S., Liebenau, J. & DeGross, J. I. 1997. *Information Systems and Qualitative Research: Proceedings of the IFIP TC8 WG 8.2 International Conference on Information Systems and Qualitative Research, 31st May-3rd June 1997, Philadelphia, Pennsylvania, USA,* London, Chapman & Hall.

Lee, D. T. S., Chan, K. P. M. & Yip, P. S. F. 2005. Charcoal burning is also popular for suicide pacts made on the internet. *British Medical Journal,* 330,7491, 602.

Lee, E. & Leets, L. 2002. Persuasive Storytelling by Hate Groups Online. *American Behavioral Scientist,* 45,6, 927-957.

Leets, L. 2001. Responses to Internet Hate Sites: Is Speech Too Free in Cyberspace? *Communication Law and Policy,* 6,2, 287-317.

Lenhart, A. 2005. Protecting Teens Online. Washington DC: Pew Internet & American Life Project.

Lenhart, A. 2009. Teens and Sexting. Washington DC: Pew Internet & American Life Project.

Lenhart, A. & Madden, M. 2007. Social Networking Websites and Teens: an overview. Pew Internet & American Life Project.

Lerner, J. S. & Keltner, D. 2000. Beyond valence: Toward a model of emotion-specific influences on judgement and choice. *Cognition & Emotion,* 14,4, 473-493.

Lerner, J. S. & Keltner, D. 2001. Fear, anger, and risk. *Journal of Personality and Social Psychology,* 81,1, 146-159.

Leskovec, J., Adamic, L. A. & Huberman, B. A. 2007. The dynamics of viral marketing. *ACM Transactions on the Web (TWEB) archive,* 1,1.

Levin, B. 2002. Cyberhate. *American Behavioral Scientist,* 45,6, 958-988.

Levinson, J. C. 1984. *Guerrilla Marketing: Secrets for Making Big Profits from Your Small Business.,* Boston, Houghton Mifflin Company.

Lewis, K., Kaufman, J. & Christakis, N. 2008. The Taste for Privacy: An Analysis of College Student Privacy Settings in an Online Social Network. *Journal of Computer-Mediated Communication,* 14,1, 79-100.

Li, Q. 2006. Cyberbullying in Schools: A Research of Gender Differences *School Psychology International,* 27,2, 157-170

Li, Q. 2007a. Bullying in the new playground: Research into cyberbullying and cyber victimisation. *Australasian Journal of Educational Technology,* 23,4, 435-454.

Li, Q. 2007b. New bottle but old wine: A research of cyberbullying in schools. *Computers in Human Behavior,* 23,4, 1777-1791.

Liau, A. K., Khoo, A. & Peng Hwa, A. 2005. Factors Influencing Adolescents Engagement in Risky Internet Behavior. *CyberPsychology & Behavior,* 8,6, 513-520.

Lichtenstein, J. 2010. Digital Diplomacy. *The New York Times,* Sunday, July 18, 2010

Liebermann, Y. & Stashevsky, S. 2002. Perceived risks as barriers to Internet and e-commerce usage. *Qualitative Market Research,* 5,4, 291.

Lima, M. L., Barnett, J. & Vala, J. 2005. Risk Perception and Technological Development at a Societal Level. *Risk Analysis,* 25,5, 1229-1239.

Lin, K.-Y. & Lu, H.-P. 2011. Why people use social networking sites: An empirical study integrating network externalities and motivation theory. *Computers in Human Behavior,* 27,3, 1152-1161.
Lincoln, Y. S. & Guba, E. G. 1985. *Naturalistic inquiry* Beverly Hills (Calif.) ; London, Sage Publication.
Liu, H. & Maes, P. 2005. Interestmap: Harvesting social network profiles for recommendations. *In:* Beyond Personalization - IUI 2005, 9th January 2005 2005 San Diego, California.
Liu, X. & Wei, K. K. 2003. An empirical study of product differences in consumers' E-commerce adoption behavior. *Electronic Commerce Research and Applications,* 2,3, 229-239.
Livingstone, S. 2008. Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression. *New Media & Society,* 10,3, 393-411.
Livingstone, S., Bober, M. & Helsper, E. 2005. Internet literacy among children and young people: findings from the UK Children Go Online project. London: LSE Rerearch Online.
Livingstone, S. & Brake, D. R. 2010. On the Rapid Rise of Social Networking Sites: New Findings and Policy Implications. *Children & Society,* 24,1, 75-83.
Livingstone, S. & Haddon, L. 2008. Risky Experiences for Children Online: Charting European Research on Children and the Internet. *Children & Society,* 22,4, 314-323.
Livingstone, S., Haddon, L., Görzig, A. & Ólafsson, K. 2010a. Risks and safety for children on the internet: the UK Report. LSE, London: EU Kids Online.
Livingstone, S., Haddon, L., Görzig, A. & Ólafsson, K. 2010b. Risks and safety on the internet: The perspective of European Children. Initial Findings. LSE, London: EU Kids Online.
Livingstone, S., Haddon, L., Görzig, A. & Ólafsson, K. 2011a. Risks and safety on the internet: The perspective of European Children. Full Findings. LSE, London: EU Kids Online.
Livingstone, S. & Helsper, E. 2007. Gradations in digital inclusion: children, young people and the digital divide. *New Media & Society,* 671-696.
Livingstone, S., Ólafsson, K. & Staksrud, E. 2011b. Social Networking, Age and Privacy. LSE, London: EU Kids Online.
Lloyd, A. J. 2001. The extent of patients' understanding of the risk of treatments. *Quality in Health Care,* 10,1, i14-i18.
Loewenstein, G. & Furstenberg, F. 1991. Is Teenage Sexual Behavior Rational? *Journal of Applied Social Psychology,* 21,12, 957-986.
Lounsbury, K., Mitchell, K. J. & Finkelhor, D. 2011. The True Prevalence of "Sexting". Available: https://www.unh.edu/ccrc/pdf/Sexting%20Fact%20Sheet%204_29_11.pdf [Accessed 4 July 2011].
Lowenstein, G. F., Weber, E. U., Hee, C. K. & Welch, N. 2001. Risk as feelings. *Psychological Bulletin,* 127,2, 267-286.
Lu, H.-P., Hsu, C.-L. & Hsu, H.-Y. 2005. An empirical study of the effect of perceived risk upon intention to use online applications. *Information Management & Computer Security,* 13,2/3, 106.
Luce, R. D. & Weber, E. U. 1986. An axiomatic theory of conjoint, expected risk. *Journal of Mathematical Psychology,* 30,2, 188-205.
Lupton, D. 1999. *Risk,* Abingdon, Oxon, Routledge.

Lyons, E. J., Mehl, M. R. & Pennebaker, J. W. 2006. Pro-anorexics and recovering anorexics differ in their linguistic Internet self-presentation. *Journal of Psychosomatic Research,* 60,3, 253-256.

Lyytinen, K. & Mathiassen, L. 1998. Attention Shaping and Software Risk--A Categorical Analysis of Four Classical Risk Management Approaches. *Information Systems Research,* 9,3, 233-255.

Ma, X. 2001. Bullying and being bullied: To what extent are bulliers also vicitim? *American Educational Research Journal,* 38,2, 351-370.

Maccrimmon, K. R. & Wehrung, D. A. 1985. A portfolio of risk measures *Journal Theory and Decision,* 19,1, 1-29.

MacGregor, D. G. 2003. Public response to Y2K: social amplification and risk adaption: or, "how I learned to stop worrying and love Y2K". *In:* Pidgeon, N., Kasperson, R. E. & Slovic, P. (eds.) *The Social Amplification of Risk.* Cambridge, UK: Cambridge University Press.

MacGregor, D. G., Slovic, P. & Morgan, M. G. 1994. Perception of Risks From Electromagnetic Fields: A Psychometric Evaluation of a Risk-Communication Approach. *Risk Analysis,* 15,5, 815-828.

Machlis, G. E. & Rosa, E. A. 1990. Desired Risk: Broadening the Social Amplification of Risk Framework. *Risk Analysis,* 10,1, 161-168.

Madden, M. & Smith, A. 2010. Reputation Management and Social Media: How people monitor their identity and search for others online. Pew Internet & American Life Project.

Malhotra, N. K., Kim, S. S. & Agarwal, J. 2004. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research,* 15,4, 336.

Manago, A. M., Graham, M. B., Greenfield, P. M. & Salimkhan, G. 2008. Self-presentation and gender on MySpace. *Journal of Applied Developmental Psychology,* 29,6, 446-458.

Maple, C., Short, E. & Antony, B. 2011. Cyberstalking in the United Kingdom, An Analysis of Echo Pilot Survey. National Centre for Cyberstalking Research, University of Bedfordshire.

March, J. G. & Shapira, Z. 1987. Managerial Perspectives on Risk and Risk Taking. *Management Science,* 33,11, 1404-1418.

Marks, L. E. & Gescheider, G. A. 2002. Psychophysical Scaling. *In:* Pashler, H. (ed.) *Stevens' Handbook of Experimental Psychology.* 3rd edition ed. New York: John Wiley & Sons, Inc.

Marlowe, L. 2010. Nine teens indicted in connection with suicide of Irish high school pupil. *The Irish Times,* March 31, 2010.

Marr, N. & Field, T. 2001. *Bullycide : death at playtime,* Didcot, Success Unlimited.

Marris, C., Langford, I. H. & O'Riordan, T. 1998. A Quantitative Test of the Cultural Theory of Risk Perceptions: Comparison with the Psychometric Paradigm *Risk Analysis,* 18,5, 635-647.

Martin, N. 2008. Facebook users at risk of identity fraud. *Telegraph,* 21/02/2008.

Maxwell, J. A. 2005. *Qualitative research design : an interactive approach,* London, Sage.

Mayer-Schönberger, V. 2011. *Delete : the virtue of forgetting in the digital age,* Princeton, N.J. ; Woodstock, Princeton University Press.

Mayer, R. C., Davis, J. H. & Schoorman, D. F. 1995. An Integrative Model of Organisational Trust. *Academy of Management Review,* 20,3, 709-734.

Mayfield, R. 2005. Social Network Dynamics and Participatory Politics. *In:* Lebkowsky, J. & Ratcliffe, M. (eds.) *Extreme Democracy.* Lulu.com.

McDaniels, T. L., Axelrod, L. J., Cavanagh, N. S. & Slovic, P. 1997. Perception of Ecological Risk to Water Environments. *Risk Analysis,* 17,3, 341-352.

McDonald, M. 1999. CyberHate: Extending persuasive techniques of low credibility sources to the world wide web. *In:* Schumann, D. W. & Thorson, E. (eds.) *Advertising and the world wide web.* Mahwah, NJ: Lawrence Erlbaum Associates.

McElroy, J. C., Hendrickson, A. R., Townsend, A. M. & DeMarie, S. M. 2007. Dispositional Factors in Internet Use: Personaility versus Cognitive Style. *MIS Quarterly,* 31,4, 809-820.

McGrath, K. 2005. Doing critical research in information systems: a case of theory and practice not informing each other. *Information Systems Journal,* 15,2, 85-101.

McKay, H. G., Glasgow, R. E., Feil, E. G., Boles, S. M. & Barrera, M., Jr. 2002. Internet-based diabetes self-management and support: Initial outcomes from the Diabetes Network project. *Rehabilitation Psychology,* 47,1, 31-48.

McKenna, K. Y. A. & Bargh, J. A. 1998. Coming out in the age of the Internet: Identity 'demarginalization' through virtual group participation. *Journal of Personality and Social Psychology,* 75,3, 681-694.

McKenna, K. Y. A. & Bargh, J. A. 2000. Plan 9 From Cyberspace: The Implications of the Internet for Personality and Social Psychology. *Personality & Social Psychology Review (Lawrence Erlbaum Associates),* 4,1, 57-75.

McKeon, M. 2010. *The Evolution of Privacy on Facebook* [Online]. Available: http://www.mattmckeon.com/facebook-privacy/ [Accessed 3rd June 2011].

McKnight, D. H. & Chervany, N. L. 2002. What Trust Means in E-Commerce Customer Relationships: An Interdisciplinary Conceptual Typology. *International Journal of Electronic Commerce,* 6,2, 35-59.

McKnight, D. H., Choudhury, V. & Kacmar, C. 2002. The impact of initial consumer trust on intentions to transact with a web site: a trust building model. *Journal of Strategic Information Systems,* 11,3-4, 297-323.

McKnight, D. H., Cummings, L. L. & Chervany, N. L. 1998. Initial Trust Formation in New Organizational Relationships. *The Academy of Management Review,* 23,3, 473-490.

McLean, H. 2008. Identity theft: Six clicks from a cyber crook *Telegraph*, 29/02/2008.

Meyer, D. 2011. German state bans Facebook pages, 'Like' buttons. *ZDNet UK* [Online], 2011 Available: http://www.zdnet.co.uk/news/compliance/2011/08/22/german-state-bans-facebook-pages-like-buttons-40093735/ [Accessed 22 August 2011].

Microsoft 2011. Microsoft Security Intelligence Report. Redmond, WA: Microsoft.

Milgram, S. 1967. The small world problem. *Psychology Today,*, 6, 62-67.

Miller, D., Kets De Vries, M. F. R. & Toulouse, J.-M. 1982. Top Executive Locus of Control and Its Relationship to Strategy-Making, Structure, and Environment. *The Academy of Management Journal,* 25,2, 237-253

Miller, D. C. & Byrnes, J. P. 1997. The role of contextual and personal factors in children's risk taking. *Developmental Psychology,* 33,5, 814-823.

Miller, K. S., Forehand, R. & Kotchick, B. A. 2000. Adolescent sexual behavior in two ethnic minority groups: A multisystem perspective. *Adolescence,* 35,138, 313.

Millstein, S. G. & Halpern-Felsher, B. L. 2002a. Judgements about Risk and Perceived Invulnerability in Adolescents and Young Adults. *Journal of Research on Adolescence,* 12,4, 399.

Millstein, S. G. & Halpern-Felsher, B. L. 2002b. Perceptions of risk and vulnerability. *Journal of Adolescent Health,* 31,1, Supplement 1, 10-27.

Millwood Hargrave, A., Livingstone, S. & Brake, D. 2007. Harm and Offence in Media Content: Updating the 2005 Review. Ofcom's Submission to the Byron Review. Annex 6: Literary Review. London: OFCOM, UK Office of Communications.

Mingers, J. 2001. Combining IS Research Methods: Towards a Pluralist Methodology. *Information Systems Research,* 12,3, 240-259.

Mingers, J. 2003. The paucity of multimethod research: a review of the information systems literature. *Information Systems Journal,* 13,3, 233-249.

Mingers, J. 2004. Real-izing information systems: critical realism as an underpinning philosophy for information systems. *Information and Organization,* 14,2, 87-103.

Mislove, A., Marcon, M., Gummad, K., P. , Druschel, P. & Bhattacharjee, B. 2007a. Measurement and analysis of online social networks. *Proceedings of the 7th ACM SIGCOMM conference on Internet measurement.* San Diego, California, USA: ACM.

Mislove, A., Marcon, M., Gummadi, K. P., Druschel, P. & Bhattacharjee, B. 2007b. Measurement and analysis of online social networks. *Proceedings of the 7th ACM SIGCOMM conference on Internet measurement.* San Diego, California, USA: ACM.

Mitchell, K. J., Finkelhor, D. & Wolak, J. 2001. Risk Factors for and Impact of Online Sexual Solicitation of Youth. *JAMA,* 285,23, 3011-3014.

Mitchell, K. J., Finkelhor, D. & Wolak, J. 2003. The Exposure Of Youth To Unwanted Sexual Material On The Internet: A National Survey of Risk, Impact, and Prevention. *Youth Society,* 34,3, 330-358.

Mitchell, K. J. & Ybarra, M. 2009. Social Networking Sites: Finding a Balance Between Their Risks and Benefits. *Arch Pediatr Adolesc Med,* 163,1, 87-89.

Mitchell, P. 2000. Internet addiction: genuine diagnosis or not? *The Lancet,* 355,9204, 632-632.

Miyazaki, A. D. & Fernandez, A. 2001. Consumer perceptions of privacy and security risks for online shopping. *The Journal of Consumer Affairs,* 35,1, 27.

Monge, P. & Contractor, N. 2000. Emergence of communication networks. *In:* Jablin, F. M. & Putnam, L. L. (eds.) *The new handbook of organizational communication : advances in theory, research, and methods.* 2nd ed. Thousand Oaks, Calif. ; London: Sage Publications.

Montgomery, K. 2001. Digital kids: The new on-line children's consumer culture. *In:* Singer, D. G. & Singer, J. L. (eds.) *Handbook of children and the media.* Thousand Oaks, CA: Sage Publications.

Moody, E. J. 2001. Internet Use and Its Relationship to Loneliness. *CyberPsychology & Behavior,* 4,3, 393-401.

Moore, E. S. 2004. Children and the Changing World of Advertising. *Journal of Business Ethics,* 52,2, 161-167.

Moore, E. S. & Rideout, V. J. 2007. The Online Marketing of Food to Children: Is It Just Fun and Games? *Journal of Public Policy & Marketing,* 26,2, 202-220.

Moore, G. C. & Benbasat, I. 1991. Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation. *Information Systems Research,* 2,3, 192-222.

Moore, S. & Gullone, E. 1996. Predicting adolescent risk behavior using a personalized cost-benefit analysis. *Journal of Youth and Adolescence,* 25,3, 343-359.

Moore, S. & Rosenthal, D. 1991. Adolescent Invulnerability and Perceptions of AIDS Risk. *Journal of Adolescent Research,* 6,2, 164-180.

Morahan-Martin, J. & Schumacher, P. 2000. Incidence and correlates of pathological Internet use among college students. *Computers in Human Behavior,* 16,1, 13-29.

Moreno, M. A., VanderStoep, A., Parks, M. R., Zimmerman, F. J., Kurth, A. & Christakis, D. A. 2009. Reducing At-Risk Adolescents' Display of Risk Behavior on a Social Networking Web Site: A Randomized Controlled Pilot Intervention Trial. *Arch Pediatr Adolesc Med,* 163,1, 35-41.

Morgan, D. L. 1996. Focus groups. *Annual Review of Sociology,* 22, 129.

Morgan, D. L. 2007. Paradigms Lost and Pragmatism Regained: Methodological Implications of Combining Qualitative and Quantitative Methods. *Journal of Mixed Methods Research,* 1,1, 48-76.

Morozov, E. 2009. The brave new world of slacktivism. *Foreign Policy: Net Effect* [Online]. Available from: http://neteffect.foreignpolicy.com/posts/2009/05/19/the_brave_new_world_of_slacktivism [Accessed May 19 2009 2011].

Morozov, E. 2011. *The net delusion : how not to liberate the world,* London Allen Lane.

Morse, J. M. 1999. Myth #93: Reliability and Validity Are Not Relevant to Qualitative Inquiry. *Qualitative Health Research,* 9,6, 717-718.

Morse, J. M. 2003. Principles of mixed methods and multimethod research design. *In:* Tashakkori, A. & Teddlie, C. (eds.) *Handbook of mixed methods in social and behavioral research.* Thousand Oaks, CA: Sage.

Morse, J. M., Barrett, M., Mayan, M., Olson, K. & Spiers, J. 2008. *Verification Strategies for Establishing Reliability and Validity in Qualitative Research*.

Mulveen, R. & Hepworth, J. 2006. An Interpretative Phenomenological Analysis of Participation in a Pro-anorexia Internet Site and Its Relationship with Disordered Eating. *Journal of Health Psychology,* 11,2, 283-296.

Murdock, G., Petts, J. & Horklick-Jones, T. 2003. After amplification: rethinking the role of the media in risk communication. *In:* Pidgeon, N., Kasperson, R. E. & Slovic, P. (eds.) *The Social Amplification of Risk.* Cambridge: Cambridge University Press.

Murray, C. D. & Fox, J. 2006. Do Internet self-harm discussion groups alleviate or exacerbate self-harming behaviour? *Australian e-Journal for the Advancement of Mental Health (AeJAMH),* 5,3, 9.

Myers, I. B., H., M. M., Quenk, N. L. & Hammer, A. L. 1998. *MBTI Manual (A guide to the development and use of the Myers Briggs type indicator),* Palo Alto, CA,, Consulting Psychologists Press, Inc.,.

Myers, M. D. & Newman, M. 2007. The qualitative interview in IS research: Examining the craft. *Information and Organization,* 17,1, 2-26.

Narayanan, A. 2009. De-anonymizing Social Networks. *In:* Vitaly, S., ed., 2009. 173-187.

Nasr, O. 2010. Nasr explains controversial tweet on Lebanese cleric *This Just In* [Online]. Available from: http://news.blogs.cnn.com/2010/07/06/nasr-explains-controversial-tweet-on-lebanese-cleric/ [Accessed 29 June 2011].

National_Campaign_to_Prevent_Teen_and_Unplanned_Pregnancy & CosmoGirl.com 2008. Sex and tech: Results from a survey of teens and young adults Washington DC: The national campaign to prevent teen and unplanned pregnancy.

National_Research_Council 1996. *Understanding risk: informing decisions in a democratic society,* Washington DC, National Academy Press.

NCTE/SAFT 2003. Children's study – investigating online behaviour.: Safety Awareness Fact and Tools.

Negroponte, N. 1996. *Being Digital,* New York, Vintage.

Ngwenyama, O. & Lee, A. S. 1997. Communication Richness in Electronic Mail: Critical Social Theory and the Contextuality of Meaning. *MIS Quarterly,* 21,2, 145-168.

Nie, N. H. 2001. Sociability, interpersonal relations, and the Internet: Reconciling conflicting findings. *The American Behavioral Scientist,* 45,3, 420.

Nie, N. H. & Hillygus, D. S. 2002. The Impact of Internet Use on Sociability: Time-Diary Findings. *IT&Society,* 1,1, 1-20.

Niemz, K., Griffiths, M. & Banyard, P. 2005. Prevalence of Pathological Internet Use among University Students and Correlations with Self-Esteem, the General Health Questionnaire (GHQ), and Disinhibition. *CyberPsychology & Behavior,* 8,6, 562-570.

Norberg, P. A., Horne, D. R. & Horne, D. A. 2007. The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *Journal of Consumer Affairs,* 41,1, 100-126.

Norris, M. L., Boydell, K. M., Pinhas, L. & Katzman, D. K. 2006. Ana and the Internet: A review of pro-anorexia websites. *International Journal of Eating Disorders,* 39,6, 443-447.

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

Nugent, H. & Dean, J. 2007. Millions of Facebook users 'leave themselves open to identity theft'. *The Times,* August 14, 2007.

Nyland, R. & Near, C. 2007. Jesus is My Friend: Religiosity as a Mediating Factor in Internet Social Networking Use. *AEJMC Midwinter Conference.* Reno, Nevada.

O'Halloran, M. 2011. Agency cites internet misuse for marital rifts. *The Irish Times,* August 12, 2011.

O'Moore, M. & Minton, S. J. 2010. Cyber-bullying: The Irish Experience. *In:* Columbus, A. M. (ed.) *Advances in Psychology Research, .* Hauppauge, NY: Nova Science Publishers, Inc.

O'Neill, B., Grehan, S. & Ólafsson, K. 2011. Risks and safety for children on the internet: the Ireland Report. LSE, London: EU Kids Online.

Oates, B. J. 2006. *Researching information systems and computing,* London, Sage.

OFCOM 2008. Social Networking - A quantitative and qualitative research report into attitudes, behaviour and use. London: UK Office of Communications.

Office, C. S. 2009. *Labour Market, Principal Statistics, Persons aged 15 years and over classified by sex and principal economic status. (000's)* [Online]. Central Statistics Office. Available: http://www.cso.ie/statistics/persons_by_sex_ecstatus.htm [Accessed 24th August 2010 2010].

Ogilvie, E. 2001. Cyberstalking. *Crime & Justice International,* 17,50, 9-10.

Olsen, R. A. 1997. Investment risk: The experts' perspective. *Financial Analysts Journal,* 53,2, 62-67.

Olsen, R. A. 2001. Behavioral Finance as Science: Implications From the Research of Paul Slovic. *Journal of Psychology & Financial Markets,* 2,3, 157-159.

Orlikowski, W. J. & Baroudi, J. J. 1991. Studying Information Technology in Organizations: Research Approaches and Assumptions. *Information Systems Research,* 2,1, 1-28.

Ortega, A., Høgh, A., Pejtersen, J. & Olsen, O. 2009. Prevalence of workplace bullying and risk groups: a representative population study. *International Archives of Occupational and Environmental Health,* 82,3, 417-426.

Osgood, D. W., Johnston, L. D., O Malley, P. M. & Bachman, J. G. 1988. The Generality of Deviance in Late Adolescence and Early Adulthood. *American Sociological Review,* 53,1, 81.

Owens, L. T. 2011. *Criminals Exploiting Japan's Tragedy: A Chance to Teach Digital Literacy* [Online]. TrendMicro. Available: http://internetsafety.trendmicro.com/criminals-exploiting-japans-tragedy-a-chance-to-teach-digital-literacy [Accessed 23 June 2011].

Palich, L. E. & Bagby, D. R. 1995. Using cognitive theory to explain entrepreneurial risk-taking: Challenging conventional wisdom. *Journal of Business Venturing,* 10,6, 425-438.

Palmer, M. 2008. Ofcom warns parents over children's networking sites. *Financial Times,* 2nd April 2008, p.4.

Pan, Y. & Zinkhan, G. M. 2006. Exploring the impact of online privacy disclosures on consumer trust. *Journal of Retailing,* 82,4, 331.

Pardini, D., Lochman, J. & Wells, K. 2004. Negative Emotions and Alcohol Use Initiation in High-Risk Boys: The Moderating Effect of Good Inhibitory Control. *Journal of Abnormal Child Psychology,* 32,5, 505-518.

Parks, M. R. & Floyd, K. 1996. Making Friends in Cyberspace. *The Journal of Communication,* 46,1, 80-97.

Parsons, J. T., Halkitis, P. N., Bimbi, D. & Borkowski, T. 2000. Perceptions of the benefits and costs associated with condom use and unprotected sex among late adolescent college students. *Journal of Adolescence,* 23,4, 377-391.

Parsons, J. T., Siegel, A. W. & Cousins, J. H. 1997. Late adolescent risk-taking: effects of perceived benefits and perceived risks on behavioral intentions and behavioral change. *Journal of Adolescence,* 20,4, 381-392.

Pasek, J., more, e. & Hargittai, E. 2009. Facebook and academic performance: Reconciling a media sensation with data. *First Monday,* 15,5.

Patchin, J. W. & Hinduja, S. 2006. Bullies Move Beyond the Schoolyard: A Preliminary Look at Cyberbullying. *Youth Violence and Juvenile Justice,* 4,2, 148 - 169.

Pather, S. & Remenyi, D. 2004. Some of the philosophical issues underpinning research in information systems: from positivism to critical realism. *Proceedings of the 2004 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries.* Stellenbosch, Western Cape, South Africa: South African Institute for Computer Scientists and Information Technologists.

Pattinson, M. & Anderson, G. 2006. Risk Communication, Risk Perception and Information Security *In:* Dowland, P., Furnell, S., Thuraisingham, B. & Wang, X. S. (eds.) *Security Management, Integrity, and Internal Control in Information Systems* Boston: Springer

Pattinson, M. & Anderson, G. 2007. How well are information risks being communicated to your computer end-users? *Information Management & Computer Security,* 15,5, 362-371.

Patton, M. Q. 2002. *Qualitative research & evaluation methods,* Thousand Oaks, Calif. ; London, Sage.

Pavlou, P. A. 2003. Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model. *International Journal of Electronic Commerce,* 7,3, 101-134.

Pelling, E. L. & White, K. M. 2009. The Theory of Planned Behavior Applied to Young People's Use of Social Networking Web Sites. *CyberPsychology & Behavior,* 12,6, 755-759.

Peluchette, J. & Karl, K. 2008. Social Networking Profiles: An Examination of Student Attitudes Regarding Use and Appropriateness of Content. *CyberPsychology & Behavior,* 11,1, 95-97.

Pérez, M. C. 2008. Facebook brings protest to Colombia. *New York Times,* Friday, February 8, 2008.

Perloff, L. S. 1987. Social comparison and illusions of invulnerability to negative life events. *In:* Snyder, C. R. & Ford, C. E. (eds.) *Coping with negative life events: Clinical and social psychological perspectives.* New York: Plenum Press.

Perry, B. 2000. *Button-down terror : The metamorphosis of the hate movement,* Cincinnati, OH, University of Cincinnati.

Perry, C. L., Kelder, S. H., Murray, D. M. & Klepp, K. I. 1992. Communitywide smoking prevention: long-term outcomes of the Minnesota Heart Health Program and the Class of 1989 Study. *Am J Public Health,* 82,9, 1210-1216.

Perry, D. G., Kusel, S. J. & Perry, L. C. 1988. Victims of peer aggression. *Developmental Psychology,* 24,6, 807-814.

Peter, J., Valkenburg, P. M. & Schouten, A. P. 2006. Characteristics and Motives of Adolescents Talking with Strangers on the Internet. *CyberPsychology & Behavior,* 9,5, 526-530.

Pfeffer, J. 1993. Barriers to the advance of organizational science: Paradigm. *Academy of Management. The Academy of Management Review,* 18,4, 599.

Phelps, J., Nowak, G. & Ferrell, E. 2000. Privacy Concerns and Consumer Willingness to Provide Personal Information. *Journal of Public Policy & Marketing,* 19,1, 27-41.

Phippen, A. 2009. Sharing Personal Images and Videos Among Young People. Exeter: SouthWest Grid for Learning, University of Plymouth.

Phippen, A., Davey, R. & Furnell, S. M. 2009. Should We Do It Because We Can? Methodological and Ethical Implications for Information Revelation in Online Social Networks. *Methodological Innovations Online,* 4,3, 41-55.

Pidgeon, N. 1998. Risk assessment, risk values and the social science programme: why do we need risk perception research. *Reliability, Engineering and System Safety,* 59,1, 5-15.

Pidgeon, N., Hood, C., Jones, D., Turner, B. & Gibson, R. (eds.) 1992. *Risk perception,* London: The Royal Society.

Pike, J. C., Bateman, P. J. & Butler, B. S. 2009. I Didn't Know You Could See That: The Effect of Social Networking Environment Characteristics on Publicness and Self-Disclosure. *In:* AMCIS 2009 Proceedings, August 6 - 9, 2009 2009 San Francisco, California. Paper 421.

Pingdom 2010. Pingdom Study: Ages of Social Network Users. Pingdom Inc.

Piquero, A. R., Brame, R., Mazerolle, P. & Haapanen, R. 2002. Crime in Emerging Adulthood. *Criminology,* 40,1, 137.

Pollet, T. V., Roberts, S. G. B. & Dunbar, R. I. M. 2011. Use of Social Network Sites and Instant Messaging Does Not Lead to Increased Offline Social Network Size, or to Emotionally Closer Relationships with Offline Network Members. *CyberPsychology, Behavior & Social Networking,* 14,4, 253-258.

Pollitt, M. M. 1998. Cyberterrorism -- fact or fancy? *Computer Fraud & Security,* 1998,2, 8-10.

Postmes, T. O. M., Spears, R. & Lea, M. 1998. Breaching or Building Social Boundaries?: SIDE-Effects of Computer-Mediated Communication. *Communication Research,* 25,6, 689-715.

Prasad, V. & Owens, D. 2001. Using the internet as a source of self-help for people who self-harm. *Psychiatric Bulletin,* 25, 222-225.

Pratarelli, M. E., Browne, B. L. & Johnson, K. 1999. The bits and bytes of computer/Internet addiction: A factor analytic approach. *Behavior Research Methods, Instruments, & Computers,* 31,2, 305-314.

Preece, J., Nonnecke, B. & Andrews, D. 2004. The top five reasons for lurking: improving community experiences for everyone. *Computers in Human Behavior,* 20,2, 201-223.

Preibusch, S., Hoser, B., Gürses, S. & Berendt, B. 2007. Ubiquitous social networks - opportunities and challenges for privacy-aware user modelling. *In:* Data Mining for User Modelling Workshop (DM.UM'07), June 2007 2007 Corfu.

Privitera, C. & Campbell, M. A. 2009. Cyberbullying: The New Face of Workplace Bullying? *CyberPsychology & Behavior,* 12,4, 395-400.

Putnam, H. 1995. *Pragmatism : an open question,* Oxford, Blackwell.

Quadrel, M. J., Fischhoff, B. & Davis, W. 1993. Adolescent (in)vulnerability. *American Psychologist,* 48,2, 102-116.

Quinn, J. 2010. Tiger takes a bite of Linked ln to value it at $2bn-plus. *The Daily Telegraph,* July 29, 2010, p.3.

Rainer, R. K., Snyder, C. A. & Carr, H. H. 1991. Risk analysis for information technology *Journal of Management Information Systems*, 8,1, 129-147.
Rajagopal, S. 2004. Suicide pacts and the internet. *British Medical Journal*, 329,7478, 1298-9.
Rau, P.-L. P., Gao, Q. & Ding, Y. 2008. Relationship between the level of intimacy and lurking in online social network services. *Computers in Human Behavior*, 24,6, 2757-2770.
Rayner, S. 1992. Cultural Theory and Risk Analysis. *In:* Krimsky, S. & Golding, D. (eds.) *Social Theories of Risk.* Westport CT: Praeger.
Raynes-Goldie, K. 2010. Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. *First Monday (Online)*, 15,1.
Reichheld, F. F. & Schefter, P. 2000. E-Loyalty: Your Secret Weapon on the Web. *Harvard Business Review*, 78,4, 105-113.
Remenyi, D., Williams, B., Money, A. & Swartz, E. 1998. *Doing Research in Business and Management*, Sage Publications.
Renn, O. 1991 Risk communication and the social amplification of risk. *Technology risk and society*, 4, 287-326.
Renn, O. 1998. Three decades of risk research: accomplishments and new challenges. *Journal of Risk Research*, 1,1, 49-71.
Renn, O. 2005. Risk Rationality Diagram. *In:* Social Contexts and Responses to Risk Inaugural Conference, 2005 University of Kent at Canterbury.
Renn, O. 2008. *Risk Governance - Coping with Uncertainty in a Complex World*, London, Sterling VA, Earthscan.
Renn, O., Burns, W. J., Kasperson, J. X., Kasperson, R. E. & Slovic, P. 1992. The Social Amplification of Risk: Theoretical Foundations and Empirical Applications. *Journal of Social Issues*, 48,4, 137-160.
Renn, O. & Rohrmann, B. 2000. *Cross-cultural risk perception : a survey of empirical studies* Dordrecht; London, Kluwer.
Repetti, R. L., Taylor, S. E. & Seeman, T. E. 2002. Risky families: Family social environments and the mental and physical health of offspring. *Psychological Bulletin*, 128,2, 330-366.
Rescher, N. 2000. *Realistic pragmatism : an introduction to pragmatic philosophy*, Albany, N.Y., State University of New York Press.
Resnick, M. D., Bearman, P. S., Blum, R. W., Bauman, K. E., Harris, K. M., Jones, J., Tabor, J., Beuhring, T., Sieving, R. E., Shew, M., Ireland, M., Bearinger, L. H. & Udry, J. R. 1997. Protecting adolescents from harm. Findings from the National Longitudinal Study on Adolescent Health. *JAMA*, 278,10, 823-832.
Richardson, B., Sorensen, J. & Soderstrom, E. J. 1987. Explaining the Social and Psychological Impacts of a Nuclear Power Plant Accident1. *Journal of Applied Social Psychology*, 17,1, 16-36.
Richardson, H. & Robinson, B. 2007. The mysterious case of the missing paradigm: a review of critical information systems research 1991â€“2001. *Information Systems Journal*, 17,3, 251-270.
Richmond, R. 2010. Facebook "Dislike" Button is a Scam. *The New York Times Gadgetwise* [Online]. Available from: http://gadgetwise.blogs.nytimes.com/2010/08/17/facebook-dislike-button-is-a-scam/ [Accessed 24 June 2011].
Richtel, M. 2003. The Lure of Data: Is It Addictive? *The New York Times*, Sunday, July 6, 2003.
Riegel, R. 2007. Bullied teen took overdose. *Irish Independent*, December 12 2007.
Rippl, S. 2002. Cultural theory and risk perception: a proposal for a better measurement. *Journal of Risk Research*, 5,2, 147-165.

Robey, D. 1996. Research Commentary: Diversity in Information Systems Research: Threat, Promise, and Responsibility. *Information Systems Research,* 7,4, 400-408.
Rochlen, A. B., Zack, J. S. & Speyer, C. 2004. Online therapy: Review of relevant definitions, debates, and current empirical support. *Journal of Clinical Psychology,* 60,3, 269-283.
Rodgers, K. B. 1999. Parenting Processes Related to Sexual Risk-Taking Behaviors of Adolescent Males and Females. *Journal of Marriage and the Family,* 61,1, 99-109.
Rogers, A., Day, J., Randall, F. & Bentall, R. 2003. Patients' understanding and participation in a trial designed to improve the management of anti-psychotic medication. *Social Psychiatry and Psychiatric Epidemiology,* 38,12, 720-727.
Rogers, G. O. 1997. The Dynamics of Risk Perception: How Does Perceived Risk Respond to Risk Events? *Risk Analysis,* 17,6, 745-757.
Rohall, D. E., Cotten, S. R. & Charlie, M. 2002. Internet use and the self concept: linking specific uses to global self-esteem. *Current Research in Social Psychology,* 8,1, 1-19.
Roman, D. 2009. Internet addiction: it's spreading, but is it real? *Commun. ACM,* 52,11, 12-12.
Romer, D., Black, M., Ricardo, I., Feigelman, S. & et al. 1994. Social influences on the sexual behavior of youth at risk for HIV exposure. *American Journal of Public Health,* 84,6, 977.
Rorty, R. 1982. *Consequences of pragmatism : essays 1972-1980,* Brighton, Harvester.
Rorty, R. 1991. *Objectivity, relativism, and truth,* Cambridge, Cambridge University Press.
Rosa, E. A. 1998. Metatheoretical foundations for post-normal risk. *Journal of Risk Research,* 1,1, 15-44.
Rosa, E. A. & Freudenburg, W. R. 2001. Risk, Sociological Study of. *In:* Smelser, N. J. & Baltes, P. B. (eds.) *International Encyclopedia of the Social and Behaviour Sciences.* Oxford: Elsevier.
Roselius, T. 1971. Consumer Rankings of Risk Reduction Methods. *The Journal of Marketing,* 35,1, 56-61.
Ross, C., Orr, E. S., Sisic, M., Arseneault, J. M., Simmering, M. G. & Orr, R. R. 2009. Personality and motivations associated with Facebook use. *Computers in Human Behavior,* 25,2, 578-586.
Rotter, J. B. 1966. Generalized expectancies for internal verus external control of reinforcement. *Psychological Monographs,* 80,Whole no: 609.
Rotter, J. B. 1990. Internal versus External Control of Reinforcement: A Case History of a Variable. *American Psychologist.,* 45,4, 489-493.
Rouleau, C. R. & von Ranson, K. M. 2011. Potential risks of pro-eating disorder websites. *Clinical Psychology Review,* 31,4, 525-531.
Ruane, J. M. 2005. *Essentials of research methods : a guide to social science research,* Malden, Mass. ; Oxford, Blackwell.
Rubin, H. J. & Rubin, I. S. 2005. *Qualitative interviewing : the art of hearing data,* Thousand Oaks, Calif., Sage Publications.
Rundmo, T. 2002. Associations between affect and risk perception. *Journal of Risk Research,* 5,2, 119-135.
Sanders, C. E., Field, T. M., Diego, M. & Kaplan, M. 2000. The Relationship of Internet Use to Depression and Social Isolation Among Adolescents. *Adolescence,* 35,138, 237.
Saris, W. E., Revilla, M., Krosnick, J. A. & Shae, E. M. 2010. Comparing Questions with Agree/Disagree Response Options to Questions with Item-Specific Response Options. *Survey Research Methods,* 4,1, 61-79.
Saunders, M., Lewis, P. & Thornhill, A. 2007. *Research Methods for Business Students,* Harlow, England, Prentice Hall, Financial Times.

Saunders, M., Lewis, P. & Thornhill, A. 2009. *Research Methods for Business Students,* Harlow, England, Pearson Education Limited.
Savadori, L., Savio, S., Nicotra, E., Rumiati, R., Finucane, M. & Slovic, P. 2004. Expert and Public Perception of Risk from Biotechnology. *Risk Analysis,* 24,5, 1289-1299.
Scherer, C. W. & Cho, H. 2003. A Social Network Contagion Theory of Risk Perception. *Risk Analysis,* 23,2, 261-267.
Scherer, K. 1997. College Life On-Line: Healthy and Unhealthy Internet Use. *JOURNAL OF COLLEGE STUDENT DEVELOPMENT,* 38,6, 655-665.
Schmidt, R., Lyytinen, K., Keil, M. & Cule, P. 2001. Identifying Software Project Risks: An International Delphi Study. *Journal of Management Information Systems,* 17,4, 5-36.
Schneier, B. 2010. Schneier on Security: Privacy and Control. *Journal of Privacy and Confidentiality,* 2,1, 3-4.
Schoeman, F. D. 1984. *Philosophical Dimensions of Privacy: an Anthology,* Cambridge; New York, Cambridge University Press.
Schwartz, B. 2005. *The paradox of choice : why more is less,* New York HarperCollins.
Schwartz, K. L., Roe, T., Northrup, J., Meza, J., Seifeldin, R. & Neale, A. V. 2006. Family Medicine Patients' Use of the Internet for Health Information: A MetroNet Study. *J Am Board Fam Med,* 19,1, 39-45.
Schwarz, N. 1996. *Cognition and communication: Judgmental biases, research methods and the logic of conversation,* Hillsdale, NJ, Erlbaum.
Schwarz, N., Knauper, B., Hippler, H.-j., Noelle-neumann, E. & Clark, L. 1991. Rating Scales Numeric Values May Change The Meaning Of Scale Labels. *Public Opin Q,* 55,4, 570-582.
Scott, J. 2000. *Social Network Analysis - a handbook,* London, Sage Publications.
Scott, J. E. & Vessey, I. 2002. Managing Risks in Enterprise Systems Implementations. *Communications of the ACM,* 45,4, 74-81.
Shaffer, H. J., Hall, M. N. & Bilt, J. V. 2000. "Computer Addiction": A Critical Consideration. *American Journal of Orthopsychiatry,* 70,2, 162-168.
Shapira, N. A., Goldsmith, T. D., Keck, P. E., Khosla, U. M. & McElroy, S. L. 2000. Psychiatric features of individuals with problematic internet use. *Journal of Affective Disorders,* 57,1-3, 267-272.
Shaw, D. S., Wagner, E. F., Arnett, J. & Aber, M. S. 1992. The factor structure of the Reckless Behavior Questionnaire. *Journal of Youth and Adolescence,* 21,3, 305-323.
Shaw, L. H. & Gant, L. M. 2002. In Defense of the Internet: The Relationship between Internet Communication and Depression, Loneliness, Self-Esteem, and Perceived Social Support. *CyberPsychology & Behavior,* 5,2, 157-171.
Sheehan, K. B. & Hoy, M. G. 2000. Dimensions of Privacy Concern Among Online Consumers. *Journal of Public Policy & Marketing,* 19,1, 62-73.
Sheldon, P. 2008. The relationship between unwillingness-to-communicate and students' Facebook use. *Journal of Media Psychology: Theories, Methods, and Applications,* 20,2, 67-75.
Shen, D., Laffey, J., Lin, Y. & Huang, X. 2006. Social Influence for Perceived Usefulness and Ease-of-Use of Course Delivery Systems. *Journal of Interactive Online Learning,* 5,3, 270-282.
Sherer, S. A. & Alter, S. 2004. Information System Risk and Risk Factors: Are They Mostly About Information Systems. *Communications of the Association for Information Systems,* 14,Article 2, 29-64.
Sheridan, L. P. & Grant, T. 2007. Is cyberstalking different? *Psychology, Crime & Law,* 13,6, 627-640.

Shiner, R. L., Masten, A. S. & Tellegen, A. 2002. A developmental perspective on personality in emerging adulthood: Childhood antecedents and concurrent adaptation. *Journal of Personality and Social Psychology,* 83,5, 1165-1177.
Shirky, C. 2011. The Political Power of Social Media. *Foreign Affairs* [Online], Available: http://www.gpia.info/files/u1392/Shirky_Political_Poewr_of_Social_Media.pdf [Accessed 30 Aug 2011].
Shklovski, I., Kiesler, S. & Kraut, R. 2006. The Internet and Social Interaction: A Meta-analysis and Critique of Studies, 1995-2003. *In:* Kraut, R., Brynin, M. & Kiesler, S. (eds.) *Computers, Phones, and the Internet: The Social Impact of Information Technology*. Oxford: Oxford University Press.
Siegel, A. W. & Cousins, J. H. 1994. Adolescents' perceptions of the benefits and risks of their own risk taking. *Journal of Emotional & Behavioral Disorders,* 2,2, 89.
Siegel, J., Dubrovsky, V., Kiesler, S. & McGuire, T. W. 1986. Group processes in computer-mediated communication. *Organizational Behavior and Human Decision Processes,* 37,2, 157-187.
Siegel, M. L. 1998. Hate Speech, Civil Rights, and the Internet: The Jurisdictional and Human Rights Nightmare. *Albany Law Journal of Science & Technology,* 9, 375-298.
Siegrist, M., Earle, T. C. & Gutscher, H. 2007a. Trust, Risk Perception and the TCC Model of Cooperation. *In:* Siegrist, M., Earle, T. C. & Gutscher, H. (eds.) *Trust in Cooperative Risk Management: Uncertainty and Scepticism in the Public Mind* London: Earthscan.
Siegrist, M. & Gutscher, H. 2006. Flooding Risks: A Comparison of Lay People's Perceptions and Expert's Assessments in Switzerland. *Risk Analysis,* 26,4, 971-979.
Siegrist, M., Keller, C., Kastenholz, H., Frey, S. & Wiek, A. 2007b. Laypeople's and Experts' Perception of Nanotechnology Hazards. *Risk Analysis,* 27,1, 59-69.
Siegrist, M., Keller, C. & Kiers, H. A. L. 2005. A New Look at the Psychometric Paradigm of Perception of Hazards. *Risk Analysis,* 25,2, 211-222.
Sigfusdottir, I.-D., Farkas, G. & Silver, E. 2004. The Role of Depressed Mood and Anger in the Relationship Between Family Conflict and Delinquent Behavior. *Journal of Youth and Adolescence,* 33,6, 509-522.
Silverman, D. 1969. Organizations: a rejoinder. *Sociology,* 3,3, 420-421.
Silverman, D. 2006. *Interpreting Qualitative Data: Methods for Analyzing Talk, Text and Interaction,* London, Sage.
Simon_Wiesenthal_Center 2009. Facebook, YouTube+: How Social Media Outlets Impact Digital Terrorism and Hate. LA: Simon Wiesenthal Center.
Sitkin, S. B. & Pablo, A. L. 1992. Reconceptualizing the Determinants of Risk Behavior. *The Academy of Management Review,* 17,1, 9-38.
Sitkin, S. B. & Weingart, L. R. 1995. Determinants of Risky Decision-Making Behavior: A Test of the Mediating Role of Risk Perceptions and Propensity. *The Academy of Management Journal,* 38,6, 1573-1592
Sjöberg, L. 1993. Life-styles and risk perception. *(RHIZIKON: Risk Research Report 14):*. Stockholm: Center for Risk Research, Stockholm School of Economics. .
Sjöberg, L. 1996. A discussion of the limitations of the psychometric and cultural theory approaches to risk perception. *Radiation Protection Dosimetry,* 68,3/4, 219-225.
Sjöberg, L. 1999. The psychometric paradigm revisitied. *In:* Royal Statistical Society Annual Conference, 1999 University of Warwick.
Sjöberg, L. 2000. Factors in Risk Perception. *Risk Analysis,* 20,1, 1-11.
Sjöberg, L. 2001. Limits of Knowledge and the Limited Importance of Trust. *Risk Analysis,* 21,1, 189-198.

Sjöberg, L. 2002a. The Allegedly Simple Structure of Experts' Risk Perception: An Urban Legend in Risk Research. *Science, Technology and Human Values,* 27,4, 443-459.
Sjöberg, L. 2002b. Are Received Risk Perception Models Alive and Well? *Risk Analysis,* 22,4, 665-669.
Sjöberg, L. & Drottz-Sjöberg, B. M. 1994. Risk Perception of Nuclear Waste: Experts and the Public. *RHIZIKONL Risk Research Report.* Centre for Risk Research, Stockholm School of Economics.
Sjöberg, L. & Fromm, J. 2001. Information Technology Risks as Seen by the Public. *Risk Analysis,* 21,3, 427-441.
Sjöberg, L. & Torell, G. 1993. The Development of Risk Acceptance and Moral Valuation. *Scandanavian Journal of Psychology,* 34, 223-236.
Sjöberg, L. & Winroth, E. 1986. Risk, Moral Values of Actions and Mood. *Scandanavian Journal of Psychology,* 27,3, 191-208.
Skills, D. o. E. a. 2010. Statistical Report 2009_2010.
Slovic, P. 1987. Perception of Risk. *Science,* 236,4799, 280-285.
Slovic, P. 1993. Perceived Risk, Trust, and Democracy. *Risk Analysis,* 13,6, 675-682.
Slovic, P. 1997. Trust, Emotion, Sex, Politics and Science: Surveying the Risk-assessment Battlefield. *In:* Bazerman, M., Messick, D., Tenbrunsel, A. & Wade-Benzone, K. (eds.) *Environment, Ethics and Behaviour.* San Francisco: New Lexington Press.
Slovic, P. 1999. Trust, Emotion, Sex, Politics, and Science: Surveying the Risk-Assessment Battlefield. *Risk Analysis: An International Journal,* 19,4, 689-701.
Slovic, P. 2000a. Do Adolescent Smokers Know the Risks? *In:* Slovic, P. (ed.) *The Perception of Risk.* London and Sterling, VA: Earthscan.
Slovic, P. 2000b. *The Perception of Risk,* London and Sterling, VA, Earthscan.
Slovic, P. 2000c. What does it mean to know a cumulative risk? Adolescents' perceptions of short-term and long-term consequences of smoking. *Journal of Behavioral Decision Making,* 13,2, 259-266.
Slovic, P., Finucane, M., Peters, E. & MacGregor, D. G. 2004. Risk as Analysis and Risk as Feelings: Some Thoughts about Affect, Reason, Risk, and Rationality. *Risk Analysis,* 24,2, 311-322.
Slovic, P., Finucane, M., Peters, E. & MacGregor, D. G. 2007a. The affect heuristic. *European Journal of Operational Research,* 177,3, 1333-1352.
Slovic, P., Fischhoff, B. & Lichtenstein, S. 1979. Rating the Risks. *Environment,* 2,3, 14-20, 36-39.
Slovic, P., Fischhoff, B. & Lichtenstein, S. 1980. Facts and Fears: Understanding Perceived Risk. *In:* Schwing, R. C. & Albers, W. a. J. (eds.) *Societal Risk Assessment: How safe is safe enough?* New York: Plenum press.
Slovic, P., Fischhoff, B. & Lichtenstein, S. 1984. Behavioral decision theory perspectives on risk and safety *Acta Psychologica,* 56,1-3, 183-203.
Slovic, P., Flynn, J., Mertz, C. K., Poumàdere, M. & Mays, C. 2000. Nuclear power and the public: a comparative study of risk perception in France and the United States. *In:* Renn, O. & Rohrmann, B. (eds.) *Cross-Cultural Risk Perception: A Survey of Empirical Studies.* Dordrecht/Boston/London: Kluwer Academic Publishers.
Slovic, P., Peters, E., Grana, J., Berger, S. & Dieck, G. S. 2007b. Risk Perception of Prescription Drugs: Results of a National Survey. *Drug Information Journal,* 41,1, 81.
Slovic, P. & Weber, E. U. 2002. Perception of Risk Posed by Extreme Events. *Risk Management strategies in an Uncertain World.* Palisades, New York.
Smith, A. M. A. & Rosenthal, D. A. 1995. Adolescents' perceptions of their risk environment. *Journal of Adolescence,* 18,2, 229-245.

Smith, H. A., McKeen, J. D. & Staples, S. 2001. Risk Management in Information Systems: Problems and Potential. *Communications of the Association for Information Systems,* 7,Article 13, 29.

Smith, H. J., Milberg, S. J. & Burke, S. J. 1996. Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly,* 20,2, 167.

Smith, J. K. 1983. Quantitative Versus Qualitative Research: An Attempt to Clarify the Issue. *Educational Researcher,* 12,3, 6-13.

Smith, P., Mahdavi, J., Carvalho, M. & Tippett, N. 2006. An investigation into cyberbullying, its forms, awareness and impact, and the relationship between age and gender in cyberbullying. A Report to the Anti-Bullying Alliance.: Unit for School and Family Studies, Goldsmiths College, University of London.

Smyth, J. D., Dillman, D. A., Christian, L. M. & Stern, M. J. 2006. Comparing Check-All and Forced-Choice Question Formats in Web Surveys. *Public Opin Q,* 70,1, 66-77.

Socialbakers. 2011. *Ireland Facebook Statistics* [Online]. Available: http://www.socialbakers.com/facebook-statistics/ireland [Accessed 15 August 2011 2011].

Sophos. 2007. *Sophos Facebook ID probe shows 41% of users happy to reveal all to potential identity thieves* [Online]. Available: http://www.sophos.com/pressoffice/news/articles/2007/08/facebook.html [Accessed 1st October 2008].

Sophos 2011. Security Threat Report 2010. Sophos.

Spiekermann, S., Grossklags, J. & Berendt, B. 2001. E-privacy in 2nd generation E-commerce: privacy preferences versus actual behavior. *Proceedings of the 3rd ACM conference on Electronic Commerce.* Tampa, Florida, USA: ACM.

Spitzberg, B. H. & Hoobler, G. 2002. Cyberstalking and the technologies of interpersonal terrorism. *New Media Society,* 4,1, 71-92.

Sproull, L. & Kiesler, S. 1986. Reducing Social Context Cues: Electronic Mail in Organizational Communications. *Management Science,* 32,11, 1492-1512.

Stahl, B. C. 2008. The ethical nature of critical research in information systems. *Information Systems Journal,* 18,2, 137-163.

Stahl, B. C. & Brooke, C. 2008. The Contribution of Critical IS Research. *Communications of the ACM,* 51,3, 51-55.

Staksrud, E. & Livingstone, S. 2008. Children and online risk *AoIR* Copenhagen.

Staksrud, E. & Lobe, B. 2010. Evaluation of the implementation of the Safer Social Networking Principles for the EU Part I: General Report. Luxembourg: European Commission Safer Internet Programme.

Stamoulis, K. & Farley, F. 2010. Conceptual Approaches to Adolescent Online Risk-Taking. Cyberpsychology. *Journal of Psychosocial Research on Cyberspace,* 4,1.

Starr, C. 1969. Social Benefit versus Technological Risk. *Science,* 165,3899, 1232-1238.

Steinfield, C., Ellison, N. B. & Lampe, C. 2008. Social capital, self-esteem, and use of online social network sites: A longitudinal analysis. *Journal of Applied Developmental Psychology,* 29,6, 434-445.

Stewart, A. 2004. On risk: perception and direction. *Computers & Security,* 23,5, 362-370.

Stewart, D. W., Shamdasani, P. N. & Rook, D. W. 2007. *Focus groups : theory and practice, 2nd Edition,* Thousand Oaks, Calif. ; London, SAGE Publications.

Strano, M. 2008. User Descriptions and Interpretations of Self-Presentation through Facebook Profile Images. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace,* 2,2, Article 1.

Strater, K. & Lipford, H. R. 2008. Strategies and struggles with privacy in an online social networking community. *Proceedings of the 22nd British HCI Group Annual Conference on HCI 2008: People and Computers XXII: Culture, Creativity, Interaction - Volume 1.* Liverpool, United Kingdom: British Computer Society.

Stutzman, F. 2006. An evaluation of identity-sharing behavior in social network communities. *In:* Proceedings of the 2006 iDMAa and IMS Code Conference, 2006 Oxford,Ohio.

Subrahmanyam, K., Reich, S. M., Waechter, N. & Espinoza, G. 2008. Online and offline social networks: Use of social networking sites by emerging adults. *Journal of Applied Developmental Psychology,* 29,6, 420-433.

Suh, B. & Han, I. 2003a. The Impact of Customer Trust and Perception of Security Control on the Acceptance of Electronic Commerce. *International Journal of Electronic Commerce,* 7,3, 135-161.

Suh, B. & Han, I. 2003b. The IS risk analysis based on a business model *Information & Management,* 41,2, 149-158

Suler, J. 2004. The Online Disinhibition Effect. *CyberPsychology & Behavior,* 7,3, 321-326.

Surowiecki, J. 2005. *The Wisdom of Crowds: Why the Many Are Smarter Than the Few and How Collective Wisdom Shapes Business, Economies, Societies and Nations,* London, Abacus.

Syverson, P. 2003. The paradoxical value of privacy. *In:* 2nd Annual Workshop on Economics and Information Security - WEIS '03, May 29-30, 2003 2003 University of Maryland.

Tan, F. B., Yan, L. & Urquhart, C. 2007. The effect of cultural differences on Attitude, Peer influence, external influence and Self-efficacy in actual online shopping behavior. *Journal of Information Science and Technology,* 4,1, 3-23.

Tan, S. J. 1999. Strategies for reducing consumers' risk aversion in Internet shopping. *The Journal of Consumer Marketing,* 16,2, 163.

Tansey, J. & O'Riordan, T. 1999. Cultural theory and risk: a review. *Health, Risk & Society,* 1,1, 71-90.

Tashakkori, A. & Teddlie, C. 2003. *Handbook of mixed methods in social and behavioral research,* Thousand Oaks, CA, Sage.

Taylor-Gooby, P. & Zinn, J. O. 2006. Current Directions in Risk Research: New Developments in Psychology and Sociology *Risk Analysis,* 26,2, 397-411.

Taylor, S. & Todd, P. 1995a. Assessing IT usage: The role of prior experience. *MIS Quarterly,* 19,4, 561.

Taylor, S. & Todd, P. A. 1995b. Understanding information technology usage: A test of competing models. *Information Systems Research,* 6,2, 144.

Teddlie, C. & Tashakkori, A. 2009. *Foundations of Mixed Methods Research : integrating quantitative and qualitative approaches in the social and behavioral sciences,* Thousand Oaks CA; London, Sage Publications.

Teese, R. & Bradley, G. 2008. Predicting Recklessness in Emerging Adults: A Test of a Psychosocial Model. *The Journal of Social Psychology,* 148,1, 105.

Teigen, K. H., Brun, W. & Slovic, P. 1988. Societal risks as seen by a Norwegian public. *Journal of Behavioral Decision Making,* 1,2, 111-130.

Tennfjord, O. S. & Rundmo, T. 2007. Risk Perception and Worry Related to Adolescents' Judgement of Three Types of Risk. *Journal of Risk Research,* 10,1, 67-84.

Terdiman, D. 2011. Zuckerberg shows off sweeping Facebook changes. *ZDNet UK* [Online], 2011 Available: http://www.zdnet.co.uk/news/desktop-apps/2011/09/23/zuckerberg-shows-off-sweeping-facebook-changes-40094010/ [Accessed 23 September 2011].

Thomas, R. M. 2003a. *Blending qualitative & quantitative research methods in theses and dissertations,* Thousand Oaks, Calif. ; London, Corwin Press.

Thomas, T. L. 2003b. Al Qaeda and the Internet: The Danger of 'Cyberplanning'. *Parameters: US Army War College,* 33,1, 112.

Thompson, R. L., Higgins, C. A. & Howell, J. M. 1991. Personal Computing: Toward a Conceptual Model of Utilization. *MIS Quarterly,* 15,1, 125.

Thompson, S. 1999. The Internet and its potential influence on suicide. *Psychiatric Bulletin,* 23,8, 449-451.

Thrift, N. 2005. *Knowing capitalism* London, Sage.

Thurlow, C., Lengel, L. & Tomic, A. 2004. *Computer Mediated Communication: Social Interaction and the Internet,* London, Sage.

Tidwell, L. C. & Walther, J. B. 2002. Computer-Mediated Communication Effects on Disclosure, Impressions, and Interpersonal Evaluations: Getting to Know One Another a Bit at a Time. *Human Communication Research,* 28,3, 317-348.

Tierney, S. 2008. Creating communities in cyberspace: pro-anorexia web sites and social capital. *Journal of Psychiatric and Mental Health Nursing,* 15,4, 340-343.

Timofeeva, Y. A. 2002. Hate Speech Online: Restricted or Protected? Comparison of Regulations in the United States and Germany. *Journal of Transnational Law and Policy,* 12,2, 253-286.

Tjaden, P. & Thoennes, N. 1998. Stalking in America: Findings From the National Violence Against Women Survey. Washington, DC: Department of Justice, National Institute of Justice.

To, P.-L., Liao, C., Chiang, J. C., Shih, M.-L. & Chang, C.-Y. 2008. An empirical investigation of the factors affecting the adoption of Instant Messaging in organizations. *Computer Standards & Interfaces,* 30,3, 148-156.

Tong, S. T., Van Der Heide, B., Langwell, L. & Walther, J. B. 2008. Too Much of a Good Thing? The Relationship Between Number of Friends and Interpersonal Impressions on Facebook. *Journal of Computer-Mediated Communication,* 13,3, 531-549.

Tourangeau, R., Couper, M. P. & Conrad, F. 2004. Spacing, Position, and Order: Interpretive Heuristics for Visual Features of Survey Questions. *Public Opin Q,* 68,3, 368-393.

Tourangeau, R., Couper, M. P. & Conrad, F. 2007. Color, Labels, and Interpretive Heuristics for Response Scales. *Public Opin Q,* 71,1, 91-112.

Tsohou, A., Karyda, M., Kokolakis, S. & Kiountouzis, E. 2006. Formulating information systems risk management strategies through cultural theory. *Information Management & Computer Security,* 14,3, 198-217.

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

Tufekci, Z. 2010. Who Acquires Friends through Social Media and Why? "Rich get Richer" versus "Seek and Ye Shall Find". *In:* Fourth International AAAI Conference on Weblogs and Social Media, May 23-26, 2010 2010 George Washington University, Washington, DC. The AAAI Press, Menlo Park, California., 170-177.

Turner, R. A., Irwin, C. E., Tschann, J. M. & Millstein, S. G. 1993. Autonomy, relatedness, and the initiation of health risk behaviors in early adolescence. *Health Psychology,* 12,3, 200-208.

Turpin-Petrosino, C. 2002. Hateful Sirens. . .Who Hears Their Song? An Examination of Student Attitudes Toward Hate Groups and Affiliation Potential. *Journal of Social Issues,* 58,2, 281-301.

Tversky, A. & Kahneman, D. 1974. Judgment under Uncertainty: Heuristics and Biases. *Science,* 185,4157, 1124-1131.

Twigger-Ross, C. L. & Breakwell, G. M. 1999. Relating risk experience, venturesomeness and risk perception. *Journal of Risk Research,* 2,1, 73-83.

Tyler, T. R. & Cook, F. L. 1984. The mass media and judgments of risk: Distinguishing impact on personal and societal level judgments. *Journal of Personality and Social Psychology,* 47,4, 693-708.

Tynes, B. 2005. Children, Adolescents and the Culture of Online Hate. *In:* Dowd, N. E., Singer, D. G. & Wilson, R. F. (eds.) *Handbook of Children,Culture and Violence.* Thousand Oaks, Calif: Sage Publications.

Utz, S. 2010. Show me your friends and I will tell you what type of person you are: How one's profile, number of friends, and type of friends influence impression formation on social network sites. *Journal of Computer-Mediated Communication,* 15,2, 314-335.

Utz, S. & 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.

Valkenburg, P. M. 2004. Uses and effects of interactive media *In:* Valkenburg, P. M. (ed.) *Children's responses to the screen: a media psychological approach.* Taylor & Francis.

Valkenburg, P. M. & Peter, J. 2007a. Online Communication and Adolescent Well-Being: Testing the Stimulation Versus the Displacement Hypothesis. *Journal of Computer-Mediated Communication,* 12,4, 1169-1182.

Valkenburg, P. M. & Peter, J. 2007b. Preadolescents' and Adolescents' Online Communication and Their Closeness to Friends. *Developmental Psychology,* 43,2, 267-277.

Valkenburg, P. M. & Peter, J. 2009. Social Consequences of the Internet for Adolescents: A Decade of Research. *Current Directions in Psychological Science (Wiley-Blackwell),* 18,1, 1-5.

Valkenburg, P. M., Peter, J. & Schouten, A. P. 2006. Friend Networking Sites and Their Relationship to Adolescents' Well-Being and Social Self-Esteem. *CyberPsychology & Behavior,* 9,5, 584-590.

Valkenburg, P. M., Schouten, A. P. & Peter, J. 2005. Adolescents' identity experiments on the internet. *New Media & Society,* 7,3, 383-402.

Van der Heijden, H., Verhagen, T. & Creemers, M. 2003. Understanding online purchase intentions: Contributions from technology and trust perspectives. *European Journal of Information Systems,* 12,1, 41.

Van Duyn, A. 2006. Child protection fears hit online social networks Reports of sexual predators exploiting sites to make contact with teenagers have led to calls for tighter security. *Financial Times,* 22nd June 2006, p.9.

Vaughn, S., Shay Schumm, J. & Sinagub, J. 1996. *Focus group interviews in education and psychology,* Thousand Oaks ; London, SAGE Publications.

Venkatesh, V., Morris, M. G., Davis, G. B. & Davis, F. D. 2003. User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly,* 27,3, 425-478.

Viscusi, W. K. 1990. Do Smokers Underestimate Risks? *Journal of Political Economy,* 98,6, 1253.

Viscusi, W. K. 1991. Age Variations in Risk Perceptions and Smoking Decisions. *The Review of Economics and Statistics,* 73,4, 577-588.

Viscusi, W. K. 1992. *Smoking : making the risky decision,* New York, Oxford University Press.

Vitale, M. R. 1986. The Growing Risks of Information Systems Success. *MIS Quarterly,* 10,4, 327-335.

Wah, L. 1998. The risky business of managing IT risks. *Management Review.,* 87,5, 6.

Walker, P. 2010. CNN fires Middle East editor for tweet tribute to Hezbollah cleric: Journalist says posting was 'error of judgment'. *The Guardian,* July 9, 2010, p.17.

Walsham, G. 1993. *Interpreting information systems in organizations,* Chichester, Wiley.

Walsham, G. 1995. The Emergence of Interpretivism in IS Research. *Information Systems Research,* 6,4, 376-394.
Walsham, G. 2005. Learning about being critical. *Information Systems Journal,* 15,2, 111-117.
Walther, J. B. 1992. Interpersonal Effects in Computer-Mediated Interaction: A Relational Perspective. *Communication Research,* 19,1, 52-90.
Walther, J. B. & Parks, M. R. 2002. Cues filtered out, cues filtered in: Computer-mediated communication and relationships. *In:* Knapp, M. L. & Daly, J. A. (eds.) *Handbook of interpersonal communication.* 3rd Edition ed. Thousand Oaks, CA: Sage.
Walther, J. B., Van Der Heide, B., Hamel, L. M. & Shulman, H. C. 2009. Self-Generated Versus Other-Generated Statements and Impressions in Computer-Mediated Communication. *Communication Research,* 36,2, 229-253.
Walther, J. B., Van Der Heide, B., Kim, S.-Y., Westerman, D. & Tom Tong, S. 2008. The Role of Friends' Appearance and Behavior on Evaluations of Individuals on Facebook: Are We Known by the Company We Keep? *Human Communication Research,* 34,1, 28-49.
Warren, S. V. & Brandeis, L. D. 1890. The Right to Privacy. *Harvard Law Review,* 4,5, 193-220.
Wästlund, E., Norlander, T. & Archer, T. 2001. Internet Blues Revisited: Replication and Extension of an Internet Paradox Study. *CyberPsychology & Behavior,* 4,3, 385-391.
Watson, S. W., Smith, Z. & Driver, J. 2006. Alcohol, Sex and Illegal Activities: An Analysis of Selected Facebook Central Photos in Fifty States.
Watts, G. 2003. The trouble with risk. Royal Statistical Society.
Weber, E. U. 2001. Risk: Empirical Studies on Decision and Choice. *In:* Smelser, N. J. & Baltes, P. B. (eds.) *International Encyclopedia of the Social and Behaviour Sciences.* Oxford: Elsevier.
WEBWISE 2009. Webwise 2008 Survey of Children's Use of the Internet in Ireland.
Weimann, G. 2005. How Modern Terrorism Uses the Internet. *The Journal of International Security Affairs,* 8.
Weimann, G. 2006. *Terror on the Internet: The New Arena, the New Challenges*, The United States Institute of Peace.
Weinstein, N. D. 1980. Unrealistic optimism about future life events. *Journal of Personality and Social Psychology,* 39,5, 806-820.
Weinstein, N. D. 1984. Why it won't happen to me: Perceptions of risk factors and susceptibility. *Health Psychology,* 3,5, 431-457.
Weinstein, N. D. 1987. Unrealistic optimism about susceptibility to health problems: Conclusions from a community-wide sample. *Journal of Behavioral Medicine,* 10,5, 481-500.
Weiser, E. B. 2001. The Functions of Internet Use and Their Social and Psychological Consequences. *CyberPsychology & Behavior,* 4,6, 723-743.
Wellman, B. 2001. Computer Networks As Social Networks. *Science,* 293,5537, 2031.
Wellman, B., Haase, A. Q., Witte, J. & Hampton, K. 2001. Does the Internet increase, decrease, or supplement social capital? Social networks, participation, and community commitment. *The American Behavioral Scientist,* 45,3, 436.
Wellman, B. & Potter, S. 1999. The elements of personal community. *In:* Wellman, B. (ed.) *Networks in the Global Village.* Boulder, Colorado: Westview Press.
West, A., Lewis, J. & Currie, P. 2009. Students' Facebook 'friends': public and private spheres. *Journal of Youth Studies,* 12,6, 615 - 627.
Westin, A. 1967. *Privacy and Freedom,* New York, Atheneum.
Westin, A. & Harris Louis, A. 1996. Equifax-Harris Consumer Privacy Survey. Conducted for Equifax Inc.

Whitaker, D. J. & Miller, K. S. 2000. Parent-Adolescent Discussions about Sex and Condoms: Impact on Peer Influences of Sexual Risk Behavior. *Journal of Adolescent Research,* 15,2, 251-273.

White, H. R., Johnson, V. & Buyske, S. 2000. Parental modeling and parenting behavior effects on offspring alcohol and cigarette use: a growth curve analysis. *Journal of Substance Abuse,* 12,3, 287-310.

Whitman, M. 2003. Enemy at the gate: Threats to Information Security. *Communications of the ACM,* 46,8, 91-95.

Widyanto, L. & Griffiths, M. 2006. 'Internet Addiction': A Critical Review. *Int J Ment Health Addict,* 4,1, 31–51.

Wilcox, B. L., Kunkel, D., Cantor, J., Dowrick, P., Linn, S. & Palmer, E. 2004. Report of the APA Task Force on Advertising and Children. Washington DC: American Psychological Association.

Willard, N. 2007. Educator's Guide to Cyberbullying and Cyberthreats. Center for Safe and Responsible Use of the Internet.

Willmott, H. 1993. Breaking the Paradigm Mentality. *Organization Studies (Walter de Gruyter GmbH & Co. KG.),* 14,5, 681.

Wilson, J. L., Peebles, R., Hardy, K. K. & Litt, I. F. 2006. Surfing for Thinness: A Pilot Study of Pro–Eating Disorder Web Site Usage in Adolescents With Eating Disorders. *Pediatrics,* 118,6, e1635-e1643.

Wilson, K., Fornasier, S. & White, K. M. 2010. Psychological predictors of young adults': use of social networking sites. 13,2, 173-177.

Winkler, T. & Buckner, K. 2006. Receptiveness of Gamers to Embedded Brand Messages in Advergames. *Journal of Interactive Advertising,* 7,1, 24-32.

Winzelberg, A. J., Classen, C., Alpers, G. W., Roberts, H., Koopman, C., Adams, R. E., Ernst, H., Dev, P. & Taylor, C. B. 2003. Evaluation of an internet support group for women with primary breast cancer. *Cancer,* 97,5, 1164-1173.

Wise, K., Bolls, P. D., Kim, H., Venkataraman, A. & Meyer, R. 2008. Enjoyment of Advergames and Brand Attitudes: The Impact of Thematic Relevance *Journal of Interactive Advertising,* 9,1.

Withers, K. & Sheldon, R. 2008. Behind the Screen: the hidden life of youth online. Institute for Public Policy Research (IPPR).

Wolak, J., Mitchell, K. & Finkelhor, D. 2006. Online victimization of youth: Five years later. Alexandria, VA.: National Center for Missing & Exploited Children.

Wolak, J., Mitchell, K. J. & Finkelhor, D. 2003. Escaping or connecting? Characteristics of youth who form close online relationships. *Journal of Adolescence,* 26,1, 105-119.

Worsley, A. & Scott, V. 2000. Consumers' concerns about food and health in Australia and New Zealand. *Asia Pacific Journal of Clinical Nutrition,* 9,1, 24-32.

Worthen, B. 2008. Security is No Match for Chocolate and Good Looking Women. *Wall Street Journal,* April 16, 2008.

Wray, R. & Arthur, C. 2010. Vodafone suspends employee after obscene tweet. *The Guardian,* Saturday 6 February 2010, p.7.

Wright, J. P. & Cullen, F. T. 2001. Parental Efficacy and Delinquent Bahavior: Do Control and Support Matter? *Criminology,* 39,3, 677-706.

Wright, K. 2000. Computer-mediated social support, older adults, and coping. *The Journal of Communication,* 50,3, 100-118.

Yancey, A. K., Siegel, J. M. & McDaniel, K. L. 2002. Role Models, Ethnic Identity, and Health-Risk Behaviors in Urban Adolescents. *Arch Pediatr Adolesc Med,* 156,1, 55-61.

Yang, S. C. & Tung, C.-J. 2007. Comparison of Internet addicts and non-addicts in Taiwanese high school. *Computers in Human Behavior,* 23,1, 79-96.

Ybarra, M. L. 2004. Linkages between Depressive Symptomatology and Internet Harassment among Young Regular Internet Users. *CyberPsychology & Behavior,* 7,2, 247-257.

Ybarra, M. L. & Mitchell, K. J. 2004a. Online aggressor/targets, aggressors, and targets: a comparison of associated youth characteristics. *Journal of Child Psychology & Psychiatry,* 45,7, 1308-1316.

Ybarra, M. L. & Mitchell, K. J. 2008. How risky are social networking sites? A comparison of places online where youth sexual solicitation and harassment occurs. *Pediatrics,* 121,2, E350-E357.

Ybarra, M. L. & Mitchell, K. J. K. J. 2004b. Youth engaging in online harassment: associations with caregiver-child relationships, Internet use, and personal characteristics. *Journal of Adolescence,* 27,3, 319-336.

Yearley, S. 2001. Risk, Sociology and Politics of. *In:* Smelser, N. J. & Baltes, P. B. (eds.) *International Encyclopedia of the Social and Behaviour Sciences.* Oxford: Elsevier.

Yin, R. K. 2003. *Case Study Research, Design and Methods,* Thousand Oaks, Sage Publications.

Youn, S. 2008. Parental Influence and Teens' Attitude toward Online Privacy Protection. *Journal of Consumer Affairs,* 42,3, 362-388.

Young, A. L. & Quan-Haase, A. 2009. Information revelation and internet privacy concerns on social network sites: a case study of facebook. *Proceedings of the fourth international conference on Communities and technologies.* University Park, PA, USA: ACM.

Young Hoon, K. 2005. A Study of Online Transaction Self-Efficacy, Consumer Trust, and Uncertainty Reduction in Electronic Commerce Transaction. *In:* Dan, J. K., ed., 2005. 170c-170c.

Young, K. S. 1996a. Internet Addiction: the emergence of a new clinical disorderI. *CyberPsychology & Behavior,* 1,3, 237-244.

Young, K. S. 1996b. Psychology of Computer Use XL. Addictive Use of the Internet: a Case That Breaks the Stereotype. *Psychological Reports,* 79,3, 899-902.

Young, K. S. 1998. *Caught in the net : how to recognize the signs of Internet addiction--and a winning strategy for recovery /* New York, John Wiley.

Young, K. S. & Rogers, R. C. 1998. The Relationship Between Depression and Internet Addiction. *CyberPsychology & Behavior,* 1,1, 25-28.

Yuen, K. S. L. & Lee, T. M. C. 2003. Could mood state affect risk-taking decisions? *Journal of Affective Disorders,* 75,1, 11-18.

Zajonc, R. B. 1980. Feeling and thinking: Preferences need no inferences. *American Psychologist.,* 35,2, 151-175.

Zaksek, M. & Arvai, J. L. 2004. Toward Improved Communication about Wildland Fire: Mental Models Research to Identify Information Needs for Natural Resource Management. *Risk Analysis,* 24,6, 1503-1514.

Zapf, D., Einarsen, S., Hoel, H. & Vartia, M. 2003. Empirical findings on bullying in the workplace. *In:* Einarsen, S., Hoel, H., Zapf, D. & Cooper, C. (eds.) *Bullying and emotional abuse in the workplace international perspectives in research and practice.* London: Taylor and Francis.

Zhang, J. & Daugherty, T. 2009. Third-Person Effect and Social Networking: Implications for Online Marketing and Word-of-Mouth Communication. *American Journal of Business,* 24,2, 53 - 64.

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

Zimbardo, P. G. 1969. The human choice: Individuation, reason, and order versus deindividuation, impulse, and chaos. . *In:* Arnold, W. J. & Levine, D. (eds.) *Nebraska symposium on motivation.* Lincoln: University of Nebraska Press.

Zuckerman, M. 1979. *Sensation seeking : beyond the optimal level of arousal*, New York, London, Wiley.

Zuckerman, M. 1994. *Behavioral expressions and biosocial bases of sensation seeking*, Cambridge, Cambridge University Press.

Zuckerman, M., Ball, S. & Black, J. 1990. Influences of sensation seeking, gender, risk appraisal, and situational motivation on smoking. *Addictive Behaviors,* 15,3, 209-220.

Zuckerman, M. & Neeb, M. 1980. Demographic influences in sensation seeking and expressions of sensation seeking in religion, smoking and driving habits. *Personality and Individual Differences,* 1,3, 197-206.

Zywica, J. & Danowski, J. 2008. The Faces of Facebookers: Investigating Social Enhancement and Social Compensation Hypotheses; Predicting Facebook™ and Offline Popularity from Sociability and Self-Esteem, and Mapping the Meanings of Popularity with Semantic Networks. *Journal of Computer-Mediated Communication,* 14,1, 1-34.

Appendix A Summary of IS/ICT Studies Examining Risk Perceptions

Author	Theory	Methodology	Sample Size	Type	Age	% Female	Sample Source	Main Research Question and Findings
Organisational Perspective								
BENER, A. B. (2000)	Cultural Theory	Case Study	n/a	Organisation	n/a	n/a	Single Case Study Internet Bank Staff and Customers	To understand how risk perception, trust and credibility relate to each other and how and why all of these concepts are related to information systems security. ● Individuals and institutions developed risk perceptions according to their previous experience, the social and economic climate, their cultural backgrounds and the trust they placed in the messages and their sources.
KEIL, M., WALLACE, L., TURK, D., DIXON-RANDALL, G. & NULDEN, U. (2000)	Decision Theory	Survey	242	Students	24.6 ± 6.1	50%	1 university - undergraduate business students	To examine the relative contribution of two factors that are believed to shape risk perception: probability that a loss will occur and the magnitude of the potential loss and to explore the relative influence of risk perception and risk propensity on decision making within an IS project context ● An individual's risk perception appears to be shaped more by perceived downside potential rather than the actual failure occurring. ● An individual's willingness to pursue a risky project appears to be influenced more by risk perception than by any innate

Author	Theory	Methodology	Sample Size	Type	Age	% Female	Sample Source	Main Research Question and Findings
Organisational Perspective								
COLES, R. & HODGKINSON, G. P. (2008)	Psychometric Paradigm	Survey	57	End-users (organisations)	41.9 ± 9.3	25%	Large DB (2,500 entries) held by KPMG	Gain an understanding of how organisational users of IT conceptualise IT risks in the workplace 6 factor solution was found: ● serious or minor in nature; ● having a high or low probability of occurrence; ● causing a high or low degree of stress; ● deliberate or accidental; ● having an impact on the organisation or on
Users (public) Perspective								
FREWER, L. J., HOWARD, C. & SHEPHERD, R. (1998)	Social construction of risk	Survey	26 227	Public Public	40.7 ± 14.4 39 ± 14	46% 68%	Consumer panel of a research company Local newspaper ad	underlying attitudes to various applications of technology ● Inverse relationship was found between perceived risk and benefits. ● Perceived benefits of IT were high compared with other technologies.
SJÖBERG, L. & FROMM, J. (2001)	Basic risk perception model	Survey	844	Public	Median age 47	50%	Random sample of 1,250 members of the Swedish public.	To provide insight into how the public perceives IT risks, which attitudes they hold and what factors influence these attitudes ● Respondents were positive to IT and were to some extent aware of the risks. ● Risks of IT were seen as more pertinent to others. ● Use of IT was strongly related to general attitude towards computers rather than risk perception.

Author	Theory	Methodology	Sample Size	Type	Age	% Female	Sample Source	Main Research Question and Findings
HUANG, D.-L., RAU, P.-L. P. & SALVENDY, G. (2007)	Psychometric Paradigm	Survey	20 602	Students Public	not given 24.3 ± 5.2	37%	University students Posted on a website	What are the Factors that can influence people's perception of information security ● Six factor model of risk perceptions was generated. ● Factors of Knowledge, Impact, Severity and Possibility had significant effects on the perceived overall danger of the threats.
FURNELL, S. M., BRYANT, P. & PHIPPEN, A. D. (2007)	Not defined	Survey	415	Public	not given	29%	Posted on a website	To asess the security perceptions of personal Internet users ● Although respondents were aware of the threats and used the relevant safeguards, many respondents lacked a deeper knowledge and understanding of these threats and safeguards. ● The majority of users gained their awareness of security threats from informal sources such as family and friends and not from professional services.
CAMPBELL, J., GREENAUER, N., MACALUSO, K. & END, C. (2007)	Optimistic bias	Survey	97	Students	Mean age 18.75	40%	1 university - undergraduate psychology students	Examine the optimistic bias within the context of negative and positive internet events and to explore the various factors that may serve to enhance or diminish optimistic attitudes ● Students believed positive Internet events were more likely to happen to them and negative events were less likely to happen to them compared to the average student. ● Heavy Internet users reported more optimistic bias than did light users. ● Controllability, desirability and personal experience were also significantly correlated with optimistic bias.

Author	Theory	Methodology	Sample Size	Type	Age	% Female	Sample Source	Main Research Question and Findings
DOWLAND, P. S., FURNELL, S. M., ILLINGWORTH, H. M. & REYNOLDS, P. L. (1999)	Not defined	Survey	175	Public and organisations	74% of respondents were under 35	20%	Distributed to organisations and individuals	Assess public awareness of, and attitudes towards, computer crime and abuse; and the influence the media has over individual views and perceptions of computer crime and abuse. ● Media has been successful in terms of informing people about computer crimes but has done a relatively poor job of raising awareness of the possible corrective actions.
PATTINSON, M. & ANDERSON, G. (2007)	Not defined	Survey	111	Students	not given	not given	1 Australian university	To examine how the risk perceptions of computer end-users may be influenced by improving the process of risk communication by embedding symbols and graphics within information security messages. ● No significant difference was found by embedding a graphic.
GOLDSTEIN, S. B., DUDLEY, E. A., ERICKSON, C. M. & RICHER, N. L. (2002)	Not defined	Survey	127	Public	22 - 16	66%	Attending evening education courses (US)	Investigation of the predictors of Y2K anxiety ● Found Y2K particularly anxiety provoking for individuals who generally tend to be anxious, who are strongly religious and who lack a strong desire for control. ● Computer use and age were not significant predictors of Y2K anxiety.
MACGREGOR, D. G. (2003)	SARF	Survey	1032 407	Public Public	18+ not given	 not given	Random sample of US households - Gallup Random sample of US households - Decision Research	Examines retrospectively Y2K using concepts from the social ampflication of risk framework. ● Media reporting tended to lead to a decrease in the perceived security of Y2K problems

Author	Theory	Methodology	Sample Size	Type	Age	% Female	Sample Source	Main Research Question and Findings
GUTTELING, J. M. & KUTTSCHREUTER, M. T. (2002)	Psychometric Paradigm	Survey	253 91	Public Experts	21 - 83 22 - 69	37% 7%	Random sample of 1574 Dutch households Sample of 328 experts in universities	Examines the role of expertise in risk communication of the millennium bug ● Respondents did not perceive the millennium bug to be a major threat ● Laypeople were more worried, saw the issue as more personally risky and thought that the levels of public awareness were higher than those predicted by experts
KUTTSCHREUTER, M. & GUTTELING, J. M. (2004)	Psychometric Paradigm	Survey	286 275	Public Public	 18 - 93	 36%	Random sample of 1574 Dutch households Random sample of 1540 Dutch households	Examine perceived risks related to the Y2K problem 10 months and a few weeks before the Millennium ● Risk perceptions decreased significantly ● a significant increase in the perceived risk mitigation at an individual and societal level ● a significant increase in public awareness ● a significant decrease in the need for information

Appendix B Summary of Internet Shopping Studies Examining Risk Perceptions

Author	Methodology	Sample Size	Type	Age	% Female	Sample Source	Main Findings (Perceived Risk)
MCKNIGHT, D. H., CHOUDHURY, V. & KACMAR, C. (2002)	Experiment & Survey	1,403	Students	20.7 ± 3.7	56%	3 Large Universities	Perceived Internet risk negatively affects consumer intentions to transact with a web-based vendor.
GRAZIOLI, S. & JARVENPAA, S. L. (2000)	Experiment & Survey	80	Students	Not given	27%	1 US University - MBA Students	Trust moderates perceived risk. A high level of trust makes consumers less sensitive to risk considerations.
JARVENPAA, S. L., TRACTINSKY, N. & VITALE, M. (2000)	Experiment & Survey	184	Students	Mean Age 22.35	36%	Undergraduate and MBA students in Australia	Higher consumer trust towards an Internet store will reduce the perceived risk associated with buying from that store.
PAVLOU, P. A. (2003)	Exploratory Survey Confirmatory Survey	103 155	Students Online Users	Mean Age 21 Not Given	43% Not Given	1 University Students Randomly collected from Web	Trust and perceived risk a shown to be direct antecedents of intention to transact.
VAN DER HEIJDEN, H., VERHAGEN, T. & CREEMERS, M. (2003)	Survey	228	Students	19-24	28%	Undergraduate students - Holland	Perceived risk and perceived ease-of-use are antecedents of attitudes towards online purchasing. The data did not support a positive effect from trust in the online store and from the perceived usefulness of the website.
LIU, X. & WEI, K. K. (2003)	Survey	308	Students	Not given	Not given	University Students	When considering purchasing goods over the Internet, consumers' decisions are more strongly influenced by their perceptions of risk. In contrast, when considering purchasing services, consumers' decisions are more strongly influenced by their perceptions of ease of use.

Author	Methodology	Sample Size	Type	Age	% Female	Sample Source	Main Findings (Perceived Risk)
TAN, S. J. (1999)	Survey	179	Students	Not given	72%	Undergraduate Students - Singapore	Consumers with a higher degree of risk aversion tend to perceive Internet shopping to be a risky activity
FORSYTHE, S. M. & SHI, B. (2003)	Survey	179	Online Users	11-50+	31%	641self-selecting sample from an online web survey in 1998 (http://www.cc.gatech.edu/gvu/user_surveys/survey-1998-10/)	Although Internet shoppers perceive several risks, these risks do not influence Internet patronage behaviours among current Internet shoppers in an extensive and systematic way. Perceived risk has a greater impact on potential Internet shoppers rather than current Internet shoppers.
FEATHERMAN, M. S. & PAVLOU, P. A. (2003)	Exploratory Survey Confirmatory Survey	214 181	Students Students	Not given	Not given	Undergraduate Students	Perceived risk was found to exert a strong inhibiting influence on TAM's criterion variables. Performance-related risk facets (time risk, privacy risk, financial risk) proved to be the most salient concerns for this study.
LU, H.-P., HSU, C.-L. & HSU, H.-Y.	Survey	1,259	Online Users	Not given	38%	Users of an online anti-virus application	Perceived risk indirectly impacts intentions to use an online antivirus application.
MIYAZAKI, A. D. & FERNANDEZ, A. (2001)	Survey	162	Internet Users	Mean age 34.5	48%	Large airport	Higher levels of Internet experience and the use of other remote purchasing methods are related to lower levels of perceived risk towards online shopping.
LIEBERMANN, Y. & STASHEVSKY, S. (2002)	Survey	465	Employed Adults	Mean age 37	42%	Israelis from a number of organisations	Two perceived risks: Internet credit card stealing and supplying personal information had a crucial effect on current and potential e-commerce usage
GABRIEL, I. J. & NYSHADHAM, E. (2008)	Survey	153	Online Consumers	Mean age 37	42%	Subjects drawn from a panel maintained by a market research company	They found that subjects distinguished online shopping risks using four dimensions: direness of consequences, ability to control or avoid risks, observability/immediacy of risk consequences and unfamiliarity of risks. The top five risky hazards identified by the study were: identity theft; unauthorised use of credit or debit cards; theft of a customer's login information; unauthorised use of consumers' personal data and dealing with a fake web site.

Appendix C Summary of Adolescent/Emerging Adult Studies Examining Risk Perceptions

		Risks Examine		Characteristics Examined														Demographics			
Author	**Theory**	**Reckless Behaviours (N)**	**Socially accepted risks (N)**	**Percieved risk to self**	**Percieved risk to others**	**Control over risk**	**Benefits vs Risks**	**Seriousness of effects**	**Knowledge about risk**	**Parental influence**	**Peer Influence**	**Engagement in behaviour**	**Invulnerability**	**Optimism bias**	**Affect**	**Sensation seeking**	**Other**	**Age**	**Gender**	**Ethnicity**	**Other**
BENTHIN, A., SLOVIC, P. & SEVERSON, H. (1993)	Psychometric Paradigm	12	18	✓	✓	✓	✓	✓	✓		✓	✓					Old/new risk Avoidability	✓	✓		
SMITH, A. M. A. & ROSENTHAL, D. A. (1995)	Psychometric Paradigm	10		✓	✓	✓	✓			✓	✓							✓	✓		Type of school
HAMPSON, S. E., SEVERSON, H. H., BURNS, W. J., SLOVIC, P. &	Psychometric Paradigm	10	6	✓	✓	✓	✓			✓	✓	✓				✓	Avoidability Ego control Independence Acievement	✓	✓		
CURRY, L. A. & YOUNGBLADE, L. M. (2006)	Psychometric Paradigm & Affect Heuristic	6		✓			✓	✓				✓			✓		Anger Depression Self-restraint	✓	✓	✓	Household composition Family size Family income
BENTHIN, A., SLOVIC, P., MORAN, P., SEVERSON, H., MERTZ, C. K. & GERRARD, M. (1995)	Affect heuristic	8					✓					✓			✓			✓	✓	✓	

		Risks		Characteristics Examined														Demographics			
Author	**Theory**	**Reckless Behaviours (N)**	**Socially accepted risks (N)**	**Percieved risk to self**	**Percieved risk to others**	**Control over risk**	**Benefits vs Risks**	**Seriousness of effects**	**Knowledge about risk**	**Parental influence**	**Peer Influence**	**Engagement in behaviour**	**Invulnerability**	**Optimism bias**	**Affect**	**Sensation seeking**	**Other**	**Age**	**Gender**	**Ethnicity**	**Other**
COHN, L. D., MACFARLANE, S., YANEZ, C. & IMAI, W. K. (1995)	Not defined	19	9	✓								✓		✓				✓	✓		
GERRARD, M., GIBBONS, F. X., BENTHIN, A. C. & HESSLING, R. M. (1996)	Not defined	3		✓	✓						✓	✓					Avoidance	✓	✓		
MILLSTEIN, S. G. & HALPERN-FELSHER, B. L. (2002)	Probability assessments of risk	10		✓								✓	✓					✓	✓	✓	Parental education
GOLDBERG, J. H., HALPERN-FELSHER, B. L. & MILLSTEIN, S. G. (2002)	Probability assessments of risk	2		✓			✓					✓						✓	✓	✓	
LAVERY, B., SIEGEL, A. W., COUSINS, J. H. & RUBOVITS, D. S. (1993)	Decision Theory	23		✓			✓					✓	✓				Social maladjustment and personal beliefs and attitudes	✓	✓	✓	

		Risks		Characteristics Examined														Demographics			
Author	**Theory**	**Reckless Behaviours (N)**	**Socially accepted risks (N)**	**Percieved risk to self**	**Percieved risk to others**	**Control over risk**	**Benefits vs Risks**	**Seriousness of effects**	**Knowledge about risk**	**Parental influence**	**Peer Influence**	**Engagement in behaviour**	**Invulnerability**	**Optimism bias**	**Affect**	**Sensation seeking**	**Other**	**Age**	**Gender**	**Ethnicity**	**Other**
BEYTH-MAROM, R., AUSTIN, L., FISCHHOFF, B., PALMGREN, C. & JACOBS-QUADREL, M. (1993)	Decision Theory	6		✓								✓						✓	✓		Parental education
HALPERN-FELSHER, B. L. & CAUFFMAN, E. (2001)	Decision Theory		3	✓			✓				✓							✓	✓	✓	Parental education
GULLONE, E. & MOORE, S. (2000)	Not defined	73		✓								✓					Five factor model of personality	✓	✓		
PARSONS, J. T., SIEGEL, A. W. & COUSINS, J. H. (1997)	Theory of reasoned action	18		✓			✓					✓						✓	✓	✓	
BRADLEY, G. & WILDMAN, K. (2002)	Not defined	14	4	✓							✓	✓				✓	Social desirability	✓	✓		Employment Education Relationship
TEESE, R. & BRADLEY, G. (2008)	Not defined	15		✓			✓				✓	✓					Disinhibition Social Desirability	✓	✓		Education Relationship status

Table C.1 Summary of Theories and Risk Characteristics from Studies Examining Risk Perceptions in Adolescents and Emerging Adults

Author	Methodology	Sample Size	Type	Age	% Female	Sample	Main Findings (Perceived Risk)
BENTHIN, A., SLOVIC, P. & SEVERSON, H. (1993)	Survey	41	Adolescents	14-18	60%	Voulunteers from 2 US high schools	Adolescents who participated in an activity perceived the risks to be smaller, better known and more controllable than did non participants. Participants also perceived greater benefits relative to risks, greater peer pressure to engage in the activity and a higher rate of participation by others.
SMITH, A. M. A. & ROSENTHAL, D. A. (1995)	Survey	650	Adolescents	12-17	53%	13 Australian Schools	Factor analyses consistently found a distinction between high and low risk activities. The factor analysis identified three second order factors: the inherent danger; the trade off between pleasure and peer approval and locus of control. There was significant variation in item ratings within domains with respect to sex, age and type of school attended.
HAMPSON, S. E., SEVERSON, H. H., BURNS, W. J., SLOVIC, P. & FISHER, K. J. (2001)	Survey	382	Adolescents	14-18	52%	1 US high school	Adolescents perceptions of the risk and benefits of alcohol-related activities are associated with their willingness to participate in the activity. Higher participation was associated with the perception of greater benefits and fewer risks.
CURRY, L. A. & YOUNGBLADE, L. M. (2006)	Survey	290	Adolescents	14-20	60%	Random sample from 28,000 in Florida Healthy Kids Programme	Anger and perception of risk directly predicted risk behaviour. The association between risk perception and risk behaviour was stronger for older than younger adolescents.
BENTHIN, A., SLOVIC, P., MORAN, P., SEVERSON, H., MERTZ, C. K. & GERRARD, M.	Survey	411	Adolescents	14-20	47%	1 US high school	Participants in an activity were far more likely than nonparticipants to associate that activity with positive outcomes, concepts and affect and less likely to produce negative associations.

Author	Methodology	Sample Size	Type	Age	% Female	Sample	Main Findings (Perceived Risk)
GERRARD, M., GIBBONS, F. X., BENTHIN, A. C. & HESSLING, R. M. (1996)	Survey - 3 year longitudinal study	477	Adolescents and Parents	13-16	51%	Rural area in US	Results indicated that health cognitions predict risk behaviour. Increases in risk behaviour are accompanied by increases in perceptions of vulnerability and prevalence and by decreases in concern about the risk.
COHN, L. D., MACFARLANE, S., YANEZ, C. & IMAI, W. K. (1995)	Survey	376 160	Adolescents Parents	13-18	50%	1 US medical practice	Compared with adults, teenagers minimized the perceived risk of experimental and and occasional involvement in health threatening activities. Teenagers were less optimistic than about avoiding injury and illness than were their parents and teenagers at greatest risk were the least optimistic about avoiding them.
MILLSTEIN, S. G. & HALPERN-FELSHER, B. L. (2002)	Survey	433 144	Adolescents Young adults	10-15 20-30	50% 60%	6 US schools 3 universities	Adolescents were less likely than than were young adults to see themselves as invulnerable. Individuals perceptions about the magnitude of their personal risk for experiencing negative outcomes showed an inverse relationship to age.
GOLDBERG, J. H., HALPERN-FELSHER, B. L. & MILLSTEIN, S. G.	Survey - longitudinal study	395	Adolescents	10-16	55%	13 US schools	Perceptions of the benefits with alcohol and tobacco were significantly related to behaviour over and above perceptions of risk, age of repondent and experience level.
LAVERY, B., SIEGEL, A. W., COUSINS, J. H. & RUBOVITS, D. S. (1993)	Survey	80	Adolescents	11-17	59%	US counselling clinics	Both benefit and risk perceptions were significantly correlated with risk involvement (in opposite directions). Egocentrism measures were not significantly related to risk involvement or risk and benefit perceptions.
QUADREL, M. J., FISCHHOFF, B. & DAVIS, W. (1993)	Survey	86 86 95	Low risk adolescents Parents High risk adolescents	11-18	67% 23%	US public schools US group homes	All 3 groups saw themselves as facing somewhat less risk than the target others. This perception of relative invulnerability was no more pronounced for adolescents than adults.

Author	Methodology	Sample Size	Type	Age	% Female	Sample	Main Findings (Perceived Risk)
BEYTH-MAROM, R., AUSTIN, L., FISCHHOFF, B., PALMGREN, C. & JACOBS-QUADREL, M. (1993)	Survey	199 199	Adolescents Parents	12-18	75%	Various - scouts, sports teams etc	Response patters related to opportunities to engage in risky behaviours were similar for adolescents and adults.
HALPERN-FELSHER, B. L. & CAUFFMAN, E.	Survey	149 33	Adolescents Young adults	11-18 23.4±6.4	60% 80%	US Schools Unspecified	Adolescents and adults decision making competence differs with adults outperforming adolescents.
GULLONE, E. & MOORE, S. (2000)	Survey	459	Adolescents	11-18	48%	4 Australian Schools	Younger adolescents and girls generally reported engaging in risky behaviours less frequently than older adolescents and males. Risk judgements, personality factors, age and sex were found to be significant predictors of risk behaviours
PARSONS, J. T., SIEGEL, A. W. & COUSINS, J. H. (1997)	Survey	187	Late Adolescent	17-20	54%	1 US university	Among late adolescents perceived benefits are better determinants of behaviour change for risk-taking behaviours than are perceived risks. Both perceived benefits and perceived risks are important determinants of behavioural intentions.
BRADLEY, G. & WILDMAN, K. (2002)	Survey	326 54	College students Non students	18-25	54%	Australian University Convenience sample	Risk behaviours were found to be reliably predicted by sensation seeking but not by antisocial peer pressure, the reverse pattern of association was evident for reckless behaviours.
TEESE, R. & BRADLEY, G. (2008)	Survey	240	College students	18-25	60%	1 Australian University	Controlling for gender, relationship status and social desirability, impulsivity predicted reckless substance abuse and sexual practices, peer pressure predicted reckless substance abuse, perceived risk predicted reckless driving and perceived benefits predicted all three recklessness types.

Table C.2 Summary of Samples from Studies Examining Risk Perceptions in Adolescents and Emerging Adults

Appendix D Risk Characteristics Examined in ICT/IS Studies and Adolescent Studies Using the Psychometric Paradigm

		Voluntariness	Immediacy	Known to exposed	Known to science/experts	Controllability	Newness	Chronic	Common/dread	Severity of consequences	Personal risk	Frequency	Liklehood	Stress/Worry/Fear/Affect	Accidental/deliberate	Recovery	Technology/human cause	Costs	Individual/organisational effects	Effects contained within/outside organisation	Embarrassment	Reputation	Familiarity	Understanding	Observability	Ease of reduction	Preventive control	Media attention	Accident history	Reversability	Duration of Impacts	Scope of impacts	Predictability	Societal risk	Attention	societal acceptability	Unfair and immoral	Warning	Risk to peers	Benefits vs Risks	Information value	Peer influence	Admiration of peers	Need for regulation	Avoidabilty	Perceived Participation	Ease of doing	Parental upset	TOTAL
Original Psychometric Studies																																																
FISCHHOFF, B., SLOVIC, P., LICHTENSTEIN, S., READ, S. & COMBS, B. (1978)	How Safe is Safe Enough? A Psychometric Study of Attitudes Toward Technological Risks and Benefits	x	x	x	x	x	x	x	x	x	x																																				9
ICT Psychometric Studies																																																
COLES, R. & HODGKINSON, G. P. (2008)	'A Psychometric Study of Information Technology Risks in the Workplace.'									x	x	x	x	x	x	x	x	x	x	x	x	x																										13
HUANG, D.-L., RAU, P.-L. P. & SALVENDY, G. (2007)	A Survey of Factors Influencing People's Perception of Information Security	x	x	x		x	x	x		x	x		x										x	x	x	x	x	x	x	x	x	x	x													20
GUTTELING, J. M. & KUTTSCHREUTER, M. T. (2002)	'The role of expertise in risk communication: laypeople's and expert's perception of the millennium bug risk in The Netherlands.'			x	x						x		x	x																			x												6

		Voluntariness	Immediacy	Known to exposed	Known to science/experts	Controllability	Newness	Chronic	Common/dread	Severity of consequences	Personal risk	Frequency	Likelihood	Stress/Worry/Fear/Affect	Accidental/deliberate	Recovery	Technology/human cause	Costs	Individual/organisational effects	Effects contained within/outside organisation	Embarrassment	Reputation	Familiarity	Understanding	Observability	Ease of reduction	Preventive control	Media attention	Accident history	Reversability	Duration of Impacts	Scope of impacts	Predictability	Societal risk	Attention	societal acceptability	Unfair and immoral	Warning	Risk to peers	Benefits vs Risks	Information value	Peer influence	Admiration of peers	Need for regulation	Avoidabilty	Perceived Participation	Ease of doing	Parental upset	TOTAL
KUTTSCHREUTER, M. & GUTTELING, J. M. (2004)	'Time will tell: changes in risk perception and the processing of risk information about the Y2K-risk.'										x		x	x																			x														4
GABRIEL, I. J. & NYSHADHAM, E. (2008)	A Cognitive Map of People's Online Risk Perceptions and Attitudes: An Empirical Study		x	x		x	x		x	x								x						x	x	x							x	x	x	x										14
Adolescent Psychometric Studies																																																
BENTHIN, A., SLOVIC, P. & SEVERSON, H. (1993)	'A Psychometric study of adolescent risk perception.'			x		x	x			x	x			x																								x	x	x	x	x				14
SMITH, A. M. A. & ROSENTHAL, D. A. (1995)	'Adolescents' perceptions of their risk environment.'					x					x																											x	x			x				x	6
HAMPSON, S. E., SEVERSON, H. H., BURNS, W. J., SLOVIC, P. & FISHER, K. J. (2001)	'Risk perception, personality factors and alcohol use among adolescents.'					x					x																											x	x		x	x			x	x	9
CURRY, L. A. & YOUNGBLADE, L. M. (2006)	'Negative affect, risk perception, and adolescent risk behavior.'									x	x																												x								3

Appendix E Typologies of Research Paradigms

Burrell and Morgan (1979) developed an influential typology of paradigms for the analysis of social and organisational theory. They compared the paradigms on the basis of ontological, epistemological, human nature and methodological assumptions. By identifying different assumptions concerning the nature of science and the nature of society, they developed a matrix composed of four different research paradigms. The four different research paradigms defined by Burrell and Morgan are functionalism, interpretivism, radical structuralism and radical humanism and are summarised in Figure E.1 below.

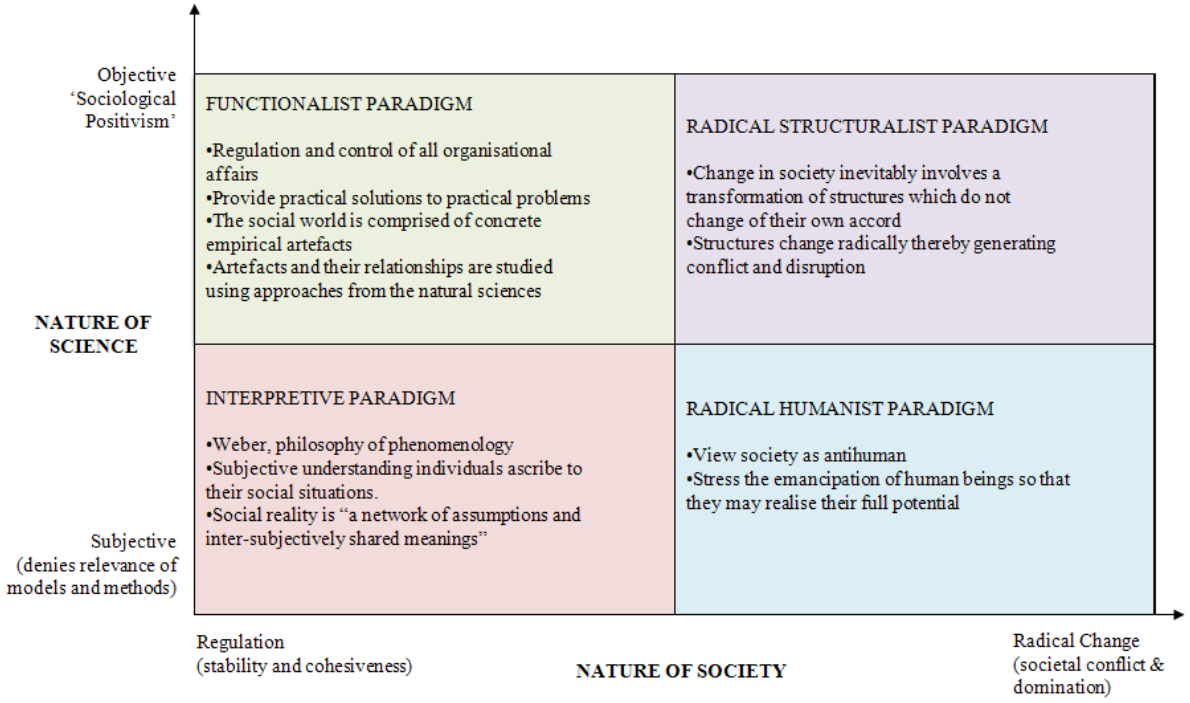


Figure E.1 Summary of Burrell and Morgan's Four Paradigms.

According to Willmott (1993) one of the most significant contributions of the Burrell and Morgan framework has been to highlight alternative approaches to the study of organisations and to encourage researchers to move away from the dominant functionalist "positivist" paradigm. This framework is not without its critics, it is seen by some as over simplistic and incapable of dealing with the subtleties of social theories (Hopper and Powell, 1985, Chua, 1986). A further and more serious problem with the framework is that Burrell and Morgan maintain that the four paradigms are mutually exclusive and that researchers cannot operate using more than one paradigm at any given time, this is known as "*paradigm incommensurability*".

The second typology commonly cited in IS research is proposed by Guba and Lincoln (2005). This typology compares five paradigms: positivism, post-positivism, critical theory, constructivism and participatory. Apart from comparing the paradigms by the standard epistemological, ontological and methodological means, they also compared the paradigms with respect to the nature of knowledge, how knowledge is accumulated, goodness or quality criteria, values, ethics, researcher position and the training needs.

The third typology suggested by Orlikowski and Baroudi (1991) specifically addresses IS research. Orlikowski and Baroudi examined three distinct epistemological categories: positivist, interpretive and critical. They too contrasted the paradigms from ontological, epistemological and methodological viewpoints but also included beliefs about human rationality, social relations and the relationship between theory and practice.

All three typologies include the positivist/post-positivist (called a functionalist paradigm by Burrell and Morgan) and the interpretive (termed constructivism by Guba and Lincoln) paradigms. Both Orlikowski & Baroudi and Guba & Lincoln include critical theory, it could be argued that the radical paradigms suggested by Burrell and Morgan have some similar traits to critical theory as they espouse transformation and emancipation

Appendix F Research Paradigms

F.1 Positivism and Post-positivism

The concept of positivism was first coined by French philosopher Auguste Comte (1875). Positivists assume that reality is objectively given and can be described by measurable properties which are independent of the researcher and their research instruments (Avison and Myers, 2005). Easterby-Smith *et al.* (2002, p28) state that "*the key idea of positivism is that the social world exists externally and that its properties can be measured through objective methods rather than being inferred subjectively through sensation, reflection or intuition*". Being a positivist therefore implies that "*the researcher is working with an observable social reality and that the end product of such research can be the derivation of laws or law-like generalisations similar to those produced by the physical and natural scientists*" (Remenyi *et al.*, 1998, p32). Positivism is also known as the "*natural science model of social science research"* (Lee *et al.*, 1997, p3).

Other components of positivism are:

1. Positivists accept *the unity of the scientific method*. This means that the accepted approach for knowledge acquisition (the scientific method) is valid for all forms of inquiry regardless of the domain of study.
2. The research is undertaken, as far as possible, in a *value-free* way, the choice of what to study and how to study it can be determined by objective criteria rather than by human beliefs and interests;
3. The researcher is *independent* of the research subject and can neither affect or be affected by the subject of research;
4. Positivists emphasise *deductive logic* in their research, i.e. research starts from a general theory or conceptual framework from which observable consequences are deduced.
5. Positivists contend that *uni-directional cause-effect relationships* exist that are capable of being identified and tested via *hypothetic-deductive logic and analysis*. Positivist studies often use existing theories to develop hypotheses (but not exclusively, as otherwise there would be no new theories). These hypotheses are tested and then confirmed or refuted, which leads to further development of the theory which then may be tested by further research;

6. The positivist methodology is concerned with the empirical testability of theories and these theories are *verified* or *falsified*.
7. The positivist researcher places an emphasis on *quantifiable observations* that are suitable for statistical or mathematical analysis;
8. Positivists contend that problems as a whole are better understood if they are *reduced* into the simplest possible elements;
9. In order to be able to *generalise* about irregularities in human and social behaviour it is necessary to select samples of sufficient size from which statistical inferences may be drawn about the wider population.

Burrell and Morgan's (1979) functionalist paradigm most closely matches that of positivism. They assert that functionalists assume the social world to be composed of concrete empirical artifacts and these artifacts can be studied using approaches derived from natural science. Orlikowski and Baroudi (1991) classified IS studies as positivist if there was evidence of formal propositions, quantifiable measures of variables, hypotheses testing and the drawing of inferences about a phenomenon from the sample to a stated population.

From an ontological point of view, positivists assume that reality is external and objective. They believe that an objective physical and social world exists, independent of humans, which can be apprehended, characterized and measured (Orlikowski and Baroudi, 1991). On an epistemological level, positivists assert that knowledge is only of significance if it is based on observations of this external reality. The researcher plays a passive, neutral role in the investigation and does not intervene in the phenomenon of interest. From a human nature viewpoint, positivists view humans as deterministic (humans are products of their environment) and passive. The positivist methodology is concerned with the empirical testability of theories and these theories are "verified" or "falsified". Sample surveys and controlled experiments are the primary data collection techniques and inferential statistics is the data analysis method typically used to "discover" causal laws. The validity and reliability of these methods are crucial.

A number of authors (Burrell and Morgan, 1979, Chua, 1986, Orlikowski and Baroudi, 1991) have discussed the limitations of the positivist research perspective. Its limitations include:

1. It offers a narrow epistemology if everything has to be based on direct observation;

2. It is impossible for research to be completely value-free as a positivist researcher will choose the issue to study, the research objectives, the method of research and the data collected;
3. It is regarded as having a reliance on quantitative data and thus disregards other forms of knowledge that cannot be so easily converted into numerical data;
4. It is geared towards testing theories and is less suited to building theories;
5. As numerical data is not as contextually or socially rich as "soft" data such as words and pictures, it is less powerful when it comes to gaining insight from data;
6. Positivist studies are rooted in the status quo and tend to disregard the historical context of phenomena.

In IS research, positivism has come under increasing criticism as some researchers feel that it isn't a appropriate epistemology for IS research (Hirschheim, 1992, Walsham, 1995, Remenyi *et al.*, 1998). Remenyi *et al.* (1998) contend that positivism is not an approach that will lead to profound or interesting insights into complex problems such as those presented in the IS field. Insights into the complex social world are lost if this complexity is reduced to a series of "*laws*" in the same way as the physical sciences. Walsham (1995) argues that interpretivism is a valuable approach for studying IS in organisations and is a better approach than positivism, especially when researchers are examining the social aspects of IS.

F.2 Interpretivism

Many researchers do not agree with the assumption in positivist research that reality is external and objective, but assert that reality is socially constructed and given meaning by people. This has led to alternative epistemologies such as interpretivism. Interpretivists maintain that the methods of natural science are inadequate for social science. Interpretive studies assume that researchers create and associate their own subjective meanings as they interact with the world around them (Orlikowski and Baroudi, 1991). Interpretive studies generally attempt to understand phenomena through the meanings that people assign to them, and interpretive methods of research in IS are "*aimed at producing an understanding of the context of the information system, and the process whereby the information system influences and is influenced by the context*" (Walsham, 1993, p4-5).

The major propositions of interpretivism are:

1. Interpretive studies reject the possibility that "objective" data can be collected by the researcher and instead suggest a *relativistic, shared, understanding of phenomena*;
2. The researcher has to adopt an *empathetic* stance in order to understand the world from a research subject's point of view;
3. The researcher and the object of research are assumed to be *interactively linked* so that the findings are literally created as the investigation proceeds, this means that value-free data cannot be obtained;
4. Interpretivists emphasise *inductive logic*, i.e. the research starts with the data collected from which theories are generated.
5. Instead of the researcher coming to the field with a well-defined set of constructs and instruments with which to measure the social reality, the interpretive researcher attempts to *derive their constructs from the field* by in-depth examination of and exposure to the phenomenon of interest;
6. In interpretative research, generalisation from the study or sample is not sought. Interpretivists argue that *generalisability is not of crucial importance* as the circumstances being studied today may not be applicable in three months time so some of the generalization is lost. Also, if the contexts being studied are unique then generalisation is less valuable.

In contrast to the positivist approach, Orlikowski and Baroudi (1991) classified IS studies as interpretivist if there was evidence of a nondeterministic perspective where the intent of the research was to increase understanding of the phenomenon within cultural and contextual situations; where the phenomenon of interest is examined in its natural setting and from the perspective of the participants and where researchers did not impose their outsider *a priori* understanding of the situation.

There are two different views on the role of the researcher in interpretive studies. The first is a "weak constructionist" view. Here the researcher describes a phenomenon in the words and categories of the actors. In the second, "strong constructionist" view, the researcher is presumed to enact the social reality they are studying.

As already noted, from an ontological point of view, interpretivists assume that reality is socially constructed. Interpretive IS research assumes that the social world is produced and reinforced by humans through their actions and interactions and this social world can only be interpreted. On an epistemological level, interpretive research is subjective and transactional. The researcher and the object of research are assumed to be interactively linked so that the findings are literally created as the investigation proceeds (Guba and Lincoln, 1994). From a human nature viewpoint, interpretivists view humans as voluntarists who have the potential and the ability to influence and change their environment. From a methodological viewpoint, individual constructions can be elicited and refined only through interaction between and among the researcher and respondents. The primary aim is to describe, interpret, analyse and understand the social world from the participant's perspective and any rigid *a priori* researcher-imposed formulations are resisted (Glaser and Strauss, 1967). Interpretivism uses research methods such as those associated with ethnography, participant observation and hermeneutics.

The interpretive research philosophy has also been subject to criticism. The limitations include:

1. The knowledge produced may not be generalisable to other people or settings.
2. It generally takes more time to collect the data when compared to quantitative research;
3. Data analysis is often time consuming;
4. The results are more susceptible to the researcher's personal biases.
5. The interpretive perspective does not address structural conflicts within society and organizations and ignores contradictions, this perspective cannot account for situations where participants accounts of actions and intentions are inconsistent with their actual behaviour (Fay, 1987);
6. The interpretive perspective does not explain historical change, i.e. how a particular social order came to be and how it is likely to change over time (Fay, 1987).

F.3 Critical Research

According to Stahl (2008, p137) research is critical "*when it is motivated by the intention to change social realities and promote emancipation*". There are many similarities between interpretive and critical research, but there are some differentiating characteristics, as pointed out by Stahl and Brooke (2008):

1. Critical research is based on an intention to make a difference. Critical research is not purely descriptive or explanatory but aims to change social reality;
2. Critical researchers hold a deep belief that the current state of the world is unjust and disadvantages many;
3. A major aim of critical research is to promote individual empowerment and emancipation.

Like interpretive researchers, critical researchers believe they need to understand the language of the humans they are studying. However critical researchers depart from their interpretive colleagues in that they believe interpretation of the social world is not enough. Researchers working in the critical tradition do not merely accept the self understanding of participants, but also critically analyse it through the particular theoretical framework which they adopt to do their work (Orlikowski and Baroudi, 1991). Benson (1983) suggests that the role of the critical researcher is always to go beyond mere studying and theorising, to actively affect change in the phenomenon being studied. Heydebrand (1983) extends this even further by suggesting a critical researcher must also be reflective hence transforming not only the object of investigation, but also the researcher. Orilowski and Baroudi (1991) contend however that these components are not seen as an essential component of the critical research agenda. Orilowski and Baroudi classified critical studies as those that showed evidence of a critical stance towards taken for granted assumptions about organizations and IS and a dialectical analysis which attempted to reveal the historical, ideological and contradictory nature of existing social practices.

From an ontological point of view, critical researchers assume that reality is historically and socially constructed. Reality is assumed, to be shaped, over time by social, political, cultural, economic, ethnic and gender factors (Guba and Lincoln, 1994). The epistemological belief of the critical perspective is that knowledge is grounded in social and historical practices (Orlikowski and Baroudi, 1991). From a human nature viewpoint,

critical researchers, similar to interpretivists, view humans as voluntarists who have the potential and the ability to influence and change their environment, but the critical researcher argues that the ability to do so is constrained. From a methodological viewpoint, the transactional nature of inquiry requires a dialogue between the researcher and the subjects of the inquiry, that dialogue must be dialectical in nature (Guba and Lincoln, 1994). The research methods used in critical research include long-term historical studies and critical ethnographic studies of organisational processes and structures.

There can be difficulties in carrying out critical research in business and management studies. One reason is that critical research is based on the work of Habermas and Foucault who are from the Marxist school and is thus seen to be on the political left. As one of the central tenets of critical research is emancipation, it can be perceived to be in disagreement with organizational power structures which are generally geared towards control and not towards emancipation (Stahl and Brooke, 2008).

Critical research methods are also beginning to gain a foothold in IS research, examples include Ngwenyama and Lee (1997), Hirschheim and Klein (1994), Carlsson (2003) and Mingers (2004). Critical research in IS (CRIS) is concerned with the purpose, use and misuse of IS in organizations and society (Cecez-Kecmanovic *et al.*, 2008). CRIS has challenged the assumption that technology innovation is inherently desirable and provides benefits to all (McGrath, 2005). Because of its critical nature, critical research is best suited to topics where there is a perceived injustice, examples in the IS domain include the digital divide, gender issues and also the affect of IS on corporate power structures and on individual work patterns, remuneration and control (Pather and Remenyi, 2004, Stahl and Brooke, 2008). As Walsham (2005) notes, a critical stance is a matter of personal motivation and commitment which is not to everyone's taste.

F.4 Pragmatism

The roots of pragmatism can be traced to the work of authors such as Charles Pierce (1839-1914), William James (1842-1910) and John Dewey (1859-1952). Since the 1960's there has been a resurgence of interest in pragmatism (also known as neo-pragmatism), and includes the work of Rorty (1982, 1991) Rescher (2000) and Putnam (1995). Tashakkori & Teddlie (2003, p713) define pragmatism as "*a deconstructive paradigm that debunks concepts such as "truth and reality" and focuses instead on "what works" as the truth*

regarding the research questions under investigation. Pragmatism rejects the either or choices associated with the paradigms wars, advocates for the use of mixed methods in research, and acknowledges that the values of the researcher play a large role in the interpretation of results." There has been much debate in the academic literature regarding research paradigms and this has become known as the "*paradigm war*" or "*paradigms debate*". Much of the disagreement has been associated with the interpretivist and positivist paradigms, where both sets of researchers view their paradigm as the ideal for research. Pragmatism has attempted to find a middle ground between these two philosophical stances.

Johnson and Onwuegbuzie (2004) suggest that in judging ideas researchers should consider the empirical and practical consequences. In some situations, the qualitative approach will be more appropriate and in other situations the quantitative approach will be more suitable. In many situations, the researcher can combine methods and insights from both approaches to produce a superior product (Johnson and Onwuegbuzie, 2004). Pragmatism offers a philosophical middle position and offers a practical outcome-oriented method of enquiry. The aim of pragmatism is to find a middle ground between the philosophical dogmatism between positivism and interpretivism.

The main characteristics of pragmatism as presented by Johnson and Onwuegbuzie (2004) are as follows:

1. pragmatism rejects traditional dualisms (e.g., nominalism versus realism and free will versus determinism, facts versus values) and posits a more moderate and common sense version of philosophical dualisms based on how well they work in solving problems;
2. it recognises the existence of the natural and physical world as well as the social and psychological world;
3. knowledge is viewed as being both socially constructed and based on the reality of the world we experienced and live in;
4. it endorses fallibilism, i.e. current beliefs and research conclusions are rarely, if ever, viewed as perfect, certain or absolute;
5. it endorses eclecticism and pluralism in that different, even conflicting theories and perspectives can be useful in gaining an understanding of the research question;

6. human inquiry (i.e. what we do in our day-to-day lives as we interact with the environment) is viewed as being analogous to experimental and scientific enquiry;
7. views current truth, meaning and knowledge as tentative and as changing over time and asserts that what we obtain in research should be viewed as provisional truths and absolute Truth (with a capital T) is what will be the "final opinion" perhaps at the end of history;
8. it takes an explicitly value-oriented approach to research;
9. pragmatism prefers action to philosophizing and endorses practical theory (theory that informs effective practice; praxis)

Pragmatic research uses both deductive and inductive logic as proposed by the inductive-deductive research cycle (see Figure F.1). This research cycle is a response to the inductive-deductive dichotomy. It is clear that the cycle involves both inductive and deductive reasoning processes and induction or deduction could come first depending on where a researcher is in terms of studying the phenomenon of interest.

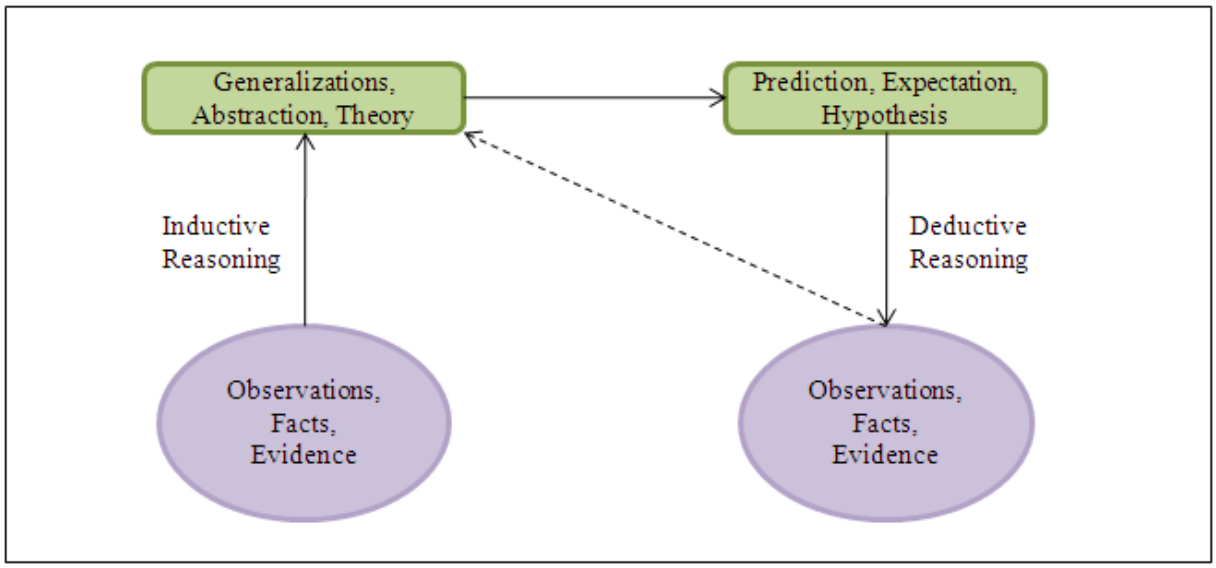


Figure F.1 The Inductive-Deductive Research Cycle (cycle of scientific methodology) (Teddlie and Tashakkori, 2009, p27).

Pragmatism, like all research philosophies, has some limitations. Some believe that it is inappropriate to mix quantitative and qualitative methods due to the fundamental differences in the paradigms underlying those methods (Burrell and Morgan, 1979, Smith, 1983, Guba, 1990). This follows Thomas Kuhn's (1970) argument that competing paradigms were "*incommensurable paradigms*" (also known as the "*incompatibility thesis*").

Appendix G Mixed Method Design Types

Creswell and Plano Clark (2007) have summarised mixed method designs into four major types, the Triangulation Design, the Embedded Design, the Explanatory Design and the Exploratory Design. The following section provides a brief overview of each of these designs and highlights their advantages and disadvantages.

G.1 The Triangulation Design

This is the most common and well-known approach to mixing methods. This purpose of this design is to bring together the differing strengths of quantitative methods (e.g. large sample sizes, trends, generalisations) with those of qualitative methods (e.g. small numbers, in-depth analyses). This design is used when a researcher wants to directly compare and contrast quantitative statistical results with qualitative findings or to validate and expand quantitative results with qualitative data. The triangulation design is a one-phase design in which researchers implement the quantitative and qualitative methods during the same timeframe and with equal weight. The design generally involves the concurrent, but separate, collection and analysis of quantitative and qualitative data and for this reason it has also been referred to as the "*concurrent triangulation design*"(Creswell *et al.,* 2003). The researcher attempts to merge the two data sets, typically by bringing the separate results together in the interpretation or by transforming data to facilitate integrating the two data types during analysis. The advantages of this design are:

- the design makes intuitive sense and it is often the design chosen by researchers that renewed to mixed methods research;
- it is an efficient design in that both types of data are collected during a single phase of research and roughly at the same time;
- each type of data can be collected and analysed separately and independently using the techniques traditionally associated with each data type.

There are some challenges in using this design, these include:

- researchers need expertise in both quantitative and qualitative data collection methods;
- researchers may sometimes find that the quantitative and qualitative results do not agree and they may need collect further data;
- it can be very challenging to integrate the two sets of very different data and present the results in a meaningful way.

G.2 The Embedded Design

This is a mixed method design in which one dataset provides a supportive, secondary role in a study based primarily on the other data type. Researchers use this design when they need to include qualitative or quantitative data to answer a research question within a largely quantitative and qualitative study. The embedded design can use either a one phase or a two phase approach for the embedded data and the quantitative and qualitative data are used to answer different research questions within the study. As an example, Rogers *et al.* (2003) carried out a study to examine patients understanding and participation in a drug trial. They embedded qualitative data within their experimental design in two different ways: before the trial, to inform the development of the treatment and after the trial to explain the treatment results. It can be difficult to differentiate between a study using an embedded design and a study using a different mixed method design. Creswell and Plano Clark (2007) suggest asking whether the results of the secondary data type would be useful or meaningful if they were not embedded within the other data, to see whether the secondary data is only playing a supplemental role within the design. The advantages of the embedded design are:

- it can be useful when a researcher does not have sufficient time or resources to carry out an extensive quantitative and qualitative data collection;
- this design can be appealing to funding agencies because the primary focus of the design is traditionally quantitative.

The difficulties with this design are:

- there are similar difficulties to the triangulation design in integrating results from the two methods, however researchers using an embedded design can keep the two sets of results separate in their reports or even report them in separate papers;
- few examples exist and very little has been written about embedding quantitative data within traditionally qualitative designs.

G.3 The Explanatory Design

The explanatory design is a two phase mixed method design. The overall purpose of this design is that qualitative data helps explain or build upon initial quantitative results (Creswell *et al.*, 2003). This design is well-suited to studies in which the researcher needs qualitative data to explain significant (or non-significant) results. This design starts with the collection and analysis of quantitative data. This first phase is followed by the

subsequent collection and analysis of qualitative data. The second, qualitative phase of the study is designed so that it follows from (or connects to) the results of the first quantitative phase. Because the design begins quantitatively, researchers typically place greater emphasis on the quantitative methods than the qualitative methods. The advantages of this design are:

- this design is considered the most straightforward of the mixed methods designs;
- its two phase structure makes it straightforward to implement because the researcher conducts the two methods in separate phases and collects only one type of data at a time;
- the final report can also be written in two phases, making it straightforward to write and providing a clear delineation for readers;
- this design appeals to quantitative researchers because it often begins with a strong quantitative orientation.

Although this design is straightforward, researchers can still face challenges:

- this design requires a lengthy amount of time for implementing the two phases;
- the researcher has to decide whether to use the same individuals for both phases;
- it can be difficult to secure ethical approval for this design because the researcher cannot specify how participants will be selected for the second phase until the initial findings are obtained;
- the researcher has to decide which quantitative results need to be further explained.

G.4 The Exploratory Design

As with the explanatory design, the aim of the two phase exploratory design is that the results of the first method (qualitative) can help develop or inform the second method (quantitative). This design is particularly useful when a researcher needs to develop and test an instrument because one is not available or identify important variables to study quantitatively when the variables are unknown. Because this design begins qualitatively a greater emphasis is often placed upon the qualitative data. The exploratory design shares many of the same advantages and disadvantages as the explanatory design.

Table G.1 summarises each of the mixed methods design types. In choosing a research design, Creswell and Plano Clark (2007) suggest that the primary concern should be whether the research design matches the research problem. They also suggest that researchers should examine their own expertise and select a design that fits with their area

of expertise. Other considerations include the availability of resources, including the time to conduct the study, the funding resources to enable team work or hiring of research assistants. The audience for the research can also influence the design choice, particularly if the audience values one type of evidence over another.

Design Type	Variants	Timing	Weighting	Mixing	Notation
Triangulation	• Convergence • Data transformation • Validating quantitative data • Multilevel	Concurrent: quantitative and qualitative at the same time	Usually equal	Merge the data during the interpretation or analysis	QUAN + QUAL
Embedded	• Embedded experimental • Embedded correlational	Concurrent or sequential	Unequal	Embed one type of data within a larger design using the other type of data	QUAN (qual) or QUAL (quan)
Explanatory	• Follow up explanations • Participant selection	Sequential: Quantitative followed by qualitative	Usually quantitative	Connect the data between the two phases	QUAN – qual
Exploratory	• Instrument development • Taxonomy development	Sequential: Qualitative followed by quantitative	Usually qualitative	Connect the data between the two phases	QUAL - quan

Table G.1 The Major Mixed Methods Design Types.
Source: (Creswell and Plano Clark, 2007, p85)

Appendix H Ethical Considerations and Documentation

This appendix describes the ethical considerations raised by this study and how they were addressed. It also includes sample documentation.

H.1 Ethical Considerations

Harm

An important consideration with this research was the avoidance of harm (non-maleficence) to the participants. There was a possibility, although unlikely, that the survey, focus group interviews and semi-structured interviews could cause harm and stress to participants. This was because participants were asked to reveal if they had or knew of friends that had encountered any risks on social networking sites or if they had encountered these risks themselves. These risks could include bullying and harassment, encountering disturbing content and stalking. It was necessary to ask participants these questions as it is assumed that experience of risks may imply higher risk perceptions. In case participants were distressed by these disclosures, they were guided to online resources and supports (such as counsellors) in their School, College or work environment.

Informed Consent

It is important with any research project, not to apply any pressure on intended participants to take part in the research. Attaining "*informed consent*" ensures that a participants consent is given freely (voluntary) and is based on full information about participation rights and how their data will be used and stored (Saunders *et al.*, 2007). To achieve this, participants were given *participant information sheets* which fully explained the research study.

As there were a number of phases and cohorts to this study, separate participant information sheets were prepared for the:

1. Questionnaire (College Students & Working Adults)
2. Questionnaire (Parents/Guardians of School Students)
3. Questionnaire (School Students)
4. Focus Group Interview (Parents/Guardians of School Students)
5. Focus Group Interview (School Students)
6. Semi-Structured Interviews (College Students)

These participant information sheets were carefully worded for their intended audience, for example the participant information sheets for school students were designed to be comprehensible by a 12 year old. All six participant information sheets are shown in Section H.2. After participants had read the participant information sheet, they signed a form giving their informed consent. Getting informed consent for the school students (< 18 years old) involved two stages. The first stage was to seek informed consent from their guardians/parents, after this has been attained then the school student could make an informed decision to participate in the study.

A further consideration with informed consent is "*how much information should be given and when*" (Kvale and Brinkmann, 2009, p71). Fully disclosing the purpose or content of the research can bias the results (Ruane, 2005). As the participant information leaflets were sent to the participants prior to conducting this study, the specific purpose of the study was initially withheld in order to obtain the participants spontaneous views and to avoid leading them to specific answers. The study was worded innocuously as "*a research study examining social networking sites*". Full information about the purpose of the research was given to the participants in a debriefing after the survey/interview.

Frankfort-Nachmias and Nachmias (1996) suggest that the level of consent obtained should be related to the risk posed to the participant by the research. As the level of risk posed to participants by this research is low, attaining informed consent in this manner does seem to be over the top. For some researchers the return of a completed questionnaire by a respondent is taken as *implied consent* and they do not seek full informed consent. The problem with implied consent, however, is that participants may not fully understand their rights and this violates the autonomy principle. Some researchers with children suggest that a teacher/principal should be able to give consent in lieu of parental consent. This was not possible as the ethical guidelines of the College stipulated that parents/guardians had to give consent for participants under 18. It has to be recognised, however, that getting informed consent in this manner does, particularly with the school students, significantly reduce the sample size and much of the burden of pursuing and collecting consent forms is placed on the school.

Compensation/Incentives

The issues of whether and how to compensate participants involves questions of both ethics and data quality. On one hand offering incentives can lead to bias by affecting participants responses and increasing participation rates but on the other hand participants can give up a considerable amount of time to participate in a study (Patton, 2002). In order to reduce bias, incentives were not offered to participants in this study. To encourage participation, participants were informed of the value of their contribution to research in this area and were sent copies of the research findings. Students who took part in the focus group interviews were given a small token to thank them for participating in the study but were not informed of this before agreeing to take part. Snacks were made available for all the qualitative interviews.

Anonymity

The essence of anonymity is that information provided by respondents should in no way reveal their identity (Cohen *et al.*, 2007). Anonymity was guaranteed for the survey phase of the study as no identifying information was collected. Only respondent's ages and gender were collected. Anonymity could not be guaranteed at the interview phase of the study. Participants were informed that any personal identifying information would not be included on any documentation relating to the results of this study. Participants would therefore remain anonymous to everyone apart from the researcher and supervisor.

Confidentiality

Confidentiality in research implies that private data identifying the participants will not be disclosed (Kvale and Brinkmann, 2009). In accordance with the Data Protection Act 1998, all informed consent forms were stored in a secure office in a locked filing cabinet which was only accessible by the researcher and supervisor. The focus group interviews and semi-structured interviews were recorded on a digital voice recorder. These audio files were transferred to the researcher's computer and stored in a password protected folder. The audio files were named using a code. A paper record was kept of the interviewee names and the code of their recording. This paper record was kept in the researcher's office in a locked filing cabinet that was only accessible by the researcher and supervisor.

Confidentiality cannot be guaranteed if information is divulged by participants indicating that they or others are at risk of serious harm. It was explained on both the Information

Sheet for School Students and the Information Sheet for Parents/Guardians that information of this nature would be passed to the school principal.

Behaviour and Objectivity of Researcher

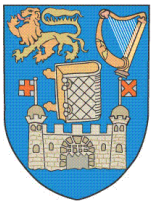
Another ethical principal relates to the maintenance of the objectivity of the researcher. The researcher has to take measures to ensure during the data collection, analysis and reporting phases that the data is collected accurately and subjective selectivity is avoided when reporting the data (Saunders *et al.*, 2007). This relates to the validity and reliability of the research and is discussed in further detail in Section 4.8.

Harm to Researcher

The possibility of harm to the researcher is an important ethical issue which also needed to be considered (Saunders *et al.*, 2007). One aspect of this is related to divulging personal information about the researcher. The participant information leaflet only showed the work e-mail and phone number of the researcher. From a safety point of view, the interviews conducted in schools were conducted in a room close to a central office where a teacher with responsibility for the children could easily see the researcher and the school students. It is recommended that ideally researchers should be accompanied when conducting research outside the College, but this was not feasible due to limited resources.

H.2 Participant Information Sheets

Participant Information Sheet for Questionnaire (College Students & Working Adults)



Trinity College Dublin
School of Computer Science and Statistics

A Study Examining Social Networking Sites

Information Leaflet for College Students

You are being invited to take part in a research study examining social networking sites such as Facebook and Bebo. Before you decide if you wish to take part in this study, it is important that you understand why this study is being conducted and what will be involved. Please take some time to read the following information carefully and discuss it with others if you wish. Please ask if anything is unclear or if you would like more information.

Introduction:

My name is Aideen Keaney. I am a lecturer of Information Systems in the School of Computer Science and Statistics in Trinity College Dublin. I am doing research for a PhD on social networking sites. There are no restrictions for taking part in this study and you don't even have to be a user of social networking sites.

You will not benefit directly from participating in this research, but you will be helping to advance knowledge and understanding of social networking sites.

If you agree to take part in the study:

Your participation in this study is voluntary and you can withdraw from the study at any time.

You have to give your written consent to participate in this study by signing both copies of the Informed Consent Form which is attached. The researcher will keep the original of this form (green copy) and you will also keep a copy.

The study involves filling in a questionnaire. This questionnaire should take between 15 and 20 minutes to complete and can be completed during this lecture slot.

Findings of this study:

If you would like to receive a summary of the findings of this study, please enter your email details on the Informed Consent Form.

Privacy and confidentiality

All information given in this questionnaire is **anonymous** and it is not possible to identify an individual from this questionnaire. The only personal information you will be asked to provide are your gender and your age in years. You will not be asked to give your name on the questionnaire.

As the informed consent forms are collected separately, it will not be possible to match consent forms with questionnaires.

The completed consent forms and questionnaires will be kept in a secure office in a locked filing cabinet that will only be accessible to the researcher.

The questionnaires will be computerised and will be stored on the researcher's computer in a password protected folder.

The consent forms and questionnaires will be stored for the duration of the study, i.e. until the work is fully reported and disseminated. It will then be kept in a locked cabinet for a further five years.

Who has reviewed the study?

This study has been subject to review by the Research Ethics Committee in the School of Computer Science and Statistics, Trinity College Dublin. The study will also be reviewed on a regular basis by supervisors at the School of Computer Science and Statistics, Trinity College Dublin.

Further information

If you have any questions about this research you can ask now or at any point during the study.

Aideen Keaney (01) 896 2199 aideen.keaney@tcd.ie

Some people may find the topics addressed in this study distressing. The following websites and college services will be useful to you if you have any concerns:

Websites

www.makeitsecure.org

www.internetsafety.ie

www.webwise.ie

www.saferinternet.org

College Services

Senior Tutors Office	http://www.tcd.ie/Senior_Tutor/
Bullying and harassment complaints	http://www.tcd.ie/Senior_Tutor/faq/#Q21
Student Counselling Service	http://www.tcd.ie/Student_Counselling/

Trinity College Dublin
School of Computer Science and Statistics

A Study Examining Social Networking Sites

Information Sheet for Parents/Guardians

I would like to ask your permission to allow your child to take part in a research study about social networking sites. This study will take place in school in a few days time. Before you decide if you wish them to take part in this study, it is important that you understand why this study is being conducted and what will be involved.

Introduction:

My name is Aideen Keaney. I am a lecturer of Information Systems in the School of Computer Science and Statistics in Trinity College Dublin. I am doing research for a PhD which aims to develop an understanding of social networking sites. It would help our study if you would allow your child to take part.

Your child will not benefit directly from participating in this research, but their taking part will help to advance the knowledge and understanding of social networking sites.

If you agree to allow your child take part in the study:

Participation in this study is voluntary and your child can withdraw from the study at any time.

The study involves filling in a questionnaire that should take no longer than half an hour to complete. This will be completed in school during a free time period. A member of staff of the school will be in attendance.

Both parents and children have to give their written consent to participate in this study (see Informed Consent Form attached).

Privacy and confidentiality

All information given in the questionnaire is **anonymous** and it will not be possible to identify your child from the questionnaire. The only personal information your child will be

asked to provide is their gender and age in years. They will not be asked to give their name on the questionnaire.

As the Informed Consent Forms will be collected before the questionnaire is given out, it will not be possible to match consent forms with questionnaires.

The completed consent form and questionnaires will be kept in a secure office in a locked filing cabinet that will only be accessible to the researcher and supervisor. The questionnaires will be computerised and will be stored on the researcher's computer in a password protected folder. The consent forms and questionnaires will be stored for the duration of the study, i.e. until the work is fully reported and disseminated. They will then be kept in a locked cabinet for a further five years.

Confidentiality cannot be guaranteed in the unlikely event that a child indicates that they or others are at risk of serious harm. Information of this nature will be passed to the school principal.

Who has reviewed the study?

This study has been subject to review by the Research Ethics Committee in the School of Computer Science and Statistics, Trinity College Dublin. The study will also be reviewed on a regular basis by supervisors at the School of Computer Science and Statistics, Trinity College Dublin.

Contact information

You can get more information or answers to your questions about this study from Aideen Keaney who can be telephoned at 01 896 2199 or by email aideen.keaney@tcd.ie

If you are happy to allow your child take part in this study, can you please sign the Parents/Guardians section on the Informed Consent Form (in green attached)? The student will need to bring the Informed Consent Form with them to class. The student will sign their section, when the study has been explained to them in class, and they are happy to volunteer for the study.

Aideen Keaney. School of Computer Science and Statistics, Trinity College, Dublin 2.
Ph 01 896 2199

Participant Information Sheet for Questionnaire (School Students)

Trinity College Dublin
School of Computer Science and Statistics

A Study Examining Social Networking Sites

Information Sheet for School Students

Would you consider taking part in this study?

My name is Aideen Keaney and I work in Trinity College Dublin.

I am carrying out research to learn about social networking sites such as Facebook and Bebo. It would really help my research if you would answer some questions about social networking sites. Before you decide if you want to take part in this study, it is important that you understand why this study is being conducted and what you will have to do.

The reason I am doing this study is that there is very little research into social networking sites and carrying out this study will help increase the knowledge and understanding of social networking sites.

Do I have to take part?

No you do not; taking part in this study is entirely up to you. If you do take part in the study, you can withdraw at any time.

If I do take part, what do I have to do?

You will need an Informed Consent Form that a parent or guardian has signed. This means that they agree to you taking part in this study. You **also have to agree** to take part and sign the Informed Consent Form. Once you agree to take part in this study, you will be given a questionnaire to complete. It shouldn't take longer than half an hour to fill in and you can complete it during this class time.

Confidentiality

All information given in the questionnaire is **anonymous** which means that it will not be possible to identify you from the questionnaire. The only personal information your will be asked to provide is your gender and age in years.

The completed consent forms and questionnaires will be kept in a secure office in a locked filing cabinet that will only be accessible to the researcher and supervisor. The questionnaires will be computerised and will be stored on the researcher's computer in a password protected folder.

If you indicate that you or others are at risk of serious harm, I will have to tell the school principal.

Further information

If you have any questions about this research you can ask now or during the study.

Aideen Keaney, aideen.keaney@tcd.ie
ph 896 2199

Trinity College Dublin
School of Computer Science and Statistics

A Study Examining Social Networking Sites (Interview)

Information Sheet for Parents/Guardians

I would like to ask your permission to allow your child to take part in a research study about social networking sites. This study will take place in their school. Before you decide if you wish them to take part in this study, it is important that you understand why this study is being conducted and what will be involved.

Introduction:

My name is Aideen Keaney. I am a lecturer of Information Systems in the School of Computer Science and Statistics in Trinity College Dublin. I am doing research for a PhD which aims to develop an understanding of social networking sites. I am asking about 30 people to take part in an interview to examine their views of social networking sites. It would help our study if you would allow your child to take part.

Your child will not benefit directly from participating in this research, but their taking part will help to advance the knowledge and understanding of social networking sites.

If you agree to allow your child take part in the study:

Participation in this study is voluntary and your child can withdraw from the study at any time.

The study involves an interview that should take no longer than an hour. This interview will take place in the school during a free time period.

Both parents and children have to give their written consent to participate in this study (see Informed Consent Form attached). The researcher will keep the original of this form and you will also get to keep a copy.

Privacy and confidentiality

I would like to record the interview on a digital voice recorder. This is because what your child says is important and I want to make sure that I remember what we talked about. What is said in the interview is completely confidential, which means that whatever is discussed or spoken about in the interview will not be told to other people. Confidentiality cannot be guaranteed in the unlikely event that a child indicates that they or others are at risk of serious harm. Information of this nature will be passed to the school principal.

The audio files will be transferred to computer and will be stored on the researcher's computer in a password protected folder. I will do my best to make sure that people are not able to identify your child in the study by giving them a "made up" name (what researchers call a "pseudonym")

Who has reviewed the study?

This study has been subject to review by the Research Ethics Committee in the School of Computer Science and Statistics, Trinity College Dublin. The study will also be reviewed on a regular basis by supervisors at the School of Computer Science and Statistics, Trinity College Dublin.

Contact information

You can get more information or answers to your questions about this study from Aideen Keaney who can be telephoned at 01 896 2199 or by email aideen.keaney@tcd.ie

If you are happy to allow your child take part in this study, can you please sign and date the Parents/Guardians section on <u>both</u> of the Informed Consent Forms (in green attached). The student will need to bring <u>both</u> Informed Consent Forms with them to school on ??. The student will keep one form and the other will be retained by the researcher.

Aideen Keaney. School of Computer Science and Statistics, Trinity College, Dublin 2.
Ph 01 896 2199

Participant Information Sheet for Focus Groups (School Students)

Trinity College Dublin
School of Computer Science and Statistics

A Study Examining Social Networking Sites

Information Sheet for School Students

Would you consider taking part in the second phase of my study?
My name is Aideen Keaney and I work in Trinity College Dublin.

Last term/month you filled in a questionnaire about social networking sites. At the time you said that you would be interested in being involved in the second phase of the study which involves a focus group discussion. Before you decide if you want to take part in this focus group, it is important that you understand why this study is being conducted and what you will have to do.

The reason I am doing this study is that there is very little research into social networking sites and carrying out this study will help increase the knowledge and understanding of social networking sites.

Do I have to take part?
No you do not; taking part in this study is entirely up to you. If you do take part in the study, you can withdraw at any time.

If I do take part, what do I have to do?
You will need an Informed Consent Form that a parent or guardian has signed. This means that they agree to you taking part in this study. You **also have to agree** to take part and sign the Informed Consent Form. A focus group is an informal discussion. If you decide that you would like to take part, I will hold the focus group in your school. The discussion will last about an hour. You will not have to do anything special to prepare for the focus group.

Confidentiality
With your permission I will record the discussion on a digital voice recorder. This is because what you say is important and I want to make sure that I remember what we talk about. I will turn off the recorder at any time if you are not comfortable with it. What you say in the interview is completely confidential, which means that whatever is discussed or spoken about in the interview will not be told to other people except where you indicate that there is an immediate risk of harm to you or another person. Information of this nature will be passed to the school principal.

The audio files will be transferred to computer and will be stored on the researcher's computer in a password protected folder. I will do my best to make sure that people are not able to identify you in the study by giving you a "made up" name (what researchers call a "pseudonym")

Further information
If you have any questions about this research you can ask now or during the study.
Aideen Keaney, aideen.keaney@tcd.ie
ph 896 2199

Trinity College Dublin
School of Computer Science and Statistics

A Study Examining Social Networking Sites (Interview)

Information Leaflet for College Students & Adult Workers

You are being invited to take part in a research study examining social networking sites such as Facebook and Bebo. Before you decide if you wish to take part in this study, it is important that you understand why this study is being conducted and what will be involved. Please take some time to read the following information carefully and discuss it with others if you wish. Please ask if anything is unclear or if you would like more information.

Introduction:

My name is Aideen Keaney. I am a lecturer of Information Systems in the School of Computer Science and Statistics in Trinity College Dublin. I am doing research for a PhD on social networking sites.

I am asking about 30 people to take part in an interview to examine their views of social networking sites. There are no restrictions for taking part in this study and you don't even have to be a user of social networking sites.

You will not benefit directly from participating in this research, but you will be helping to advance knowledge and understanding of social networking sites.

If you agree to take part in the study:

Your participation in this study is voluntary and you can withdraw from the study at any time.

If you decide that you would like to take part, I will hold the interview in your college or workplace at a time that suits you. The interview will last about an hour. You will not have to do anything special to prepare for this interview.

Privacy and confidentiality

With your permission I will record the interview on a digital voice recorder. This is because what you say is important and I want to make sure that I remember what we talk about. I will turn off the recorder at any time if you are not comfortable with it. What you say in the interview is completely confidential, which means that whatever is discussed or spoken about in the interview will not be told to other people except where you indicate that there is an immediate risk of harm to you or another person. If this happens, we will discuss it with you first.

The audio files will be transferred to computer and will be stored on the researcher's computer in a password protected folder. I will do my best to make sure that people are not able to identify you in the study by giving you a "made up" name (what researchers call a "pseudonym")

Who has reviewed the study?

This study has been subject to review by the Research Ethics Committee in the School of Computer Science and Statistics, Trinity College Dublin. The study will also be reviewed on a regular basis by supervisors at the School of Computer Science and Statistics, Trinity College Dublin.

Further information

If you have any questions about this research you can ask now or at any point during the study.

Aideen Keaney (01) 896 2199 aideen.keaney@tcd.ie

Some people may find the topics addressed in this study distressing. The following websites and college services will be useful to you if you have any concerns:

Websites

www.makeitsecure.org

www.internetsafety.ie

www.webwise.ie

www.saferinternet.org

TCD College Services

Senior Tutors Office	http://www.tcd.ie/Senior_Tutor/
Bullying and harassment complaints	http://www.tcd.ie/Senior_Tutor/faq/#Q21
Student Counselling Service	http://www.tcd.ie/Student_Counselling/

H.3 Ethical Approval Applications

Ethical Approval Application – School Questionnaire

School of Computer Science and Statistics
Ethics Committee

Application for approval

1.	Title of Project	**A Study of the Awareness of the Risks in Using Social Networking Sites** (Post Primary School Students)

2.	Date of application for ethics approval	23rd March 2009

3a	Name of Principal Investigator	Aideen Keaney
3b	Status	Lecturer and PhD Student
3c.	Contact Details	aideen.keaney@tcd.ie ph 896 2199

4a	Name/s and status of other staff involved	PhD Supervisor: Dr. Frank Bannister
4b	Contact details (e.g. e-mail)	frank.bannister@tcd.ie Ph 896 2186

5	Proposed Start date for project	13th April 2009

6	Duration of fieldwork	13th April – 22nd May 2009

7a	Has ethical approval been sought from another organisation?	Yes			No	X	
7b	If answer to 7a is No is it intended to seek it?	Yes		Go to 7c	No	X	If no go to 8.
7c	If yes from whom?						
7d	When is a response expected?						

(Please note: You may exceed the space provided if necessary)

8	What is the research question (or the aims of the study)? (max 30 words)	The aim of this study is to explore the risks perceptions of post primary school students with regard to using social networking sites such as bebo and facebook.

9	Describe the procedures the participants will encounter during the study. This account should convey, in straightforward language, what will happen to participants in your study.	Students will be given a 14 page questionnaire (attached). This questionnaire should take approx 30 minutes to complete and will be administered during a free period. The questionnaire has yet to be pilot tested and the wording of some questions may change but it is not anticipated that the content will change substantially after pilot testing. Any changes made to the questionnaire that will require further consideration by the ethics committee will be re-submitted.

10	Participant Group ((Specify key characteristics: age, gender, etc)	Post primary school children – there are no exclusion criteria.

11 How many participants are required?	600-800, in 6-8 schools in the Dublin area.

12.	What research setting are involved (home, CRC, school, clinic, hostel other? (*Please list as many as known)*	The questionnaire will be administered in the school, in a free period, if possible in the presence of a third party (adult) who is known to the students.

13.	Describe the design of the study	Quantitative data study

14.	What methods of data collection will be used?	Questionnaire

15.	How long (per participant) will the testing/ interviewing take?	Approx 30 minutes

16a.	Does the study involve deception or withholding of information?	No
16b.	If yes why is this necessary?	

17a	Does the study involve physical risk to the participants?	No
17b	If yes, why is this necessary?	

17c. How has it been minimised?	

18a	Does the study involve any psychological risk to participants (e.g. upset, worry, stress, fatigue, feelings of being demeaned.)?	The study may increase respondents awareness of the risks associated with using social networking sites
18b	If yes, how has this been minimised?	The questionnaire has been worded so as to enquire about "people your age" rather than the respondent directly.
18c.	If yes, what supports have been put in place?	The study will be explained verbally to the participants before they consent to take part. Participants will be encouraged to discuss any concerns they have with the researcher. The participants will also be given an Information Leaflet for Participants (attached) which suggests web sites to visit for further information.

19a	Does the study involve social risk to participants (e.g. loss of status, privacy or reputation)?	No
19b	If yes, why is this necessary?	
19c.	How has it been minimised?	

20a	Does the study require participants to reveal information of a sensitive nature?	Participants are asked to reveal if they have or know of friends that have encountered any risks on social networking sites.
20b	If yes, why is this necessary?	It is assumed that those that have experience of risks may have higher risk perceptions.
20c.	How will the procedure minimise distress caused by such disclosures?	The study will be explained verbally to the participants before they consent to take part. Participants will be encouraged to discuss any concerns they have with the researcher. The participants will also be given an Information Leaflet for Participants (attached) which suggests web sites to visit for further information. The questionnaire is totally anonymous and individual participants cannot be identified. This will also be verbally explained to the participants.

21a	Are there any risks other than those encountered in every day life?	No
21b	If yes, how have they been minimised	
21c	What supports have been put in place??	

22	How will confidentiality of participants be assured?	Two forms of consent will be needed for participants. As the students are under 18, their parents have to provide consent and the students also have to consent to taking part in the study. The Informed Consent Forms for Parents and Students (attached) can identify participants as it collects participant's names. These forms will be collected prior to the participant being given the questionnaire. This means it will not be possible to match consent forms with questionnaires and thus identify participants with questionnaires. All information given in the questionnaire is anonymous and it is not possible to identify an individual from this questionnaire. The only personal information requested is gender and age in years. The completed consent forms and questionnaires will be kept in a secure office in a locked filing cabinet that will only be accessible to the researcher and supervisor. The questionnaires will be computerised and will be stored on the researcher's computer in a password protected folder. The consent forms and questionnaires will be stored for the duration of the study, i.e. until the work is fully reported and disseminated. They will then be kept in a locked cabinet for a further five years.

23	What is being done to preserve anonymity?	See Q22

24	Will funders of the research have access to information about individual participants?	N/A

25a	Have conditions been imposed on the ownership/publication of the findings?	No
25b	If so, please outline.	
26a	Can participants withdraw from the study at any point?	Yes

26b	How will this be communicated to participants?	This will be verbally explained to the participants before they consent to take part in the study. It is also clearly stated on both the Information Leaflet for Participants (attached) and the Informed Consent Forms (attached).

27	If observational research is to be undertaken without prior consent, describe the situation and how privacy confidentiality and dignity will be preserved?	N/A

28a	Do you anticipate any Child Protection issues to be relevant for the research process?	??
28b	If so, please describe briefly and state what measures will be put in place to deal with them.	

29a	Will participants receive any other reward for participation?	No
29b	Please specify.	

30	With reference to the Freedom of Information Act what measures will you take for data storage? Please see http://www.tcd.ie/foi	See Q22

31a	How will consent be obtained? (Attach a copy of the consent form). Tick box to confirm attachment [X]	As the participants in this study are under 18, it is necessary to gain consent from their parents. An Informed Consent Form for Parents (attached) will be sent to parents at least three days prior to the administration of the questionnaire. This form will also provide information about the study and what is involved for the participant. Details of the study will be verbally explained to the students before they agree to take part. They will be given a Participant Information Leaflet which also explains the study. If they wish to volunteer for the study, they will sign the Informed Consent Form for Parents (attached). Both parents and students will retain a copy of the Informed Consent Form.

31b	How will you ensure informed consent (Please attach information sheet) Tick box to confirm attachment X	The Informed Consent Form for Parents (attached) will explain to parents what is involved in the study. The details of the study will be explained verbally to the students and the Participant Information Leaflet will explain what is required of the participant in this study (attached)

32	What is your feedback procedure?	Schools will be sent a summary of the research findings once they are completed.

33	What do you expect to be the benefits / consequences for participants?	Filling out this questionnaire may make respondents more aware of the risks associated with the use of social networking sites. This may encourage them to learn more about these risks. It also may make them more concerned and want to protect themselves on these sites. Website links are provided for further information and respondents are welcome to talk to the researcher about any concerns they may have.

Appendix I Designing the Questionnaire

This appendix describes in detail the steps taken in designing the questionnaire and presents the final version of the school student questionnaire.

I.1 Designing the Questionnaire

Visual presentation of questionnaire

A number of guidelines were followed to help respondents to quickly understand the layout and organisation of the questionnaire:

- A consistent font and format was used throughout the questionnaire to ensure all response options were processed equally. Capitalisation is only used to draw attention to important words, white square boxes were used for responses and bolding is only used for question stems.
- The line spacing, font and text size were chosen to ensure legibility. The font chosen was Arial, 11pt which is a proportionally spaced font with no serifs.
- Visual clutter was reduced by reducing the number of questions presented on each page and increasing the amount of blank space.
- All questions were numbered to help respondents identify the beginning of each question.
- To differentiate the question and answer choices, darker print was used for the questions and lighter print was used for the answer choices.
- To help create the impression that the response options were all part of one group, they were placed in close vertical proximity to one another and spaced equally. They were also indented underneath the question stem to reinforce their subgrouping.
- To emphasise important considerations in questions, text was capitalised, e.g. Have you EVER put any of the following information on a social networking site? Often text is emphasised by the use of underlining, but as the questionnaire was also going to have a web version, capitalisation was used.
- Instructions that the respondent may already know (e.g tick one) were distinguished from the main question stem by placing it in parentheses and in a lighter print.

Ordering the questions

The following considerations were implemented in the questionnaire to ensure a logical ordering of questions:

- Related questions were grouped together under relevant sections. The sections were clearly labelled for respondents with white text on a black background. Within each section, the questions that were most salient and interesting to respondents were placed first to help respondents commit to the questionnaire.
- More sensitive questions, such as a respondents own experience of the risks associated with SNSs, were placed towards the end of the questionnaire after respondents had an opportunity to become engaged with the questionnaire.

Constructing open-ended questions

Two types of open-ended questions were used in the questionnaire, *numerical response questions* (e.g. How old were you when you first started using the Internet) and *descriptive questions* (e.g. If you have removed personal information from a social networking site, what information did you remove and why?). Based on a synthesis of recent research in this area, the following recommendations proposed by Dillman (2009) were followed:

- To discourage the respondents from entering invalid responses in the open-ended numerical response questions, the unit desired was specified in the question stem, the answer spaces were sized appropriately and unit labels were provided after the answer space, as shown below:

  28. What is your age in years? ☐ years

- The aim of the open-ended descriptive questions was to collect thick, rich descriptive information so adequate space was provided for respondents to completely answer these questions and scrollable boxes were used in the Internet survey.

Constructing closed-ended questions

In this questionnaire, closed-ended questions with ordered (ordinal) and unordered (nominal) response categories were used. Some of the questions required only one answer and some required multiple answers. Dillman (2009) suggests guidelines for each closed-ended question type but also includes some guidelines that apply to all closed-ended questions. The guidelines followed were:

All closed-ended questions

- Both positive and negative sides were stated in the question stem in either/or types of questions. This was to reduce the bias of implicitly suggesting a preferred response. e.g. To what extent do you agree/disagree with these statements?
- The spacing between answer categories was set consistently. This was particularly important for the 7 and 5 item Likert scales, as giving one item more space than another suggests to a respondent that it is more important and they are thus likely to select it.

Closed-ended questions – Nominal Scales

- Forced-choice questions were used instead of "*tick all that apply*" questions. Research (Smyth *et al.*, 2006) has shown that when a "*tick all that apply*" question is used in surveys that respondents seem to use a satisficing response strategy. They answered the question very quickly and were more likely to select the items in the top half of the list. Using a forced-choice format ensures a better response for all the questions in the scale. Table I.1 shows a comparison of both question types.

Forced-choice question			**"Tick all that apply" question**	
16. Have you EVER put any of the following information on a social networking site?			**16. Have you EVER put any of the following information on a social networking site?** (tick all that apply)	
A picture of yourself	☐$_1$ Yes	☐$_2$ No	A picture of yourself	☐$_1$
Photos of your friends	☐$_1$ Yes	☐$_2$ No	Photos of your friends	☐$_2$
Your date of birth	☐$_1$ Yes	☐$_2$ No	Your date of birth	☐$_3$
Your first name	☐$_1$ Yes	☐$_2$ No	Your first name	☐$_4$
Your last name	☐$_1$ Yes	☐$_2$ No	Your last name	☐$_5$

Table I.1 Comparison of a Forced-choice and a "Tick All That Apply" Question

- Following normal web protocols, radio-buttons were used for single-answer questions and check-boxes were used for multiple-answer questions on the Internet questionnaires.

Closed-ended questions – Ordinal Scales

- There has been much research into the construction of ordinal scales ((Schwarz *et al.*, 1991, Krosnick and Fabrigar, 1997, Tourangeau *et al.*, 2007, Christian *et al.*, 2009). As many of the scales utilised in this questionnaire were pre-existing scales,

the formats of the original scales were adhered to, all of these measures used bipolar Likert scales. Research suggests that for bipolar scales the optimal response category is either 5 or 7. Both sizes were used in this study. Both scales used are balanced with an equal number of positive and negative categories.

- Where possible construct-specific questions were constructed, for example instead of asking respondents the question "to what extent do you agree/disagree that your classmates are concerned about the risks on SNSs?" (1 = strongly agree, 7 = strongly disagree), the question was simplified to "would your classmates be concerned about the risks on SNSs?" (1=not at all concerned, 7 = very concerned). Research has shown that using the latter simplified format reduces the cognitive burden on respondents (Saris *et al.*, 2010).
- Research suggests that all points on these scales should be labelled. Krosnick and Fabrigar (1997) found that fully labelled scales rate higher on reliability and validity. The scales were not labelled in this questionnaire as the scales were based on previous studies where labels were only provided at each end of the scale. As recommended by Christian *et al.* (2009) numeric labels were not included on the scales.
- There is some disagreement in the literature as to whether to present the positive or negative end of the scale first. Tourangeau *et al*. (2004) suggest that the postitive category should be presented first, Christian *et al.* (2009) found in web surveys, no difference to the presentation, except that respondents answered the question quicker when the positive category was presented first. In this questionnaire the positive categories were presented first.

I.2 School Questionnaire – Option 1

Trinity College Dublin
School of Computer Science and Statistics

Awareness of the Risks in Using Social Networking Sites

Questionnaire for School Students

All information given in this questionnaire is **anonymous** and you cannot be identified from this questionnaire.

SECTION A: PLEASE TELL US ABOUT YOUR USE OF COMPUTERS AND THE INTERNET

1. How do you MOSTLY use the Internet at home? (tick one)

- ☐₁ By myself
- ☐₂ With one or more friends
- ☐₃ With a brother or sister
- ☐₄ With my mother
- ☐₅ With my father
- ☐₆ Others, Please specify: _____

2. How old were you when you FIRST started using the Internet? ☐☐ years

3. How would you rate yourself at using the Internet? (tick one)

- ☐₁ I am just finding my feet
- ☐₂ I am up and running but there are still things I cannot do
- ☐₃ I can do pretty much everything I want to do
- ☐₄ I am very good and friends often come to me for computer advice

4. Do your parents/guardians set rules about your use of the Internet?

- ☐₁ Yes
- ☐₂ No

5. Does your school set rules about your use of the Internet?

- ☐₁ Yes
- ☐₂ No

6. Do you know how to stay safe on the Internet (e.g. how to behave in a chat room etc.)

- ☐₁ Yes
- ☐₂ No
- ☐₃ Don't know

7. Do you know how to decide if information online can be trusted?

- ☐₁ Yes
- ☐₂ No
- ☐₃ Don't know

SECTION B: PLEASE TELL US ABOUT YOUR USE OF SOCIAL NETWORKING SITES

8. Have you ever used a social networking site? ☐₁ Yes ☐₂ No

(A social networking site is one where you can create a profile, add friends and communicate with these friends, e.g. sites such as Bebo and Facebook, BUT NOT sites where you exclusively share videos and photos such as YouTube and Flickr.)

9. If you have NEVER used a social networking site, can you tell us why?

If you have NEVER used a social networking site, please go to Q25, pg 7

10. How old were you when you FIRST started using social networking sites? ☐ years

11. Which social networking sites have you used?

	Used to use it but no longer	Use it less than once a week	Use it more than once a week
Bebo (tick one)	☐₁	☐₂	☐₃
Facebook (tick one)	☐₁	☐₂	☐₃
MySpace (tick one)	☐₁	☐₂	☐₃
Others: (please specify)	☐₁	☐₂	☐₃

_____

12. On average, how OFTEN do you access social networking sites? (tick one)

- ☐₁ Several times a day
- ☐₂ About once a day
- ☐₃ A couple of times a week
- ☐₄ About once a week
- ☐₅ A couple of times a month
- ☐₆ About once a month
- ☐₇ Less often

13. **In the past week, on average, approximately how many minutes PER DAY have you spent on social networking sites?** (tick one)

- ☐₁ Less than 10 minutes
- ☐₂ Between 10 and 30 minutes
- ☐₃ Between 31 and 60 minutes
- ☐₄ Between 1 – 2 hours
- ☐₅ Between 2 – 3 hours
- ☐₆ More than 3 hours

14. **How many friends, in total, do you have on social networking sites?** (tick one)

- ☐₁ Less than 50 friends
- ☐₂ Between 51 and 100 friends
- ☐₃ Between 101 and 200 friends
- ☐₄ Between 201 and 300 friends
- ☐₅ Between 301 and 400 friends
- ☐₆ More than 400 friends.

15. **Which of the following features have you EVER used on social networking sites?**

Created a profile	☐₁ Yes	☐₂ No
Uploaded photos	☐₁ Yes	☐₂ No
Used tags on photos	☐₁ Yes	☐₂ No
Loaded personal videos	☐₁ Yes	☐₂ No
Created a blog or journal	☐₁ Yes	☐₂ No
Used applications provided by social networking site (e.g. games, photo editing applications etc.)	☐₁ Yes	☐₂ No

16. Have you EVER put any of the following information on a social networking site?

A picture of yourself	☐, Yes	☐, No
Photos of your friends	☐, Yes	☐, No
Your date of birth	☐, Yes	☐, No
Your first name	☐, Yes	☐, No
Your last name	☐, Yes	☐, No
Your e-mail address	☐, Yes	☐, No
Your instant message screen name	☐, Yes	☐, No
Your mobile phone number	☐, Yes	☐, No
Your home address	☐, Yes	☐, No
The name of your school	☐, Yes	☐, No
Your list of hobbies and interests	☐, Yes	☐, No
List of your friends on your profile	☐, Yes	☐, No
Comments on other peoples profiles	☐, Yes	☐, No

17. If you have removed personal information from a social networking site, what information did you remove and why?

18. Do your parents/guardians set rules about your use of social networking sites?

☐ Yes
☐ No

19. Does your school set rules about your use of social networking sites?

☐ Yes
☐ No

20. To what extent do you agree/disagree with these statements?

	strongly disagree				strongly agree
Using a social networking site is part of my everyday activity	☐	☐	☐	☐	☐
I take pride in my social networking profile	☐	☐	☐	☐	☐
Social networking sites have become part of my daily routine.	☐	☐	☐	☐	☐
I feel out of touch when I haven't logged onto a social networking site for a while	☐	☐	☐	☐	☐
I feel I am part of the social networking site community	☐	☐	☐	☐	☐
I would be sorry if the social networking site shut down	☐	☐	☐	☐	☐
I am OK with friends viewing my social networking profile	☐	☐	☐	☐	☐
I am OK with family viewing my social networking profile	☐	☐	☐	☐	☐
I am OK with classmates viewing my profile	☐	☐	☐	☐	☐
I am OK with strangers viewing my profile	☐	☐	☐	☐	☐

21. Do you find social networking sites useful for?

Finding information about friends you see often	☐, Yes	☐, No
Finding information about friends you don't see often	☐, Yes	☐, No
Keeping in contact with friends you see often	☐, Yes	☐, No
Keeping in contact with friends you don't see often	☐, Yes	☐, No
Sharing information (e.g. photos)	☐, Yes	☐, No
Meeting new friends	☐, Yes	☐, No
Organising parties and events	☐, Yes	☐, No
Finding people who share my interests	☐, Yes	☐, No
Getting more people to become my friends	☐, Yes	☐, No
Making it more convenient for others to get in touch with me	☐, Yes	☐, No
Showing information about myself	☐, Yes	☐, No
Making me more popular	☐, Yes	☐, No
Other: (Please specify)	☐, Yes	☐, No

_____

22. Have you made your profile more private? (tick one)

- ☐₁ Yes
- ☐₂ No
- ☐₃ Don't remember or know

23. If you have made your profile more private, why did you do this?

SECTION C: PLEASE TELL US YOUR VIEWS OF THE RISKS WITH SOCIAL NETWORKING SITES

The same list of risks associated with social networking sites are presented in the next few questions and I would like your view on different aspects of these risks.

I am aware that there are other risks in using social networking sites but this study is only looking at the risks stated below.

24. Do you think that these risks could happen to YOU on a social networking site?

	not at all at risk						very much at risk
Spending too much time on the site	☐	☐	☐	☐	☐	☐	☐
Replacing the need for meeting up with existing friends	☐	☐	☐	☐	☐	☐	☐
Meeting in person a stranger that you have only met online	☐	☐	☐	☐	☐	☐	☐
Being bullied or harassed	☐	☐	☐	☐	☐	☐	☐
Being hurt by information that others post about you	☐	☐	☐	☐	☐	☐	☐
Embarrassing information or photos being seen by people who you would prefer didn't see it	☐	☐	☐	☐	☐	☐	☐
Spam	☐	☐	☐	☐	☐	☐	☐
Your personal information being misused by strangers	☐	☐	☐	☐	☐	☐	☐
Your personal information being sold to advertisers	☐	☐	☐	☐	☐	☐	☐
Accidentally stumbling across content that made you uncomfortable	☐	☐	☐	☐	☐	☐	☐
Being stalked	☐	☐	☐	☐	☐	☐	☐
Getting a virus	☐	☐	☐	☐	☐	☐	☐

25. How LIKELY are these risks to happen on social networking sites?

	very unlikely						very likely
Spending too much time on these sites	☐	☐	☐	☐	☐	☐	☐
Replacing the need for meeting up with existing friends	☐	☐	☐	☐	☐	☐	☐
Meeting in person a stranger that they have only met online	☐	☐	☐	☐	☐	☐	☐
Being bullied or harassed	☐	☐	☐	☐	☐	☐	☐
Being hurt by information that others post about them	☐	☐	☐	☐	☐	☐	☐
Embarrassing information or photos being seen by people who they would prefer didn't see it	☐	☐	☐	☐	☐	☐	☐
Spam	☐	☐	☐	☐	☐	☐	☐
Personal information being misused by strangers	☐	☐	☐	☐	☐	☐	☐
Personal information being sold to advertisers	☐	☐	☐	☐	☐	☐	☐
Accidentally stumbling across content that made them uncomfortable	☐	☐	☐	☐	☐	☐	☐
Being stalked	☐	☐	☐	☐	☐	☐	☐
Getting a virus	☐	☐	☐	☐	☐	☐	☐

26. Do you think YOUR FRIENDS/CLASSMATES are at risk on social networking sites of/from ...?

	not at all at risk						very much at risk
Spending too much time on these sites	☐	☐	☐	☐	☐	☐	☐
Replacing the need for meeting up with existing friends	☐	☐	☐	☐	☐	☐	☐
Meeting in person a stranger that they have only met online	☐	☐	☐	☐	☐	☐	☐
Being bullied or harassed	☐	☐	☐	☐	☐	☐	☐
Being hurt by information that others post about them	☐	☐	☐	☐	☐	☐	☐
Embarrassing information or photos being seen by people who they would prefer didn't see it	☐	☐	☐	☐	☐	☐	☐
Spam	☐	☐	☐	☐	☐	☐	☐
Personal information being misused by strangers	☐	☐	☐	☐	☐	☐	☐
Personal information being sold to advertisers	☐	☐	☐	☐	☐	☐	☐
Accidentally stumbling across content that made them uncomfortable	☐	☐	☐	☐	☐	☐	☐
Being stalked	☐	☐	☐	☐	☐	☐	☐
Getting a virus	☐	☐	☐	☐	☐	☐	☐

27. Do you think, that these risks on social networking sites are SERIOUS?

	not very severe						very severe
Spending too much time on these sites	☐	☐	☐	☐	☐	☐	☐
Replacing the need for meeting up with existing friends	☐	☐	☐	☐	☐	☐	☐
Meeting in person a stranger that they have only met online	☐	☐	☐	☐	☐	☐	☐
Being bullied or harassed	☐	☐	☐	☐	☐	☐	☐
Being hurt by information that others post about them	☐	☐	☐	☐	☐	☐	☐
Embarrassing information or photos being seen by people who they would prefer didn't see it	☐	☐	☐	☐	☐	☐	☐
Spam	☐	☐	☐	☐	☐	☐	☐
Personal information being misused by strangers	☐	☐	☐	☐	☐	☐	☐
Personal information being sold to advertisers	☐	☐	☐	☐	☐	☐	☐
Accidentally stumbling across content that made them uncomfortable	☐	☐	☐	☐	☐	☐	☐
Being stalked	☐	☐	☐	☐	☐	☐	☐
Getting a virus	☐	☐	☐	☐	☐	☐	☐

SECTION D: PLEASE TELL US ABOUT YOUR EXPERIENCE OF THESE RISKS

28. Have YOU experienced any of these risks associated with social networking sites?

Spending too much time on the site	☐, Yes ☐, No
Replacing the need for meeting up with existing friends	☐, Yes ☐, No
Meeting in person a stranger that you have only met online	☐, Yes ☐, No
Being bullied or harassed	☐, Yes ☐, No
Being hurt by information that others post about you	☐, Yes ☐, No
Embarrassing information or photos being seen by people who you would prefer didn't see it	☐, Yes ☐, No
Spam	☐, Yes ☐, No
Your personal information being misused by strangers	☐, Yes ☐, No
Your personal information being sold to advertisers	☐, Yes ☐, No
Accidentally stumbling across content that made you uncomfortable	☐, Yes ☐, No
Being stalked	☐, Yes ☐, No
Getting a virus	☐, Yes ☐, No

29. Has ANYONE YOU KNOW experienced any of these risks associated with social networking sites?

Spending too much time on these sites	☐, Yes ☐, No
Replacing the need for meeting up with existing friends	☐, Yes ☐, No
Meeting in person a stranger that they have only met online	☐, Yes ☐, No
Being bullied or harassed	☐, Yes ☐, No
Being hurt by information that others post about them	☐, Yes ☐, No
Embarrassing information or photos being seen by people who they would prefer didn't see it	☐, Yes ☐, No
Spam	☐, Yes ☐, No
Personal information being misused by strangers	☐, Yes ☐, No
Personal information being sold to advertisers	☐, Yes ☐, No
Accidentally stumbling across content that made them uncomfortable	☐, Yes ☐, No
Being stalked	☐, Yes ☐, No
Getting a virus	☐, Yes ☐, No

SECTION E: PLEASE TELL US YOUR OPINION OF SOCIAL NETWORKING SITES

30. To what extent do YOU agree/disagree with these statements?
(tick one response for each statement)

	strongly disagree						strongly agree
I generally trust other people	☐	☐	☐	☐	☐	☐	☐
I tend to rely upon other people	☐	☐	☐	☐	☐	☐	☐
I have faith in people in general	☐	☐	☐	☐	☐	☐	☐
I generally trust other people unless they give me reason not to	☐	☐	☐	☐	☐	☐	☐
I am concerned about the kind of information I am revealing to others through social networking sites	☐	☐	☐	☐	☐	☐	☐
I am concerned about what a social networking site can know about me	☐	☐	☐	☐	☐	☐	☐
I am concerned about who has access to the information I publish on social networking sites	☐	☐	☐	☐	☐	☐	☐
I am concerned about how the information I publish on social networking sites could be used	☐	☐	☐	☐	☐	☐	☐
I am concerned about my privacy on social networking sites in general	☐	☐	☐	☐	☐	☐	☐
My friends think that I should use social networking sites	☐	☐	☐	☐	☐	☐	☐
Generally speaking, I want to do what my friends think I should do	☐	☐	☐	☐	☐	☐	☐
I use social networking sites because many of my friends use them	☐	☐	☐	☐	☐	☐	☐
Overall, I trust social networking sites (the companies)	☐	☐	☐	☐	☐	☐	☐

31. Are there any other risks or concerns that you have about using social networking sites?

SECTION F: PLEASE TELL US A LITTLE ABOUT YOURSELF

32. **What is your gender** (tick one) ☐ Male ☐ Female

33. **What is your age in years?** ☐ years

SECTION G: PLEASE TELL US ABOUT COMPLETING THIS QUESTIONNAIRE

34. **Has completing this questionnaire changed your opinions about using social networking sites?**

It has made me more worried about the risks	☐, Yes	☐, No
It has made me more confident about what I know about the risks	☐, Yes	☐, No
It has increased my awareness of the risks	☐, Yes	☐, No
It has made me realise that I am not aware of some of the risks	☐, Yes	☐, No
It has made me realise that I don't protect myself as much as I could	☐, Yes	☐, No
I was already aware of these risks	☐, Yes	☐, No

Any other comments:

Thank you for taking the time to complete this questionnaire

School Questionnaire – Option 2

Trinity College Dublin
School of Computer Science and Statistics

Awareness of the Risks in Using Social Networking Sites

Questionnaire for School Students

All information given in this questionnaire is **anonymous** and you cannot be identified from this questionnaire.

25. Do you think your friends/classmates KNOW about these risks on social networking sites?

	very well known						not very well known
Spending too much time on these sites	☐	☐	☐	☐	☐	☐	☐
Replacing the need for meeting up with existing friends	☐	☐	☐	☐	☐	☐	☐
Meeting in person a stranger that they have only met online	☐	☐	☐	☐	☐	☐	☐
Being bullied or harassed	☐	☐	☐	☐	☐	☐	☐
Being hurt by information that others post about them	☐	☐	☐	☐	☐	☐	☐
Embarrassing information or photos being seen by people who they would prefer didn't see it	☐	☐	☐	☐	☐	☐	☐
Spam	☐	☐	☐	☐	☐	☐	☐
Personal information being misused by strangers	☐	☐	☐	☐	☐	☐	☐
Personal information being sold to advertisers	☐	☐	☐	☐	☐	☐	☐
Accidentally stumbling across content that made them uncomfortable	☐	☐	☐	☐	☐	☐	☐
Being stalked	☐	☐	☐	☐	☐	☐	☐
Getting a virus	☐	☐	☐	☐	☐	☐	☐

26. Do you think your friends/classmates would be CONCERNED about these risks on social networking sites?

	not at all concerned						very concerned
Spending too much time on these sites	☐	☐	☐	☐	☐	☐	☐
Replacing the need for meeting up with existing friends	☐	☐	☐	☐	☐	☐	☐
Meeting in person a stranger that they have only met online	☐	☐	☐	☐	☐	☐	☐
Being bullied or harassed	☐	☐	☐	☐	☐	☐	☐
Being hurt by information that others post about them	☐	☐	☐	☐	☐	☐	☐
Embarrassing information or photos being seen by people who they would prefer didn't see it	☐	☐	☐	☐	☐	☐	☐
Spam	☐	☐	☐	☐	☐	☐	☐
Personal information being misused by strangers	☐	☐	☐	☐	☐	☐	☐
Personal information being sold to advertisers	☐	☐	☐	☐	☐	☐	☐
Accidentally stumbling across content that made them uncomfortable	☐	☐	☐	☐	☐	☐	☐
Being stalked	☐	☐	☐	☐	☐	☐	☐
Getting a virus	☐	☐	☐	☐	☐	☐	☐

27. How easily could your friends/classmates STOP these risks on social networking sites?

	very easily						not easily
Spending too much time on these sites	☐	☐	☐	☐	☐	☐	☐
Replacing the need for meeting up with existing friends	☐	☐	☐	☐	☐	☐	☐
Meeting in person a stranger that they have only met online	☐	☐	☐	☐	☐	☐	☐
Being bullied or harassed	☐	☐	☐	☐	☐	☐	☐
Being hurt by information that others post about them	☐	☐	☐	☐	☐	☐	☐
Embarrassing information or photos being seen by people who they would prefer didn't see it	☐	☐	☐	☐	☐	☐	☐
Spam	☐	☐	☐	☐	☐	☐	☐
Personal information being misused by strangers	☐	☐	☐	☐	☐	☐	☐
Personal information being sold to advertisers	☐	☐	☐	☐	☐	☐	☐
Accidentally stumbling across content that made them uncomfortable	☐	☐	☐	☐	☐	☐	☐
Being stalked	☐	☐	☐	☐	☐	☐	☐
Getting a virus	☐	☐	☐	☐	☐	☐	☐

Appendix J Measures Used in Questionnaire

This appendix describes how the measures used in the questionnaire were refined and revised based on the pretesting and piloting stages of the survey design process.

Risk Perceptions of SNSs:

Risk factors examined

The initial questions about risk characteristics were designed using the wording proposed by Benthin *et al.* (1993) as they had successfully administered their questionnaire to an adolescent sample. This wording was changed quite considerably as the expert evaluation, pilot testing and pretesting of the questionnaire indicated difficulties in understanding these questions. Table J.2 shows how the wording of each risk factor was refined. Capitals were used in the final questionnaire for emphasis.

In the first pilot study, each of the 10 risk items was rated by respondents on each of the 7 risk factors. In early drafts of the questionnaire, these questions were placed at the end of the questionnaire. Expert feedback suggested that these questions be moved to an earlier position in the questionnaire to ensure against respondent fatigue. Feedback from the pilot study indicated that the questionnaire was too long and respondents felt it was repetitive as they had to rate the same 10 risk items by so many risk factors. This was also clear from the responses, as for latter questions many respondents were just ticking the same response category repeatedly. The questionnaire was split into two questionnaires with respondents randomly assigned to each questionnaire. The risk factors were split as shown in Table J.1

Pilot Questionnaire Version 1	Pilot Questionnaire Version 2
Personal Risk	Personal Risk
Severity/Consequences	Controllability
Risk to peers	Concern
Likelihood of Risk	Knowledge of Risk

Table J.1 Risk Factors by Pilot Questionnaire.

The questionnaire was piloted a second time. The final questionnaires each assessed 4 risk factors.

Risk Factor	Initial Wording (based on (Benthin *et al.*, 1993))	Pilot Study	Final Questionnaire
Personal risk	Can you indicate to what extent you are personally at risk of the following scenarios? (1 = very much at risk; 7= not at all at risk)	Do you think you are at risk of/from …? (1 = very much at risk; 7= not at all at risk)	Do you think that these risks could happen to YOU on a social networking site? (1 = not at all at risk; 7=very much at risk)
Knowledge of risk	Can you indicate to what extent are the risks associated with each of these scenarios known to people your age? (1 = not well known; 7= very well known)	Do you think people your age know about the risk of/from …? (1 = not well known; 7= very well known)	Do you think your friends/classmates KNOW about these risks on social networking sites? (1 = very well known; 7= not very well known)
Likelihood of risk	Can you indicate to what extent are the risks associated with each of these scenarios are likely to happen? (1 = very likely; 7= very unlikely)	How likely are people your age to encounter these risks? (1 = very likely; 7= very unlikely)	How LIKELY are these risks to happen on social networking sites? (1 = very unlikely; 7= very likely)
Concern	Can you indicate to what extent are the potential dangers associated with each of these scenarios of concern or a worry to people your age? (1 = not at all concerned; 7 = very concerned)	How concerned, do you think, are people your age about these risks? (1 = not at all concerned; 7 = very concerned)	Do you think your friends/classmates would be CONCERNED about these risks on social networking sites? (1 = not at all concerned; 7 = very concerned)
Controllability	If someone your age was experiencing these scenarios, to what extent could they control the risks associated with it? (1 = risks cannot be controlled; 7 = risks can be fully controlled)	How well do you think a person your age could control these risks? (1 = not easily; 7 = very easily)	How easily could your friends/classmates STOP these risks on social networking sites? (1 = very easily; 7 = not easily)
Risk to Peers	Can you indicate to what extent your peers are at risk of the following scenarios? (1 = very much at risk; 7= not at all at risk)	Do you think your friends are at risk of/from …? (1 = very much at risk; 7= not at all at risk)	Do you think YOUR FRIENDS/CLASSMATES are at risk on social networking sites of/from …? (1 = not at all at risk; 7=very much at risk)
Severity/ Consequences	Can you indicate if something bad happened because of this scenario, would the harmful effects be mild or serious? (1 = very mild harm; 7 = very serious harm)	Are the harmful effects of these risks likely to be mild or severe? (1 = not very severe; 7= very severe)	Do you think, that these risks on social networking sites are SERIOUS? (1 = not very severe; 7= very severe)

Table J.2 Progression of Wording for Questions Describing Risk Factors

Risk Area	Initial Wording	Pilot Study	Final Questionnaire
	Can you indicate to what extent are the risks associated with each of these scenarios known to people your age?	**Do you think people your age know about the risk of/from …?**	**Do you think your friends/classmates KNOW about these risks on social networking sites?**
Time wasting	A person can spend too much time on social networking sites	Spending too much time on social networking sites	Spending too much time on these sites
Less FtF communication	Using social networking sites can mean that a person spends less time in face to face contact with existing friends	Social networking sites replacing the need for meeting up with existing friends	Replacing the need for meeting up with existing friends
Meeting strangers	A person who has communicated with strangers on social networking sites can decide to meet them in person.	Meeting in person a stranger that they have only met on a social networking site	Meeting in person a stranger that they have only met online
Cyberbullying	A person can be bullied or harrassed on social networking sites	Being bullied or harrassed on a social networking site	Being bullied or harassed
Embarrasing info	A person can be embarassed or hurt by information that others post about them on social networking sites	Being hurt by information that others post about them on social networking sites	Being hurt by information that others post about them
Embarrasing info seen	Embarrasing information posted about a person on social networking sites can be seen by parents, friends and family	Embarrasing information posted on social networking sites being seen by parents, friends and family	Embarrassing information or photos being seen by people who they would prefer didn't see it
Privacy	A persons personal information posted on social networking sites can be seen (misused?) by strangers	Personal information posted on social networking sites being misued by strangers	Personal information being misused by strangers
Commercial persuasion	A persons personal information posted on social networking sites can be sold to advertisers	Personal information posted on social networking sites being sold to advertisers	Personal information being sold to advertisers
Violent/hateful content	A person can encounter violent/hateful content on social networking sites	Accidentally stumbling across disturbing content on a social networking site	Accidentally stumbling across content that made them uncomfortable
Stalking	A person can be stalked on a social networking site	Being stalked on a social networking site	Being stalked
Spam			Spam
Virus			Getting a virus

Table J.3 Progression of Wording for Questions Describing Risk Item

Risks examined

Table J.3 shows how the wording of each risk area was refined through the expert evaluation, piloting and pretesting of the questionnaire. At the pilot stage, two further risk areas were identified and included on the final list; these risks were viruses and spam.

Experience of Risks:

In the pilot this was posed as a single question, listing all the risks and asking the respondents to indicate whether the risks had happened to them, had happened to someone they knew or hadn't happened to anyone they knew. This question was simplified after the pilot study by splitting it into two separate questions (personal experience, knew of others' experience) with a dichotomous yes/no answer.

Usage of SNSs:

SNS Sites Used

Following a question format proposed by Hargittai (2007), the initial questionnaire used a six-category variable of SNS usage typology measuring experiences with seven SNS sites. The seven SNSs included were Bebo, Facebook, MySpace, Orkut, Hi5, Last.fm and Twitter (this list was generated from the focus group interviews). To measure SNS usage, participants were asked to choose one of the following options: 'have never heard of it', 'have never used it', 'tried it only once', 'used to use it but no longer', 'use it sometimes' and 'use it often'. Following feedback from the pilot study, the pretesting questionnaire and an expert evaluation this question was simplified. Respondents were presented with the three most popular SNS sites in Ireland (Bebo, Facebook and MySpace) at the time the study was carried out and were asked if they had ever used these sites, or if they currently used these sites more/less than once a week. They were also given the opportunity to include any other sites they used/use.

Frequency/Duration of SNS Usage

The "*the facebook intensity scale*", developed by Ellison *et al*. (2007) was used in this study. The scale was slightly modified, as Facebook is not the only SNS being examined in this study, all references to Facebook were changed to social networking site. The number of response categories for the number of friends was reduced from 9 categories to 6 categories to help reduce the overall length of the questionnaire.

Purpose of Use

Respondents were presented with a list of uses of SNS, such as keeping in contact with old friends, sharing information etc. and asked to indicate whether they found these features useful or not. In the pilot questionnaire a 7 point bipolar scale (1 = not at all useful; 7 = very useful) was used, this was simplified to a dichotomous yes/no response in the final questionnaire.

Information Placed on SNS

Respondents were asked to select from a list, the type of personal information that they had ever placed on a SNS, for example name, email address, phone numbers etc. The pilot questionnaire had three response categories: "never"; "I did but removed it" and "currently on site". After the pilot study the question was simplified to a dichotomous yes/no response.

Skills:

IT skill level

Assessing the IT skill level of respondents was based on two measures as used in the UK Kids Go Online Survey (Livingstone and Helsper, 2007). The first measure was a single skill scale which summed up seven internet-related skills that each respondent claimed to be good at. Livingstone and Helsper (2007) found the reliability coefficient for this scale to be acceptable at alpha 0.70. For the pilot study the skill scale was extended to 13 items, additional items included whether respondents could install a firewall, applications from the Internet and operating systems. The second measure used by Livingstone and Helsper, asked respondents to self-rate how good they were are using the Internet, the categories used were beginner, average, experienced and expert. These categories were re-worded for the questionnaire to make them more meaningful for respondents:

- ☐1 I am just finding my feet
- ☐2 I am up and running but there are still things I cannot do
- ☐3 I can do pretty much everything I want to do
- ☐4 I am hot and friends often come to me for computer advice

Both of these measures were used in the pilot study. Subsequent analysis showed that the correlation between the two measures was significant at the 0.01 level. The self-rate measure was only used in the final questionnaire in order to reduce the overall length of the questionnaire.

Attitudes:

Privacy: Two privacy concern scales that have been adapted for addressing privacy concerns with SNSs were examined (Acquisti and Gross, 2006, Fogel and Nehmad, 2009). Fogel and Nehmad (2009) adapted the Dinev and Hart Scale (2004) to contain three items measuring privacy concerns with SNSs measured on a bipolar Likert scale from 1 = not concerned to 5 = very concerned. For example, one item from the scale is, ''I am concerned that the information I submit on Facebook could be misused." In their study sample, the Cronbach α reliability for the scale was 0.92. A similar scale to assess privacy concerns with SNS was used by Acquisti and Gross (2006). Their scale contained five items measuring privacy concerns, but used a 7 point bipolar Likert scale. For example, an additional item in this scale is, ''I am concerned about what Facebook can know about you." Both scales were used in the pilot study, but modified references to Facebook to social networking sites. From the pilot study there was a strong correlation between the two scales (r = 0.759) and both scales produced high Cronbach α reliability scores, 0.895 for the Fogel and Nehmad (2009) scale and 0.91 for the Acquisti and Gross scale (2006). The Acquisti and Gross scale (2006) was used in the final questionnaires as it was a broader scale that addressed more privacy concerns.

Trust: A number of studies have investigated trust with respect to SNSs. Dwyer *et al.* (2007) measured trust using two scales, one addressing members trust in the SNS and the second scale examining trust in other members of the site. They reported poor reliability scores for these scales, so these scales were not considered suitable for inclusion in the study. Fogel and Nehmad (2009) adapted a consumer trust scale (Pan and Zinkhan, 2006) for use with SNSs. This was a four item scale measured on a 5 point likert scale, a example item is "I can count on Facebook.com to protect my privacy". Although Fogel and Nehmad (2009) reported adequate reliability measures for this scale, it proved too awkward to use in this study as a separate four item scale was needed for each SNS. In the pilot study, this would have meant including seven sets of four repeating items with just the social networking site name changing. It was therefore decided to use the trust scale devised by Acquisti and Gross (2006). This was a four item scale, similar to that proposed by Dwyer *et al*. (2007) that examined trust in the SNS company itself and also other members of SNSs. Responses were measured on 7 point bipolar Likert scale. The cronbach α reliability score for this scale in the pilot study was extremely poor (0.388) so Gefen's (2000) disposition to trust scale was used in the final questionnaire.

Appendix K Pilot Study Comment Sheet

COMMENTS ON QUESTIONNAIRE

1. **How long did it take you to fill in this questionnaire?** ☐ minutes

2. **Overall, how easy or difficult was the questionnaire to complete?**
   - ☐ Very easy
   - ☐ Somewhat easy
   - ☐ Somewhat difficult
   - ☐ Very difficult

3. **Do you think the questionnaire is …?**
   - ☐ Too short
   - ☐ Just right
   - ☐ Too long

4. **Did you find any of the questions confusing?**
   - ☐ Yes
   - ☐ No

   If yes, please explain

5. **Are there any questions that you think people might object to answering?**
   - ☐ Yes
   - ☐ No

   If yes, please explain

6. **Have you any further thoughts or comments about the questionnaire?**

   If yes, please explain

Appendix L Focus Group

L.1 Questioning Route (Krueger and Casey, 2000)

Question	Description
Opening questions	The aim of this question is to get people talking and to help them feel comfortable. All participants should answer this question. This question should be easy and quick (usually within 30 seconds) to answer. Usually it is better to ask for facts as opposed to attitudes and opinions.
Introductory questions	Introductory questions introduce the topic of discussion and get people to start thinking about their connection with the topic. Typically, these are open-ended questions that allow participants to talk about the issue under investigation.
Transition questions	Transition questions move the conversation into the key questions that drive the study. These questions should link the introductory questions and the key questions. At this stage the participants should be becoming aware of how others view the topic.
Key questions	These are the key questions of the study. Typically, there are two to five questions in this category. These are the questions that require the greatest attention in the analysis. These key questions may need as much as ten or twenty minutes each.
Ending questions	Three types of ending question are valuable: the all-things-considered question, the summary question and the final question. The all-things-considered question is used to determine the final position of participants on critical areas of concern. This question allows each participant to reflect on all comments shared in the discussion and then identify which aspects are the most important to them. The summary question is asked after the moderator has given a short oral summary of the discussion of the key questions. After the summary, participants are asked about the adequacy of the summary. The final question in a focus group is an insurance question and its purpose is to ensure that critical aspects have not been overlooked. The question begins with a short overview of the purpose of the focus group and then the moderator asks if anything was overlooked?

Table L.1 Qualities of a Good Questioning Route. Source: (Krueger and Casey, 2000)

L.2 Questioning Route Adolescent Focus Group

The questioning route designed for the focus group to help develop the content of the survey is shown in Table L.2.

Opening:	1. Tell us your name and what your favourite TV programme is.
Introductory:	2. Tell us about your use of Social Networking Sites (SNSs)? 3. What is your general view of SNSs?
Transition: (10 mins)	[Ask participants to generate a list of the risks and concerns [for your age group] on paper and then collate them on a flip chart] 4. Generate a list of risks and concerns with SNSs.
Key: (20 mins) (assess risk characteristics) Select one risk (by group or by moderator) OR looking at the list of risks generated	5. Would everyone know about these risks? 6. Of all the risks we discussed, which ones do you feel are the most serious? 7. What would you do to reduce your chance of encountering such risks? 8. How do you find out about risks? Who should inform you?
Ending: (10 mins)	[After summarising the discussion to date] 9. Did I correctly describe what was said? 10. In this focus group we wanted to get an idea of the risks that you perceive in using social networking sites and also to get some idea of the characteristics of these risks, does the technology exacerbate the risk, is it the individual or their environment? Do you think there is anything that we missed? Is there anything that you wanted to say that you didn't get a chance to say?

Table L.2 Questioning Route for Adolescent Focus Group

L.3 Introduction by Moderator - Adolescent Focus Group

Many thanks for taking the time to join in this discussion about Social Networking Sites. My name is Aideen Keaney, I am a lecturer in TCD and I am working on a PhD in this area. You may remember filling in my questionnaire last year. XXX will be assisting me in running this focus group.

Before going any further I would like to clarify what I mean by a SNS, I am interested in sites such as Bebo and Facebook rather than sites that have been developed for a specific purpose, such as for sharing photographs (e.g. flickr and picasa) and sharing videos (e.g. YouTube).

The main aim of this focus group is to get your views and opinions about using SNSs. As your age group is one of the primary users of SNSs, we want to tap into your experiences and opinions on SNSs. There are no right or wrong answers. We expect that you will have differing points of view and would like that you would feel free to share your point of view even if it differs from others. I am moderating the focus group, but please don't feel that you have to respond to me all the time. Feel free to have a conversation with one another about these questions. My role is to ask questions, listen and make sure everyone has a chance to contribute.

We are taping this session because we don't want to miss any of your comments. No names will be included in any reports and your comments are confidential.

Let's begin. To break the ice, let's go around the room one at a time. Tell us your name and what your favourite TV programme is. I will start …

Appendix M Interviews

M.1 Interview Guide

1. Ascertain use of Social Networking Sites (SNSs)
• User / non-user of Social Networking Sites Probes: Sites used? Features used? Sites stopped using? • Intensity of use Probes: How often? For how long? • Sites used Probes: Sites no longer used? • Information placed online Checklist of items • Proficiency with computers? Probes: Able to install new OS, apps etc?
2. General view of SNSs?
Probes: Benefits of using sites (explain and explore)? Risks/dangers of using sites (explain and explore)?
3. Risks and concerns with SNSs for people your age?
• Main risks and concerns (explain and explore)? • Show list of risks generated by focus group Probes: Personally at risk? Friends/classmates at risk? Which risks most serious? Awareness of risks • Compare to survey findings (explain and explore)
4. Dealing with risks?
• How deal with risks (explain and explore)? Probes: Modified behaviour? Changed privacy settings? Personal information online? Awareness of risks • Compare to survey findings (explain and explore) • Trust Probes: SNS sites? SNS companies? Friends on SNSs? • How to reduce these risks (explain and explore)?

Table M.1 Interview Guide for Semi-Structured Interviews

Appendix N Logistic Regression Analysis

N.1 Binary logistic analysis – excessive use risk

Predictor	ß	SE ß	Wald's χ^2	df	p	$e^{ß}$ (OR)	95% CI for $e^{ß}$ Lower	Upper
Constant	-2.228	.362	37.852	1	.000	.108		
Prior Experience (1 = Yes, 0 = No)	.978	.328	8.910	1	.003	2.659	1.399	5.053
Knowledge of Risk	-.153	.054	8.065	1	.005	.858	.772	.954
Concern about Risk	.160	.050	10.077	1	.002	1.173	1.063	1.295
Control of Risk	.175	.047	13.637	1	.000	1.192	1.086	1.308
Age Cohort (Adolescent)			13.829	2	.001			
Age Cohort (Emerging Adult)	-2.380	.641	13.810	1	.000	.093	.026	.325
Age Cohort (Adult)	-.305	.670	.207	1	.649	.737	.198	2.742
Age Cohort (Adolescent) by Prior Experience			13.937	2	.001			
Age Cohort(Emerging Adult) by Prior Experience	2.530	.683	13.711	1	.000	12.554	3.290	47.908
Age Cohort(Adult) by Prior Experience	.152	.921	.027	1	.869	1.164	.191	7.084
Test			**χ^2**	**df**	**p**			
Overall model evaluation								
Likelihood ratio test			162.77	8	.000			
Goodness-of-fit test								
Hosmer and Lemeshow			7.701	8	.463			

Note R^2 = .195 (Cox & Snell), .294 (Nagelkerke).

Table N.1 Logistic Regression Analysis of Perceived Personal Risk of Spending Too Much Time on SNSs (1= High Risk, 0 = Not at High Risk).

N.2 Binary logistic analysis – threatening risk

Predictor	ß	SE ß	Wald's χ^2	df	p	$e^{ß}$ (OR)	95% CI for $e^{ß}$ Lower	Upper
Constant	-2.570	.565	20.671	1	.000	.077		
Prior Experience (1 = Yes, 0 = No)	1.150	.386	8.887	1	.003	3.157	1.483	6.723
Concern about Risk	.453	.072	39.146	1	.000	1.574	1.365	1.814
Age Cohort (Adolescent)			22.257	2	.000			
Age Cohort (Emerging Adult)	-1.199	.260	21.203	1	.000	.301	.181	.502
Age Cohort (Adult)	-1.569	1.056	2.208	1	.137	.208	.026	1.650
Disposition to Trust	-.196	.094	4.325	1	.038	.822	.683	.989
Test			χ^2	df	p			
Overall model evaluation								
Likelihood ratio test			115.08	5	.000			
Goodness-of-fit test								
Hosmer and Lemeshow			6.252	8	.619			

Note R^2 = .148 (Cox & Snell), .273 (Nagelkerke).

Table N.2 Logistic Regression Analysis of Perceived Personal Risk of Being Bullied or Harassed (1= High Risk, 0 = Not at High Risk)

N.3 Binary logistic analysis – reputational risk

Predictor	ß	SE ß	Wald's χ^2	df	p	$e^{ß}$ (OR)	95% CI for $e^{ß}$ Lower	Upper
Constant	-2.741	.325	71.236	1	.000	.064		
Prior Experience (1 = Yes, 0 = No)	1.084	.180	36.212	1	.000	2.957	2.077	4.209
Concern about Risk	.278	.051	29.296	1	.000	1.320	1.194	1.460
Risk Controllable	.139	.045	9.494	1	.002	1.149	1.052	1.256
Age Cohort (Adolescent)			20.685	2	.000			
Age Cohort (Emerging Adult)	-.850	.193	19.340	1	.000	.427	.292	.624
Age Cohort (Adult)	-1.014	.460	4.867	1	.027	.363	.147	.893
Test			χ^2	df	p			
Overall model evaluation								
Likelihood ratio test			119.67	5	.000			
Goodness-of-fit test								
Hosmer and Lemeshow			3.093	8	.928			

Note R^2 = .149 (Cox & Snell), .211 (Nagelkerke).

Table N.3 Logistic Regression Analysis of Perceived Personal Risk of Embarrassing Information or Photos Being Seen by People Who you Would Prefer Didn't See it (1= High Risk, 0 = Not at High Risk)

N.4 Binary logistic analysis – personal information risk

Predictor	ß	SE ß	Wald's χ^2	df	p	$e^{ß}$ (OR)	95% CI for $e^{ß}$ Lower	Upper
Constant	-3.293	.402	67.176	1	.000	.037		
Prior Experience (1 = Yes, 0 = No)	1.441	.337	18.309	1	.000	4.224	2.183	8.173
Concern about Risk	.313	.054	33.352	1	.000	1.367	1.229	1.520
Privacy Concern	.209	.061	11.586	1	.001	1.233	1.093	1.390
Age Cohort (Adolescent)			9.606	2	.008			
Age Cohort (Emerging Adult)	-.634	.207	9.387	1	.002	.531	.354	.796
Age Cohort (Adult)	-.137	.538	.064	1	.800	.872	.304	2.505

Test	χ^2	df	p
Overall model evaluation			
Likelihood ratio test	85.53	5	.000
Goodness-of-fit test			
Hosmer and Lemeshow	16.308	8	.038

Note R^2 = .114 (Cox & Snell), .175 (Nagelkerke).

Table N.4 Logistic Regression Analysis of Perceived Personal Risk of Personal Information Misused by Strangers (1= High Risk, 0 = Not at High Risk)

N.5 Binary logistic analysis – technological risk

Predictor	ß	SE ß	Wald's χ^2	df	p	$e^{ß}$ (OR)	95% CI for $e^{ß}$ Lower	Upper
Constant	-1.705	.397	18.488	1	.000	.182		
Prior Experience (1 = Yes, 0 = No)	1.359	.180	56.765	1	.000	3.891	2.732	5.540
Concern about Risk	.237	.046	26.178	1	.000	1.268	1.158	1.389
Risk Controllable	.121	.043	8.047	1	.005	1.129	1.038	1.228
Trust Beliefs	-.156	.070	5.013	1	.025	.855	.746	.981
Age Cohort (Adolescent)			8.398	2	.015			
Age Cohort (Emerging Adult)	-.534	.192	7.764	1	.005	.586	.403	.854
Age Cohort (Adult)	.072	.508	.020	1	.887	1.075	.397	2.911
Test			χ^2	df	p			
Overall model evaluation								
Likelihood ratio test			121.64	6	.000			
Goodness-of-fit test								
Hosmer and Lemeshow			10.50	8	.231			

Note R^2 = .158 (Cox & Snell), .221 (Nagelkerke).

Table N.5 Logistic Regression Analysis of Perceived Personal Risk of Spam (1= High Risk, 0 = Not at High Risk)