Online Trust:

An Investigation into the Privacy Attitudes and Awareness of Social Network Users in Ireland

Patricia Greene

A dissertation submitted in partial fulfillment for the award of

Master in Business Administration (MBA)

National College of Ireland

Submitted to the National College of Ireland September 2013

Abstract

The evolution of the internet has established new ways for people to communicate online in the form of social networking websites. In the last number of years, social networking has become a worldwide phenomenon. However, these advances in technology have brought with them many ethical issues surrounding consumer privacy. The purpose of this research is to investigate the level of trust in social networking websites among Irish users and to examine if they are aware of how these websites use their personal information.

Drawing on theoretical concepts identified in the literature, the researcher developed and tested a conceptual framework of trust and privacy in social networking websites. Data was collected by means of a web-based questionnaire adapted from a similar study in Finland. The questionnaire was piloted and distributed to a sample of Irish social network users. A total of 150 responses were collected and this data was then analysed using SPSS software.

The findings show that there is a lack of trust among Irish users in the social networking websites with older users less trusting than their younger counterparts. Although users had not read the privacy policy or terms of use, awareness of how their data is shared by social networking websites is high in comparison with previous studies. Despite these privacy concerns, social network users are disclosing vast amounts of personal information on their profile to a large number of people; some of whom they do not know. These results suggest that unlike e-commerce websites, trust is not a necessary requirement for people to actively use social networking websites as users are increasingly willing to trade their privacy for social interaction.

Research limitations mean that generalisations cannot be made on the total population of Irish social network users; however findings show that further research on this topic is required.

Keywords: Online Trust, Privacy, Social Networking.

Submission of Thesis and Dissertation

National College of Ireland

Research Students Declaration Form

(Thesis/Author Declaration Form)

Name: _____

Student Number: _____

Degree for which thesis is submitted: _____

Material submitted for award

(a) I declare that the work has been composed by myself.

(b) I declare that all verbatim extracts contained in the thesis have been distinguished by quotation marks and the sources of information specifically acknowledged.

(c) My thesis will be included in electronic format in the College Institutional Repository TRAP (thesis reports and projects)

(d) ***Either*** *I declare that no material contained in the thesis has been used in any other submission for an academic award.

Or *I declare that the following material contained in the thesis formed part of a submission for the award of

_____

(State the award and the awarding body and list the material below)

Signature of research student: _____

Date: _____

Acknowledgements

I would like to begin by thanking my supervisor Dr. Colette Darcy for all her guidance, support and time throughout this research project.

Secondly, I would like to thank all those who took the time to participate in this study, without you this research would not have been possible.

To the MBA class of 2013, thank you for all your support and for making the last two years such a memorable experience. I could not have asked to do this with a better group of people.

Finally I would like to take this opportunity to thank my family and friends for all their help and support not just during this research but also throughout the past two years. In particular, I would like to thank my parents and my two sisters for all their words of support and encouragement. I could not have done it without you.

Table of Contents

List of Tables

List of Figures

List of Appendices

Chapter 1: Introduction

The evolution of the internet and rapid changes in technology have altered the way business is done globally. It has become necessary for businesses to have an online presence in order to remain competitive. These changes in technology have also established new ways for people to communicate online in the form of social networking websites, such as Facebook, MySpace and Twitter, which have become major global businesses in their own right. In the last number of years, social networking has become a worldwide phenomenon; a 2009 survey conducted by Nielsen found that two thirds of internet users are browsing social networking and blogging sites (Nielsen, 2009). Today more and more people are using digital technology to communicate with each other (Pitkänen & Tuunainen, 2012) According to an Ipsos MRBI survey more than 60% of Irish people have some sort of social networking account (Ipsos MRBI, 2012).

1.1 Privacy Concerns

However, this evolution in technology has brought with it some ethical issues – principally the protection of consumer privacy. There is a growing concern among consumers about how their data is being collected and used when shopping online (Liu, Marchewka, Lu & Yu, 2004). This has resulted in trust becoming a major barrier to online business (Metzger, 2004). Many consumers feel they are losing control over their personal information when making purchases online (O'Brien & Torres, 2012). In contrast to this, many users of social networking sites have no problem with divulging large amounts of personal information on their social networking profiles and many of these users seem to be living their lives online (Rosenblum, 2007).

1.2 Third Party Access to Data

This vast sharing of personal information allows third parties to collect information on user behaviour (Pitkänen & Tuunainen, 2012). Facebook has become the largest consumer database and are now selling consumer information to third parties for market research purposes as a revenue generating method. They have been heavily criticised for the complex nature of their privacy settings, especially with the introduction of default privacy setting in 2009, which makes the majority of user's content viewable to all (Collins, 2010). It is thought that many consumers are unaware that Facebook are collecting data about them as they use the website (Barnes, 2006). There is also the question of whether internet users are knowingly sacrificing their privacy for social gains when using social networking websites. As Levin and Abril (2009) argue, in general, people are willing to compromise their privacy for many different reasons including social, financial, practical or professional.

Whether it is a lack of awareness or willingness to surrender their privacy in the name of socialising, the outcome of divulging personal information online can have negative effects on the lives of social network members. The disclosure of this personal information can be accessed by third parties and used for a variety of reasons. These include prospective employers, who wish to find out more about a particular candidate, University admission boards evaluating prospective students, marketing companies wishing to aim their products and services at a particular audience (Rosenblum,2007) and even burglars monitoring profiles to see when householders are away from home (Tomlinson, 2011).

1.3 Research Objectives

The first objective of this research is to establish what level of trust Irish internet users have in social networking websites. Once this is established, the study aims to identify why Irish internet users trust social networking websites with their personal information and if they are aware how public their personal information is on their social networking profiles. Are they aware how these websites are using their members' data and online movements to target advertising and to sell on to third parties for their own financial gain? The study also aims to discover if Irish users of social networking websites realise the effect making their personal information so public can have on their lives offline.

1.4 Overview of the Research Structure

The research will begin with a review of the relevant literature in the subject area; examining the concepts of trust and privacy and their role in social networking websites. There have been numerous journal articles, reports and books written on the role of trust and privacy online, in relation to both e-Commerce and social networking. However, the attitudes of Irish social network members towards trust and privacy on social networking websites and users awareness of how their data is being tracked and used by both the social networking companies and other third parties, is an area which requires further research. Following on from the literature review, there is an outline of the conceptual model developed for this research and an overview of the research problem and the key aims of the research. There is then an outline of the methodology which will be used to research this problem; describing the philosophy, approach and data collection and analysis methods used for this research as well as the ethical considerations and any limitations of the

research. The data collected will then be analysed using quantitative methods and presented with the use of graphs and tables. The researcher will then discuss the findings and further implications of the results followed by conclusions based on the analysis. The paper will conclude by presenting suggestions for further research in this area.

Chapter 2: Literature Review

2.1 Introduction

While the concepts of trust and privacy have been studied by researchers for many years, trust and privacy in an online environment is an area which has attracted a lot of interest in the last number of years especially with the arrival of social networking websites. There have been numerous theories put forward in the literature to explain how trust affects people's behaviour online. This chapter will firstly examine the constructs of trust and privacy in an offline context before exploring the factors which affect trust and privacy. Finally, the review will focus on how trust and privacy translate to an online environment, in particular with regard to social networking websites.

2.2 Trust

The growth in popularity of online social networking websites has raised many concerns in the area of privacy on the internet. In order to understand the attitudes of internet users to trust and privacy online, it is important to first take a closer look at the concepts and construct of both trust and privacy. Karvonen (2007) argues that, in order to understand online attitudes to trust, it is first necessary to gain an understanding of the concept of trust in an offline environment. Trust is not a new concept and has been studied by behavioural scientists for many years (Deutsch, 1958). According to Lewicki, McAllister and Bies (1998) trust is defined as a *"belief in the willingness to act on the basis of the words, actions and decisions of another"* while Rousseau, Sitkin, Burt and Camerer (1998) define trust as "*a psychological state comprising the intention to accept vulnerability based on positive expectations*

of the intentions or behaviours of another". However Wang and Emurian (2005) argue that trust is an abstract concept, which is difficult to define.

Trust affects almost every aspect of a person's life (Wang & Emurian, 2005). Lauer and Deng (2007) state that trust can be seen from either a social or rational viewpoint, while Fukuyama (1995, p.7) argues that trust plays a vital part in the functioning of society. Trust allows for the building of interpersonal relationships and determines the nature of these relationships (Ridings, Gefen & Arinze, 2002). Roloff (1981, p.16) argues that trust is central to the theory of social exchange. There must be an element of trust existing for a person to disclose personal information (Dwyer, Hiltz & Passerini, 2007). Much of the literature in the area of trust suggests that trust can take different forms (Lewicki, Wiethoff & Tomlinson, 2005, p.256). As Nissenbaum (2001) states trust covers a large variety of relationships – a person can trust or distrust other people, institutions, physical things or systems. While it is true that trust covers a multiple of objects and relationships, Koehn (2003) recognises that there is one common factor which exists when it comes to the concept of trust; *"the expectation of goodwill"*. Zimmer, Arsal, Al-Marzouq and Grover (2010) state that when people display trust, they expect the trusted party will not take advantage although they do not have any control over this. The level to which one individual will trust another can depend on the characteristics of the trustor, similarly the characteristics of the trustee will also affect the level of trust one party has in another (Mayer, Davis & Schoorman, 1995).

2.3 Privacy

The concept of trust cannot be explored without discussing the concept of privacy. Fried (1968) stated that privacy is an instrumental concept as it is required in the development of trust. Joinson, Reips, Buchanan and Schofield (2010) argue that the concepts of both trust and privacy are strongly linked. Like trust, the concept of privacy is difficult to define with many varying definitions of privacy being put forward in the literature (Borna & Sharma, 2011). Many of these definitions centre on the protection of personal information. Westin (1967, p.7) describes privacy as "*the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated*". Liu et al (2004) define privacy as the right of an individual to be left alone and to have the ability to control their personal information. Van Dyke, Midha and Nemati (2007) go along with this statement suggesting that control is central to privacy. Culnan (1993) also argues that in a social context privacy can only exist when an individual has control of their personal information. If an individual has control over their personal information they can determine the level of privacy protection they require (Levin & Abril, 2009).

2.4 Control

Fried (1968) argues that privacy is not only ensuring others do not have information about us, it is also the control we have over our personal information. The breach of consumer privacy is linked with the loss of control on the part of the consumer; of their personal information and links exist not only between privacy and trust but also between privacy and control (O'Brien & Torres, 2012). A consumer must have a level of trust in a business if they are to release control of what they consider to be

personal information to third parties (Olivero & Lunt, 2004). If there are any concerns about the privacy of the information being disclosed, there will be a lack of trust between parties and transactions may not take place (O'Brien & Torres, 2012). However, many users of social networking websites make personal information public without a huge degree of concern for the loss of control over that information (Levin & Abril, 2009).

2.5 Trust & Privacy Online

When the concept of trust moves to an online environment, the importance of trust becomes greater (O'Brien & Torres, 2012). Wang and Emurian (2005) state that although offline and online trust have many similar characteristics, differences do exist. Online trust differs from offline trust as the object of trust online is a website, the internet or the technology (Bart, Shankar, Sultan & Urban, 2005). The evolution of technology; in particular the internet, has required people to provide personal information online for many reasons (Joinson et al, 2010). This release of personal information online is usually a requirement to completing purchases online or accessing particular services (Metzger, 2004). This has led to trust becoming a significant barrier to e-Commerce and there is a perceived lack of trust on the part of consumers when it comes to making transactions online (Hann, Hui, Tom Lee & Png, 2007). Verhagen, Meents and Tan (2006) associate this lack of trust with the increased risk of completing transactions online, there are no longer only two parties involved in the purchase process, an extra factor in the form of an intermediary operating system has now entered the process. There is also a loss of face to face contact with the seller, which increases anxiety and fear among consumers and leads to a lack of trust (Metzger, 2004). As Friedman, Khan and Howe (2000) argue *"people trust people not technology"*.

The manner in which organisations treat the personal information of their customers can cause a number of privacy problems which lead to consumers becoming concerned about the privacy of their personal information (Xu, Dinev, Smith & Hart, 2011). Privacy concerns are not a new issue, privacy was a concern long before the existence of the internet (Cranor, 1999). However, advances in technology now allow organisations to share consumer's personal information with one another (Friedman et al, 2000). Consumers are increasingly concerned with how their personal information is used when making purchases online, however the recording of consumer buying habits is not a new phenomenon. Caudill and Murphy (2000) state that marketers have anonymously monitored consumer buying habits in supermarkets for many years, but the problem with collecting this data online is the loss of this anonymity. In all cases, when buying online, consumers are required to enter their name and address to complete a purchase.

2.6 Trust in Social Networking Websites

Although this lack of trust seems to exist on e-Commerce websites, the landscape changes somewhat when it comes to social networking websites. Boyd and Ellison (2008) define social networking websites as web-based services which allow users to create public profiles, identify a list of other users with whom they share some form of connection and view the profiles of their connections. A profile page is a unique web-page where the user can simply *"type oneself into being"* (Sundén, 2003, p.3). Social networking sites have grown rapidly over the last number of years (Dwyer et al, 2007) and in Ireland 63% of people have a social networking account (Ipsos MRBI, 2012). The central purpose of social networking sites is to build on connections with existing contacts and build networks of new contacts who have similar interests or common connections (O'Brien & Torres, 2012). Boyd and

Ellison (2008) state that the majority of social networking users are not using social networking sites as a forum to meet new people but rather as a means of communicating with and keeping in contact with people who they already know.

Users of social networking websites tend to post vast amounts of personal information on their social networking profiles which would traditionally be classed as private (Levin & Abril, 2009). A social networking profile usually contains a list of identifying features (Mohamed, 2010). The development of online social networks has increased the need for online disclosure (Taddei & Contena, 2013). Grabner-Krauter (2009) remarks that the average social networking profile contains information such as the users home address, where the user went to school and other family details which is exactly the type of information required to reset passwords for confidential websites such as online banking. This openness exposes users of social networks to a greater risk to their privacy (Squicciarini, Xu & Zhang, 2011). According to Sim, Liginlal and Khansa (2012) social network users make what seem to be irrational decisions when disclosing personal information online. Rosenblum (2007) argues that users of social networking websites do not exercise the same caution on these types of websites as they do on e-Commerce websites because they believe they are in a protected environment. Berendt, Gunther and Speikermann (2005) found that often internet users disclose personal information despite stating that they value privacy online. Levin and Abril (2009) state that social network users are inclined to disclose a lot of personal information online, while still expecting to retain a level privacy; while Debatin, Lovejoy, Horn and Hughes (2009) recognise that the need for social interaction can often outweigh privacy concerns about personal data. Many have labelled this type of behaviour a *"Privacy Paradox"* (Barnes, 2006).

2.7 Attitudes to Risk

Metzger (2004) identifies that often individuals weigh up the benefits against risks in social interactions. The use of online communication technology is continually increasing and while there are many benefits in using this technology, this increase in use also brings risks with it (Adams & Sasse, 2001). Zimmer et al (2010) state that *"risk is the product of uncertainty"* and define risk in an online context as *"the expectation of a high probability of loss of control over disclosed information to a website"*. Mayer et al (1995) state that there is only a need for trust when there is a risk associated with a particular situation. The disclosure of personal information carries with it a certain degree of risk (Metzger, 2004). The risk taking behaviour of social network users is the result of trust in the social networking website (Grabner-Krauter, 2009). There are arguments that age is heavily associated with an individual's attitude towards their personal privacy. Traditionally online social networks are used by the younger generation (Levin & Abril, 2009) and as Altman (1977) identifies, attitudes to privacy can differ depending on the life experience of an individual.

2.8 Awareness of How Data is Collected

However these disclosures are more likely the result of a lack of awareness about how private their social networking profiles are. Rosenblum (2007) argues that users do not realise how public and permanent anything that is posted on their social networking profile is and thus tend to lower their guard. Karvonen (2007) agrees with this summation stating that there is a gap between what users of these websites actually know and what they should know when it comes to security online. The vast majority are unaware of the reputational risk which they are leaving themselves open

to (Levin & Abril, 2009). According to Dwyer et al (2007) users of these websites admit to being concerned about online privacy, but are not proactive in taking steps to protect their personal information. Paine, Reips, Stieger, Joinson and Buchanan (2007) found that a major concern among internet users was access to and distribution of personal information. However, users often forget the privacy concerns they have and disclose personal information even when they are not compelled to do so. Especially if the exchange is entertaining or there are perceived benefits in return for revealing the information (Berendt et al, 2005).

Kuzma (2011) states that although social networking websites do have privacy policies many users do not read them. McGrath (2011) found that less than half of social networking users have actually read the privacy policy of the website but more than 86% stated that the privacy policy was important to them. This re-enforces Rosenblum's (2007) opinion that social network users are comfortable living their lives online; however O'Brien and Torres (2012) argue that this is most probably due to a lack of awareness about how social networking websites use members' data. The move to an electronic based society has led to a major reduction in cost of collecting personal information resulting in many companies profiling their customers (Camenisch, Shelat, Sommer, Fischer-Hübner, Hansen, Krassemann, Lacoste, Leenes & Tseng, 2005). Many social networking websites collect user information and use this data for data mining purposes – selling it to third parties or targeting advertising (Dwyer et al, 2007). Kuzma (2011) states that many people are unaware that companies are using various technologies to collect personal information about consumers. This poses many ethical questions about what should be private and what is not (Timm & Duven, 2008).

2.9 Awareness of the Effects of Disclosure

Many users are also unaware of the consequences of making so much personal information available on social networking websites. By posting this information on their profiles users of social networking websites are leaving themselves open to attack or misuse of their information from online crooks, bullies, stalkers and even their own "friends" (Squicciarini et al, 2011). There are numerous consequences when online privacy is violated. By not changing privacy settings on social networking profiles users are leaving themselves vulnerable to attacks not just online but also offline (Rosenblum, 2007). Social networks can provide criminals with a useful tool to gather intelligence, enabling them to carry out their crimes (Weir, Toolan & Smeed, 2011). The safety of their homes can be at risk as many users post information such as when they are going on holidays or going out for the night, making burglars aware that their property is vacant. Tomlinson (2011) states that social networking sites are being monitored by criminals to find potential targets for break-ins. Riots in the UK in 2011 have shown how social networks can have a damaging effect as many of the riot organisers used social networks as a means of gathering support and co-ordinating these riots (Weir et al, 2011). Furnell and Botha (2011) state that social network users need to understand the implications of sharing all this personal information and the tools available for restricting access in order to maintain a level of control over their social network contributions.

Damage can also be done to user's careers if they exercise poor judgement in what they post online or are simply unaware of how public their posts become. Many employers are using prospective employees or even current employees' online presence on social networking websites to make decisions on the hiring or promotion of an employee, disciplinary procedures or terminating an employee's contract

(Genova, 2009). Employers who screen applicants via their social networking profiles state that the information available has an influence on their decision whether or not to hire a particular applicant (Brandenburg, 2008). It may not be the content as such which causes an employer not to hire an applicant, but the lack of judgement shown by the applicant in posting particular information (Rosenblum, 2007). Del Riego, Abril and Levin (2012) recognise that although information posted on a social networking profile is no longer considered to be private or secret; this information can be misused or misinterpreted by employers. The consequences of these violations of privacy can also have a negative effect on the social network websites as if a user feels their privacy has been violated they may leave the social network (Kuzma, 2011). However Levin and Abril (2009) argue that the costs of leaving or switching social networks can be high as users may have to forfeit all posts, photographs etc. if they leave a particular social network.

2.10 Conclusion

The issue of online trust and privacy on social networking websites is an area which is receiving considerable attention and has become a hot topic in recent years with more and more people raising concerns about the privacy of personal information on social media. The spotlight has been placed firmly on this issue following recent events involving the US government and their monitoring of social media. However the literature review established that many social network users are either unaware of the consequences of disclosure of such a vast amount of personal information or they are willing to compromise their personal privacy for social gains.

The literature review demonstrates that attitudes of Irish social network users towards privacy online and their awareness of how their personal information is

tracked is an area lacking in research. Much of the research in this area focuses on Facebook and neglects other large social networking websites. Research published in Finland and the US on this topic have shown that many social network users are unaware of how their information is used therefore the researcher believes that Irish users are also unaware exactly how public their social networking profiles are. This research aims to discover if this is the case.

Disclosing so much personal information online can have major consequences, not only in terms of identity theft and marketing but also on social network users' career prospects and even the safety of their homes and personal possessions. Therefore it is important that further research is carried out in this area.

Chapter 3: Research Question

3.1 Research Problem

The use of online social networking websites like Facebook, MySpace and Twitter has exploded In Ireland in the last number a years; with recent figures showing over 60% of Irish people with social networking accounts (Ipsos MRBI, 2012). Users of these websites are uploading vast amounts of personal information to their profiles with a lot of this data being tracked; by companies to target advertising, by employers to assess potential employees and by criminals to identify potential victims. Much of the literature in the area of online trust focuses on the lack of trust in e-commerce websites or the privacy issues surrounding social networking websites. There is little in the way of research into consumer awareness of how public the data on their social networking profile becomes, how this data is monitored and used once the user has published it to their page, or why Irish internet users have difficulty parting with their personal information when making purchases yet are less cautious when it comes to socialising online. Therefore, it is necessary to conduct a study which explores the attitudes of Irish internet users to online trust and privacy and their awareness of how any information they post online is used by third parties. Are they oblivious to what is going on behind the scenes or is it that they are aware and just do not care? Are they willing to sacrifice personal privacy for social gains?

3.2 Research Questions

The primary objective of this research is to establish what level of trust Irish internet users have in social networking websites and to ascertain if they are aware of how their movements online are tracked and how their personal data on their social networking profile is collected and monitored by various interested parties.

The research also seeks to address the following sub questions:

- Are Irish users of social networking websites willing to forsake their personal privacy in order to socialise online?
- Do different levels of trust exist between different social networking websites?
- Do attitudes to online privacy on social networking websites vary between different age groups?

3.3 Development of Conceptual Framework

As Fisher (2004, p.101-102) states, researchers must define the main concepts of the research topic and identify the relationship between these concepts when developing a conceptual framework. An extensive review of the literature on online trust and privacy on social networking websites was conducted as part of this research which allowed the researcher to create a list of important factors that lead to trust on social networking websites. While Dwyer et al (2007) have suggested a conceptual framework on privacy and trust online, this model only focuses on the sharing of information; it does not include elements of social network users' attitudes or awareness of how their information is used or their attitudes to privacy risks. It also

fails to take into account the element of trust in technology which was identified in the literature review.

The key factors identified in the development of the conceptual framework for this study include:

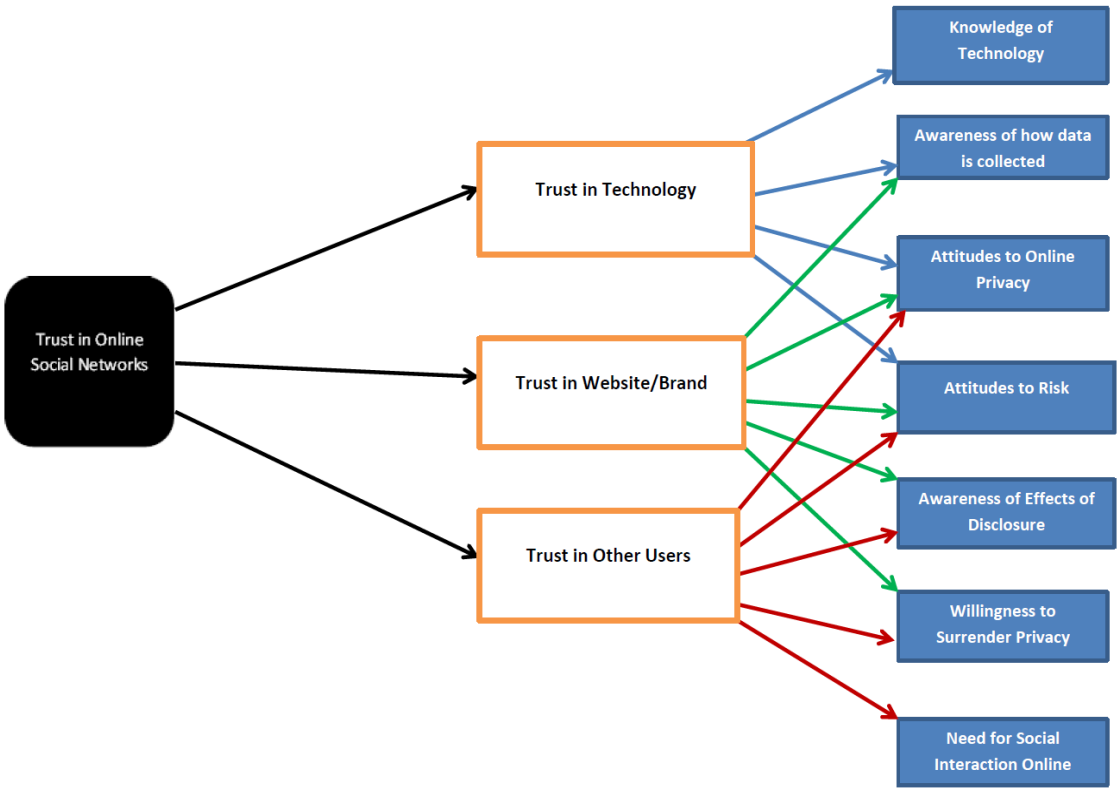
- Knowledge of technology
- Awareness of how data is collected
- Attitudes to online privacy
- Attitudes to risk
- Awareness of effects of disclosure
- Willingness to surrender privacy
- Need of social interaction

These factors relate to three key components which lead to trust in online social networks: Trust in Technology, Trust in Website/Brand and Trust in Other Users.

The conceptual model developed for this research builds on Dwyer et al's (2007) model by integrating not only the formation of new relationships and sharing of information on social networking websites but also social networks users awareness of how their data is used, attitudes to risks associated with information disclosure, trust in the technology used and users need for social interaction versus privacy concerns.

This study will use the model outlined in figure 3.1 to test trust and privacy on online social networking websites. This conceptual framework will help provide the responses to the research questions identified earlier in this chapter.

Figure 3.1: Conceptual Model of Trust & Privacy in Social Networking Websites



Chapter 4: Research Methodology

4.1 Introduction

The primary objective of this research is to investigate the attitudes and awareness of Irish users of social networking websites towards privacy online by examining how much information they disclose on their social networking profile and their awareness of how these websites use their data. As discussed in the literature review, online privacy on social media websites is a topic which is gaining a huge amount of interest. This chapter will discuss the research philosophy, approach and design used for this study. The population and sampling method and data collection method used are also described along with the ethical considerations and limitations of the research.

4.2 Research Philosophy

Researchers must be aware of their philosophical approach to research as this will not only influence what the researcher does but also how the researcher analyses the topic being studied, which causes the researcher to approach the subject in a certain manner (Gill & Johnson, 2010, p.187). Although the research in this study will be influenced to some degree by practical considerations as discussed by Saunders, Lewis and Thornhill (2012, p.128), the researcher is aware that the primary influence will be the researchers own view of the world.

The primary data collected for this research examined the attitudes and awareness of Irish social network users in relation to online trust and privacy. The researcher adopted a positivist epistemology in collecting this information. Positivism is associated with the epistemological viewpoint that knowledge is based on *"what can*

be observed and experienced" (Williamson, 2006). Positivists believe it is possible to observe social reality objectively with no interaction between researcher and participants (Collis & Hussey, 2009, p.56). This is in contrast to Interpretivism, which is concerned with people's experiences and the belief that the social world is different from the natural world (Williamson, 2006). In gathering data through web-based questionnaires, the researcher has displayed a positivist stance as there was no direct interaction with participants.

One of the key principles of positivism is that the literature is used to form hypotheses which can then be tested (Bryman & Bell, 2007, p.16). Following a review of the literature surrounding online privacy and social networking the researcher developed the research questions/hypotheses outlined in the previous chapter. As argued by Saunders, Lewis and Thornhill (2012, p.134) credible data can only be produced when phenomena are observed, therefore the researcher believed that adopting a positivist approach was the most appropriate way to examine the phenomenon surrounding social networking.

An essential element of the positivist epistemology is that the researcher must be objective in their approach. Objectivism is concerned with an ontological position that social phenomena are external facts which cannot be influenced by the researcher (Bryman & Bell, 2007, p.22). The ontology of this research involves an objective approach as the researcher was independent of the research participants. By using web based surveys the researcher was able to ensure that they were distanced from the research subjects completing the questionnaire thus allowing the researcher to approach the results objectively.

From an axiological point of view, this research adopted a value free and an unbiased approach. Axiology is the role values play in the research process, the value free approach taken by the researcher in this study is in line with the positivist stance adopted for this research (Collis & Hussey, 2009, p.59). Through the adoption of web-based questionnaires, the values of the researcher could not influence the research participants as there was no interaction between the researcher and the participants when the questionnaires were being completed.

4.3 Research Approach

There are two types of research approach a researcher can assume – deductive and inductive reasoning (Saunders et al, 2012, p.143). Deduction is associated with developing a theory before gathering any data with the aim of testing that theory (Horn, 2009, p.197) and inferences are made based on this testing (Collis & Hussey, 2009, p.8) whereas an inductive approach involves gaining a better understanding of a situation before any theory is formed (Saunders et al, 2012, p.146). The approach a researcher adopts is dependent on their philosophical position. Positivists tend to use a deductive approach whilst interpretivists adopt a more inductive approach (Bryman & Bell, 2007, p.28).

Due to the positivist stance adopted by the researcher, the research approach for this study was primarily deductive in nature; however there is an element of the inductive approach in the study as the questionnaire distributed to collect data contained some open questions. As Bell (2010, p.6) argues that although a researcher may select a certain approach this does not necessarily mean they cannot move away from methods usually associated with that approach. This study was primarily deductive due to the quantitative method of questionnaires used by the researcher to collect

data on the subject of online trust and privacy on social networking websites. This allowed for statistical data to be collected and used to test the research questions formulated following the literature review, which then allowed the researcher to draw conclusions on the subject. The inductive element came from the three open questions included in the survey which cannot be easily statistically analysed as there is such a diverse range of answers which can be given with these types of questions, therefore there is an element of the researcher needing to interpret the data provided in these questions. Often there is a need in research for both approaches to be used (Horn, 2009, p.108).

4.4 Research Design

The research design for this study involved using a quantitative approach. Quantitative research is associated with numbers and the testing of theories by examining the relationship one set of variables has to another (Creswell, 2009, p.4). The objective of this research to examine the attitudes and awareness of Irish social network users towards privacy online called for the use of a representative sample which needed to be large given the population being researched. Qualitative research methods are not practical for large samples, therefore quantitative methods were selected for this study. For the purposes of this research a survey research design was utilised, as stated by Bryman & Bell (2007, p.56) survey research design is a method in which data is collected mainly by questionnaire or structured interview and examines more than one case. Interviews were considered for this study but given the time constraints of this research, were not practical as to conduct interviews with a large enough sample would not have been possible. Also, due to the nature of the topic of online trust and privacy, the researcher ruled out interviews as a method of primary data collection as it would not allow for anonymity which may have

deterred participants from taking part in the study. Previous research in the area of online privacy on social networking websites such as O'Brien and Torres (2012) and Pitkänen and Tuunainen (2012) have adopted this method of collecting data. Therefore the researcher deemed the survey method suitable for the purposes of this study.

4.5 Questionnaire

The primary data for this research was collected by means of a cross-sectional web-based survey. Survey research allows researchers to gather numeric data to describe trends, attitudes and opinions of a population (Creswell, 2009, p.12). A cross-sectional study is used when there are time constraints or limited resources available (Collis & Hussey, 2009, p.77). While there are some weaknesses associated with survey research; such as low response rate and the possibility of participants providing false information, questionnaires have many benefits as they allow researchers to gather large amounts of data in a short space of time and at a low cost (Denscombe, 2003, p.27). Due to the time constraints which existed to complete this research by the September 2013 deadline and the subject of the research, this type of quantitative data collection was deemed most appropriate by the researcher. Given the target population for the survey consisted of social network users, the researcher believed a web-based survey was the most appropriate method to collect the required data. A web-based survey was also identified as a suitable method as it assisted with a quick rollout of the survey. It also enabled the researcher to collect the data in a fast and efficient manner. Bryman and Bell (2011, p.668) state that web-based questionnaires are more economical, have faster response rates, are more attractive, are easier to administer and have fewer unanswered questions. A web-based questionnaire was also appropriate for this research due to the nature of the topic

under investigation, online trust; the researcher felt that participants were more likely to give honest answers as they were not dealing directly with the researcher. As the topic is quite sensitive, an anonymous questionnaire made it easier for the researcher to gather the relevant information.

Although there are a large number of companies providing online survey building and distribution services, Survey Monkey is one of the most well-known brands. As people tend to trust brands they know and the topic under investigation centred on trust and privacy in an online environment, the researcher believed using a well-known provider would increase the rate of response. The use of web-based survey programmes such as Survey Monkey allow for easier analysis as data can be easily exported to other programmes.

As previously discussed Pitkänen and Tuunainen (2012) recently carried out research on attitudes and awareness of online privacy among Facebook users in Finland. The questionnaire used in this research was adapted from Pitkänen and Tuunainen's (2012) questionnaire to suit the study of online trust and privacy on social networking websites among Irish users. Bryman and Bell (2007, p.274) recommend that researchers consider using survey instruments which have been devised for other research as they have already been tested for reliability and it can enable researchers to compare their findings to other research studies. The questionnaire used by Pitkänen and Tuunainen (2012) included questions related to accessing social networks through mobile internet and questions related specifically to Finnish users. These questions were not relevant to this particular research and were therefore removed when developing the new questionnaire. As this study focussed on Irish social network users and concerned gathering data on multiple social networks; not

just Facebook, many of the questions were modified in the designing of the new questionnaire in order to fit this study.

The questionnaire used by Pitkänen and Tuunainen (2012) and adapted for this study comprised of six sections – 1. Background information, 2. Participants' use of social networking websites, 3. Privacy control, 4. General privacy and data concerns, 5. Social network privacy and data concerns and 6. Privacy policy on social networking websites. The questionnaire consisted of forty questions in total and used a combination of open and closed questions. The first part of the questionnaire was used to collect some demographic and background information relating to participants use of social networks, however to ensure confidentiality and anonymity was upheld, the questionnaire did not pose any questions which would identify participants. Thirteen questions required respondents to give their answer using a seven point Likert scale. Participants were asked to state their level of agreement or level of importance they gave a particular issue by selecting their answer from the options provided. The options were "strongly disagree", "disagree", "somewhat disagree", "neither agree nor disagree", "somewhat agree", "agree" and "strongly agree". The scales used in the questionnaire were the scales used by Pitkänen and Tuunainen (2012) and were already validated. The questionnaire also included open questions which allowed participants to give their opinion on the topic. This provided the researcher with further insight into the research problem by allowing respondents to give their opinion and give any thoughts they had on the subject of online trust and privacy on social networking websites. The open questions also ensured that all possible answers had been covered.

4.6 Validity & Reliability

As discussed the scales used were those from Pitkänen and Tuunainen's (2012) study of online privacy on Facebook in Finland and were therefore already validated. However, as the researcher adapted many of the questions to suit this study, it was necessary to re-test the validity of the questionnaire. The researcher re-tested the internal reliability of the questionnaire through the use of Cronbach's Alpha. Pallant (2001, p.85) states that values should be above .7 to indicate reliability. The Cronbach's Alpha values are given in table 4.1 below.

Table 4.1: Cronbach's Alpha Results

Scale	Online Trust	Trust in Social Networking Websites	Trust in Other Users
Cronbach's Alpha	0.732	0.704	0.702

All values are above 0.7 which indicates that the scales are reliable. If a survey instrument is modified or uses a combination of instruments the reliability and validity of the original instrument may not remain (Creswell, 2009, p.150). In order to further re-establish the reliability of the questionnaire a pilot test was conducted.

Pilot tests are necessary to ensure questions are phrased correctly, respondents understand the meaning of the questions and to check if the range of responses is adequate (De Vaus, 2002, p.114). The pilot questionnaire was sent to ten respondents via e-mail who fell within the target population. According to Fink (2003, p.108) a minimum of ten people is required for a pilot test while Saunders et al (2012, p.451) state the number of pilot questionnaires sent out is dependent on the size of the study. As Bell (2010, p.151) suggests the pilot test participants were asked to give feedback on the length of time the questionnaire took to complete, if the instructions

were clear, whether any questions were ambiguous and if so which questions, if they were comfortable answering each question, if they felt anything was overlooked on the topic, if the layout was clear and for any other feedback they had on the questionnaire. Following the completion of the pilot test the researcher made some minor amendments based on the feedback given.

The use of Survey Monkey to draft and distribute the questionnaire also contributed to the reliability of the research as it has an automatic data completion function which helps reduce human error in data input (O'Brien & Torres, 2012).

4.7 Population & Sampling

This study aims to determine the level of trust in social networking sites which Irish people have and their awareness of how their data is tracked and managed by these websites. One in five Irish people have a Twitter or LinkedIn account and more than 50% of the Irish population now use Facebook (Ipsos MRBI, 2012). Therefore, the researchers target population will be Irish users of social networking websites. Although Facebook is the most widely used social networking website in Ireland, with approximately 58% of Irish Facebook users visiting the site each day, the researcher has decided not to limit the research to Facebook users but rather get the opinion of users of various social networks. This will enable the researcher to determine if user perceptions vary between the different social networks, thus answering research sub question 2.

Having evaluated the different sampling techniques to determine what type of sampling is suitable for the data collection in this study, the researcher has decided to use non-probability sampling as this type of sampling is suitable due to the time constraints surrounding this research. As Jankowicz (2005, p.202) states, using non-

probability sampling helps researchers to gain a variety of different viewpoints in a short space of time within the chosen population. Although probability and random sampling was considered for this study the researcher has decided to adopt a snowball sampling technique to collect the required data. Snowball or network sampling is a method by which new respondents are chosen by those who have already taken part in a study (Biernacki & Waldorf, 1981). According to Gomm (2009, p.313) snowball sampling can be used not only for difficult to reach groups but also where the objective of a study is to explore social networks, therefore the researcher believed that as this research is examining online privacy on social networking websites, snowball sampling is a suitable method of achieving this. Denscombe (2003, p.16) states that snowball sampling is very effective for building up sample sizes especially when the research project is small in scale. While snowball sampling is more common in qualitative research, the researcher believes this technique will also work in this quantitative study as it will allow the researcher to access a wider range of subjects than those in the researcher's own network, therefore, being more representative of the population being studied.

The sample for this research was a network of users from various social networking websites; however it was felt that the researcher would not gain a wide variety of age groups by just using their own social network connections, thus making the study somewhat biased. Therefore friends of friends were also invited to take part in the study through the snowballing method of sampling. This method provided the researcher with greater ease of access to the target population. Using the snowball method also enabled the researcher to gain access to social network users from a variety of age groups, thus helping to determine if there is a link between age and

attitudes to privacy on social networking websites. This will allow the researcher to answer research sub question three.

4.8 Data Collection

Following the amendments based on the pilot test feedback the final questionnaire (appendix B) was distributed using two methods- through social networking websites and via e-mail. Firstly the questionnaire was sent to the researcher's social media contacts on Facebook, Twitter and LinkedIn and a link to the questionnaire was also posted on the researchers profiles on each of the three websites. Questionnaires were also distributed via e-mail to contacts of the researcher who are social network members but do not log onto their social network profiles very often. This was done in order to ensure the researcher got the opinions of all types of social network users not just those who are very active on social media as this enabled the researcher to gain a better understanding of the different levels of trust Irish people have in social networking websites. The researcher believed that only distributing the questionnaire on social media would not give a full picture of Irish attitudes and awareness of online trust and privacy on social networking websites and there would have been an element of bias.

As discussed the snowball sampling was employed for this research whereby participants were asked to pass on the questionnaire to others in their own network who would be interested in taking part in the study. Each questionnaire was accompanied by a cover letter (Appendix A) which explained the background of the researcher and the purpose of the research. The cover letter also included how long the questionnaire would take to complete and instructions on completion as well as informing participants that their responses were anonymous and entirely

confidential. According to Dillman (2007) information contained in the cover letter which accompanies a questionnaire can have an effect on the response rate. By including the above information the researcher sought to maximise the rate of response as this information can motivate respondents to answer the questions (Sekaran & Bougie, 2009, p.205). The questionnaire was available for four weeks and a follow up reminder was sent after two weeks in order to increase the response rate. Bryman and Bell (2007, p.244) state that follow up reminders can be very effective in increasing response rates.

4.9 Data Analysis

SPSS was the tool used to analyse the data collected for this research. In total 150 responses were received. On August 9th 2013 the data files were downloaded from Survey Monkey. Survey Monkey enables users to download data in Excel format and applies coding so that it can be imported into SPSS. According to Bryman and Bell (2007, p.676) this is one of the major advantages of using web-based survey software as it removes the somewhat daunting task of coding huge amounts of data. As Jankowicz (2005, p.311) recommends the researcher eliminated any unusable questionnaires due to respondents failing to answer a large number of questions. Having formatted the file and removed any unusable responses, the researcher uploaded the file to SPSS and carried out descriptive and inferential statistical tests on the data collected. As mentioned, Cronbach's Alpha was also used to re-establish the reliability of the questionnaire. A copy of the coding used to analyse the data collected for this study is SPSS is available in appendix C.

4.10 Ethical Considerations

It is essential that the rights of any person involved in research are protected (Parahoo, 2006, p.111-112) and researchers must anticipate any ethical issues which could potentially arise during the course of the research (Creswell, 2009, p.87). During this study the researcher ensured that ethical standards and principles were upheld. The researcher abided by the ethical principles described by Bryman and Bell (2007, p.132-133) by including a cover letter with the questionnaire which included a brief explanation of the purpose of the questionnaire and also details of the estimated time required to complete it, thus ensuring respondents were fully aware why the research was being conducted and how much of their time would be taken up in completing the questionnaire adhering to the principle of transparency.

The questionnaire did not require participants to provide their name which protected their anonymity and confidentiality, which according to Sekaran and Bougie (2009, p.221) is one of the main obligations of a researcher. The use of a web-based questionnaire also helped to preserve the anonymity of participants as this meant there was no face to face interaction and although the questionnaire was distributed to the researcher's social networking contacts, the only identifier on responses is the IP (Internet Protocol) address each participant used to access the questionnaire. Therefore the researcher is unable to identify individual participants

All data collected was for the purpose of this study and the researcher ensured the data collected for this study was stored securely and password protected. The data will be destroyed once it is no longer required for the purposes of this research. These steps undertaken by the researcher will ensure the rights of all research

participants are protected. The researcher has also offered all participants the opportunity to view the findings of the study should they wish to see them.

4.11 Limitations of the Research

As with all research there were some limitations associated with this study. While the researcher was successful in accessing a variety of age groups as the questionnaire was distributed through the researchers social networking contacts the age group with the highest response rate was 25-34 – the researcher's age group. Therefore there is a possibility of response bias due to this fact.

The nature of the topic may also have had an effect on the research findings. People who felt strongly about the issue of online privacy on social networking websites may have been more likely to respond than those who have no issue with it, thus skewing the results and could be seen as a limitation to the research.

Like all social research questionnaires there could be a risk of response bias which would affect the validity of results. As Saunders et al (2012, p.381) state in order to paint themselves in a favourable light respondents often feel the need to give socially desirable answers. However, in an effort to combat this limitation the researcher stressed to all participants that responses were completely anonymous and the questionnaire did not request names or other personal information which could identify a participant.

The researcher would have liked to get a larger number of respondents as it would have provided more robust results, but due to time constraints to get the research completed within the required timeframe this was not possible. However the

researcher feels that the data obtained is an accurate reflection on the opinions of social network users in Ireland.

Chapter 5: Findings

5.1 Introduction

This chapter will present the findings of the data collected through the questionnaire. Firstly the researcher will outline the background information of participants and their social network membership. Following this the major themes of the analysis will then be discussed. These themes are:

- Information Disclosure
- Protection of Privacy
- Online Trust
- Trust in Social Networking Websites
- Trust in Other Users
- Awareness of Data Collection
- Future Use

The data collected through the open feedback questions will be presented along with the statistical data.

5.2 Background Information

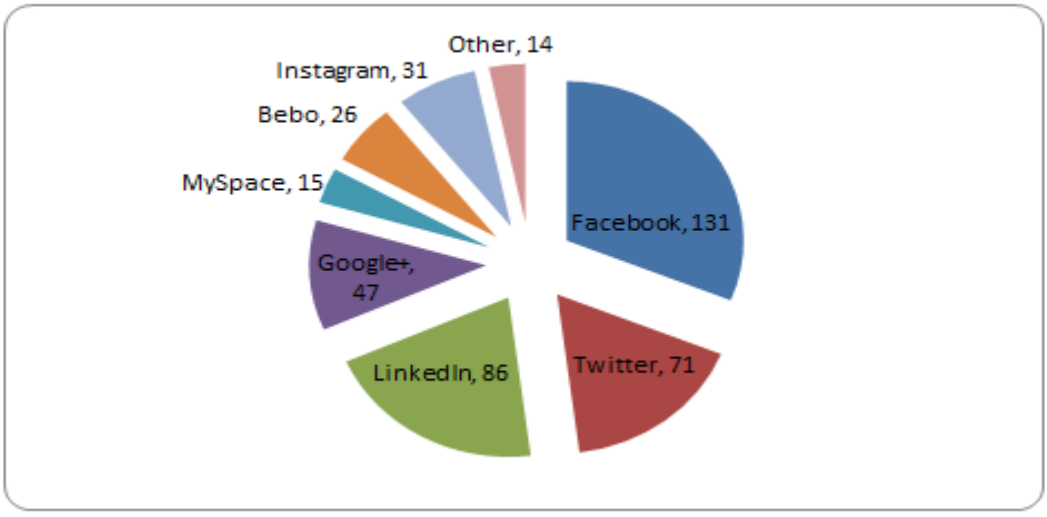
Following the distribution of the questionnaire a total of 150 responses were received. Of these the researcher discounted 7 responses from the data analysis as more than half of the questions from these participants were not answered and were therefore deemed unusable. Of the 143 valid responses 68.5% (n=98) were female and 31.5% (n=45) were male. While responses were received from all age categories included in the questionnaire, the highest proportion of respondents (47%) fell into the 25-34 age group. Most of the respondents (84%) stated that their level of

technical knowledge was average or above average. Approximately 18% of participants availed of the opportunity to provide a response to the open feedback question at the end of the questionnaire.

5.3 Social Network Membership

Figure 5.1 below gives a breakdown of which social networks respondents were members of. Facebook was the most popular social network with 92% (n=131) of respondents stating that they were members. LinkedIn was the second most popular social networking website among Irish users with 86 respondents claiming membership. The findings also show that photo sharing social networks such as Instagram and Pinterest, which are relatively new, are increasing in popularity among Irish users. 31 respondents were members of Instagram, while Pinterest was mentioned frequently in the other category. These findings are broadly in line with the research carried out by Ipsos MRBI (2013). Over two thirds of respondents stated that they have two or more social networking profiles and the majority have been online social network members for between three and five years.

Figure 5.1: Social Network Membership



The most common reason for joining a social network was to keep in touch with existing friends and family with 81.6% of respondents selecting this option. The second most popular reason was "*everyone I know has a social networking profile*" (44.7%). Other common reasons for joining social networks were *"to track down old friends and family"*, *"a friend suggested it"* and *"to find a job"*. Interestingly many respondents are using social networks to gain recognition for their business. No respondents checked the *"to find a date"* option which indicates that Irish users are joining social networking websites merely with friendship in mind. However, it may be that respondents were reluctant to admit this was among their reasons for joining. Table 5.1 shows the full breakdown of responses. We can see from this that socialising online is clearly the main reason Irish people join social networks. This concurs with previous research carried out by Pitkänen & Tuunainen (2012) in Finland and Govani and Pashley (2005) in the United States.

Table 5.1: Reasons for Joining Social Networks

Questionnaire item	**n**
To keep in touch with existing friends & family	115
"Everyone I know has a social networking profile"	63
To track down old friends & family	60
A friend suggested it	48
To find a job	28
To express opinions	22
Other	13
To find people who share my interests	12
To promote my business	12
To meet new people	8
To find a date	0

Just over 40% of respondents have more than 200 contacts on their social networking page while 34% (n=38) are connected to between 100 and 200 people on their profiles. Users in the 35+ age categories have the fewest contacts; only 13.3% in these age groups have more than 150 contacts. The most common type of contacts Irish users have requested connections with on social networking websites tend to be friends (84%), close friends (78%), family (73%) and people they know (67.2%). However, over one fifth of respondents have requested people they have met just once, while 7.5% have requested people they have never met. When it comes to accepting requests to connect, Irish users seem to be even less cautious with over one third (34.3%) accepting people they have only met once and 10% accepting requests from total strangers. This however may be due to the nature of the social network which respondents are members of. For example, it is common for users of Twitter to "follow" celebrities and well known personalities and for those people to "follow" back despite the fact that they may have never met.

5.4 Information Disclosure

It is clear from Table 5.2 that Irish social network users are sharing vast amounts of personal information on their social networking profiles. Two respondents declined to share the information they include on their profiles. Almost all respondents who did answer this question (93.6%) included their full name and most uploaded photographs of themselves (82.3%), photographs of friends and family (66%), their hometown (66.7%) and educational information (66.7%). While the results show that users are in general less likely to share information such as their contact numbers and street address, as many as 10% of Irish users are disclosing their contact phone number and 3% are including their home address. This is exactly the type of

information that is required for identity theft and it seems from these results that a number of Irish social networking users are knowingly disclosing this data.

Table 5.2: Personal Information Included on Profile

Questionnaire item	n
Full Name	132
Photographs of you	116
Hometown	94
Education Information	94
Photographs of friends & family	93
Date of Birth	88
Work Information	76
Relationship status	61
E-mail Address	56
Family Members	44
Skills & Expertise	29
Religious Views	16
Contact Number	14
Political Views	14
Street Address	4
Other	3

It is not only the type of information that Irish users are disclosing which is a cause for concern; it is also who they are sharing it with. While the majority of respondents (70.7%) are aware who can see their social networking profile, a large proportion; almost 30%, did not know who could see their profile and the information contained in it. When cross referencing the information Irish social network users disclose with the types of friends requested approximately 23% shared photographs of themselves and photographs of friends and family with people they have never met or met just once. 24.8% are sharing their full name, 16% are sharing their date of birth and 15% are sharing work information with people they don't know or people they have only

met once. Much higher results were found when cross referencing information disclosure with types of contacts accepted by Irish social network users, with 42% of respondents sharing their full name and photographs of themselves with contacts they have never met or met just once. By disclosing this information to strangers, Irish users of social networking websites are leaving themselves open to online threats such as identity theft.

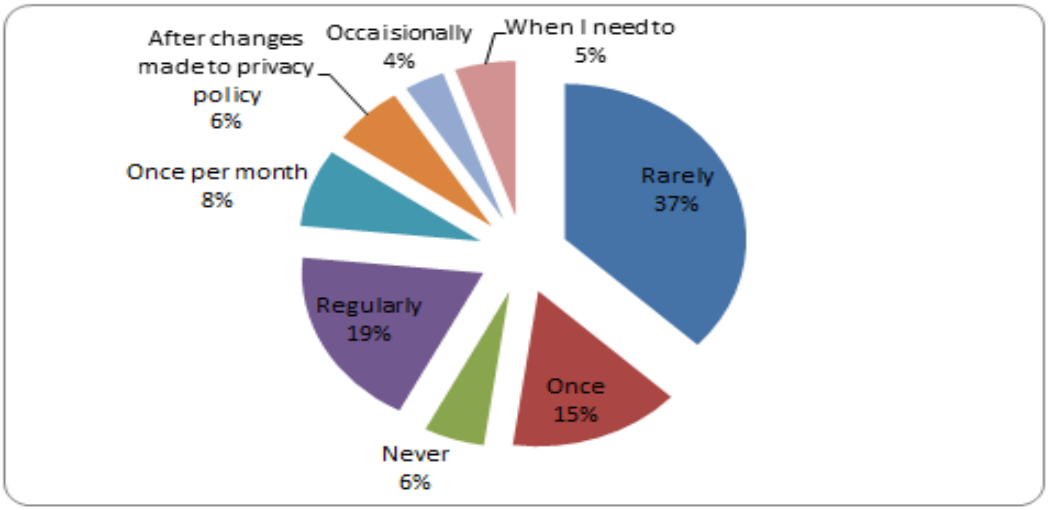
When asked if they were worried about their privacy on social networking websites, a large number of respondents admitted that they were worried about data security while using social networks, yet it seems from the information they disclose this worry is not affecting their behaviour when using these websites. Following the conducting of a one way ANOVA there was no significant difference found between a user's age and concern about posting personal information on social networks. However, there was a significant difference ($p=0.001$) in the number of contacts Irish users have and the age of a user. There was a large difference between the number of contacts an 18-24 user has and the number of contacts those in the 45+ age groups have. This indicates that older users of social networks seem to be more cautious than younger users about the amount of people they share their personal information with.

5.5 Protection of Privacy

Almost all respondents (98.6%) were aware that privacy settings could be changed with 90% stating that they had used their privacy settings at least once. However, when asked how often they updated their privacy settings figure 5.2 shows that only 18% of those respondents who answered this question updated their privacy settings

on a regular basis, while even fewer (6.3%) changed their privacy settings after there had been a change made to the privacy policy.

Figure 5.2: Frequency with which Users Change Privacy Settings



Although 90% admitted to having used their settings, approximately 30% of respondents did not know who could see their profile. It is difficult to determine from this if users had merely a recollection of viewing the privacy settings on setting up their account or they did not want to admit that they had never used the privacy settings.

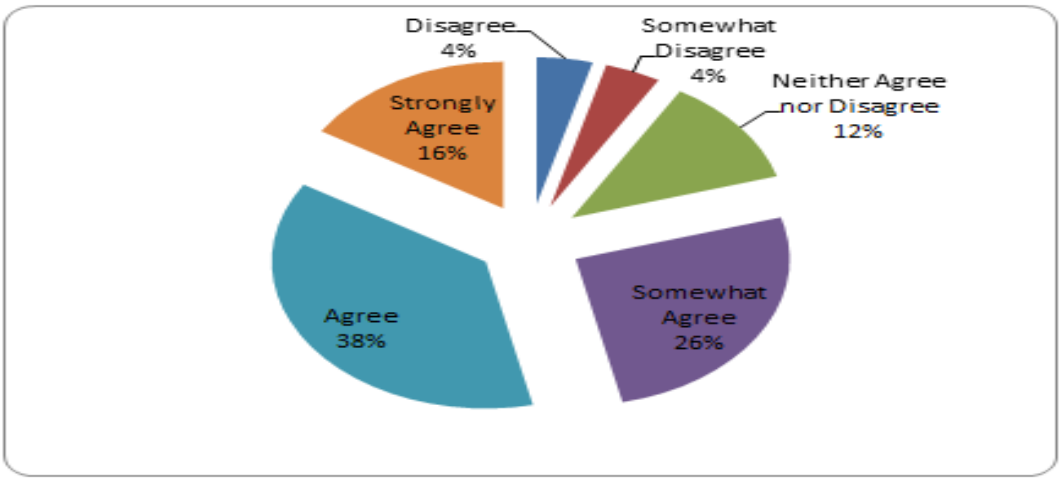
Just under two thirds of respondents (63.8%) have not read the privacy policy of the social networks which they are members of and only 30% have read the terms of use of the social networking websites they use. There was no significant difference found between age of user and those who have read the privacy policy. At the end of the questionnaire, there was an open question which asked if the questionnaire would affect their future use of social networking websites, of the 25 respondents who entered a free-text response the majority stated that they would consider reading the privacy policy or that they would update their privacy settings more regularly with

comments such as *"I will look at my privacy settings again"*, *"Even though they don't make it easy I will consider printing off the terms and conditions"*, *"I will read the privacy policy and terms of use and update my privacy settings more regularly"* and *"I will be updating my privacy settings more often"*. This shows that if users are asked to consider their attitude to privacy it will encourage them to be more proactive about protecting their personal information.

5.6 Online Trust

From the data collected, it was found that Irish social network users have privacy concerns when using the internet with 80% of respondents agreeing to some extent that they worry about their privacy when using the internet in general. The breakdown of responses is shown in figure 5.3 below.

Figure 5.3: Internet Privacy Concern



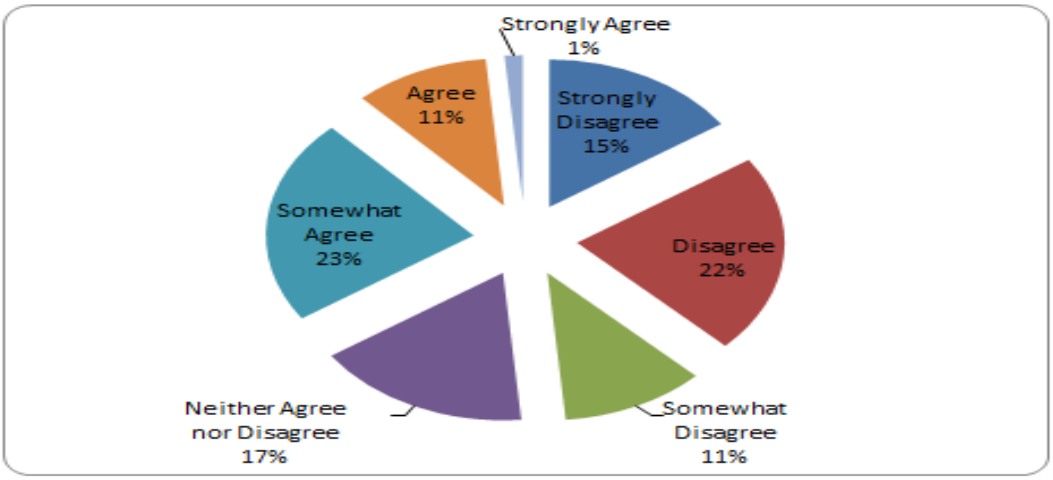
Many respondents (68.4%) are concerned about using their credit card online, however a larger than expected number (22%) stated that they were not worried when shopping online with their credit card. In the free text question at the end of the questionnaire one respondent commented *"I am not concerned with safety or*

security online, worries over credit card fraud are in my experience unfounded. I only purchase from legitimate websites or use PayPal for low priced items". While there is still a trust issue when using credit cards online, it seems that people's perceptions are changing in relation to shopping online.

5.7 Trust in Social Networking Websites

When it comes to trust in social networking websites the majority of respondents (69.5%) stated that they worried about their privacy and data security on social networks with almost half (48.6%) of Irish social network users claiming that they did not trust social networking websites with their personal information. However, it should be noted that a large number of respondents did not state whether or not they trusted social networks with their information.

Figure 5.4: Trust in Social Networking Websites



From the cross referencing of data, it appears that the level of trust Irish users have in social networks does not differ greatly between the different social networking websites. Twitter users had the highest level of trust, while MySpace had the lowest, however only 14 respondents stated that they were members of this network. A one

way ANOVA was conducted to determine if trust in social networking websites differed across age groups. There was a significant difference (p=0.036) found between 18-24 year-olds and 25-43 year-olds in relation to the level of trust they have in social networking websites. Interestingly, there was no relationship found between the level of technical knowledge respondents had and trust on social networking websites.

5.8 Trust in Other Users

Similarly to research conducted by Pitkänen and Tuunainen (2012) in Finland, the majority of respondents (78.1%) agreed that identity theft was a real risk in the online environment with 60% admitting that they worry about people not being who they say they are. However, in the social network environment this concern seems to be significantly reduced, with almost three-quarters of respondents stating that they were comfortable writing on their contacts' profiles. There is somewhat of a contradiction here as 52.2% of respondents said they worried about what other users may write about them on social networking websites and that false information may be posted about them. This indicates that although Irish social network users seem to trust their contacts, they lack trust in other users of these websites. When examining the lack of trust respondents have in other social network users the findings show that there is no one particular social networking website where lack of trust is higher. Notably age was statistically significant (p=0.045) in the level of trust respondents have in other users. Those in the 18-24 age group seem to be more trusting of other social network users than those in the 45-54 and 55-64 age categories.

5.9 Awareness of Data Collection

One of the main aims of this research was to identify if Irish users are aware of how social networks track their movements and share their data with third parties. The results show that awareness of how data is used by social networking websites is high, with 73.8% of respondents stating that they knew social networking websites could share user information with other companies for marketing purposes. When cross referencing users who have read the privacy policy with users who were aware about how social networks share their data, it was found that those who had read the privacy policy were more likely to be aware of how their personal information was used by these websites. More than two thirds of respondents (67.8%) knew that adding an application or game to their social networking profile allowed the developer of the application to access their profile information. When examined more closely it was found that this awareness was more prevalent among younger users. This may be due to the fact that younger users are more likely to download applications than older users and therefore have more knowledge of privacy surrounding the downloading of these applications.

5.10 Future Use

To further gauge users' attitudes to privacy on social networks, the penultimate question asked respondents if the information in the questionnaire would affect their future use of social networking websites. Interestingly 62% of respondents said that their future use of social networks would not be affected by the issues discussed in the questionnaire. Of the 38% of respondents who claimed they would review their use of social networks many stated that they would be more aware of the information they disclose on social networks with one user commenting *"I genuinely was not*

aware of the fact that I shared so much information on my Facebook page" while another stated *"I will be more careful with the information I provide"* but for the most part comments made for this question were along the lines of "*it made me more aware of my privacy while online"*, *"I will have to rethink my privacy on Facebook"* and *"I think I will be updating my privacy settings"*. This information would suggest that although there is some concern about the practices of social networking websites most Irish users are not willing to change their behaviour when it comes to socialising online, despite the dangers associated with it.

5.11 Other Factors

As mentioned, the last question in the questionnaire gave respondents the opportunity to give their opinions on the topic. Of the total number of respondents, 25 took the time to answer this question. One of the main themes which emerged in these responses was the issue government monitoring of social networking websites and their requesting of user information from these websites. One respondent commented that they hoped the information could be used *"to prevent large companies such as Facebook from being allowed to pass on your information to governments"* while another respondent stated *"it is governments and corporations who will ultimately struggle the most with loss of privacy as they have the most to hide"*. Given the recent news stories surrounding the revelations of US government monitoring of social networking websites, it is perhaps unsurprising that this issue has emerged and has most likely put privacy on social networking websites to the forefront of Irish users' minds.

5.12 Summary of Key Findings

Facebook is the most widely used social networking website among Irish users who took part in this research. Although the majority of respondents agreed that identity theft is a risk online, many users are divulging large amounts of personal information on their social networking profile. Table 5.3 shows the top five things respondents stated they include on their profile.

Table 5.3: Top 5 Pieces of Information Included on Social Networking Profiles

Information	n
Full Name	132
Photographs of you	116
Hometown	94
Education Information	94
Photographs of friends & family	93

While almost all respondents are aware that privacy settings can be changed, only a small number change their settings on a regular basis. The majority of those who took part have not read the privacy policy of the social networks they are members of and many are unaware who can see their profile and the information contained in it. A large number of Irish social network users do not trust social networking websites with their information; however the results also indicate that they are not proactive in taking steps to secure their data. In general, Irish social network users also worry about what others may post about them on social networking websites. This lack of trust in other members is highest among older users.

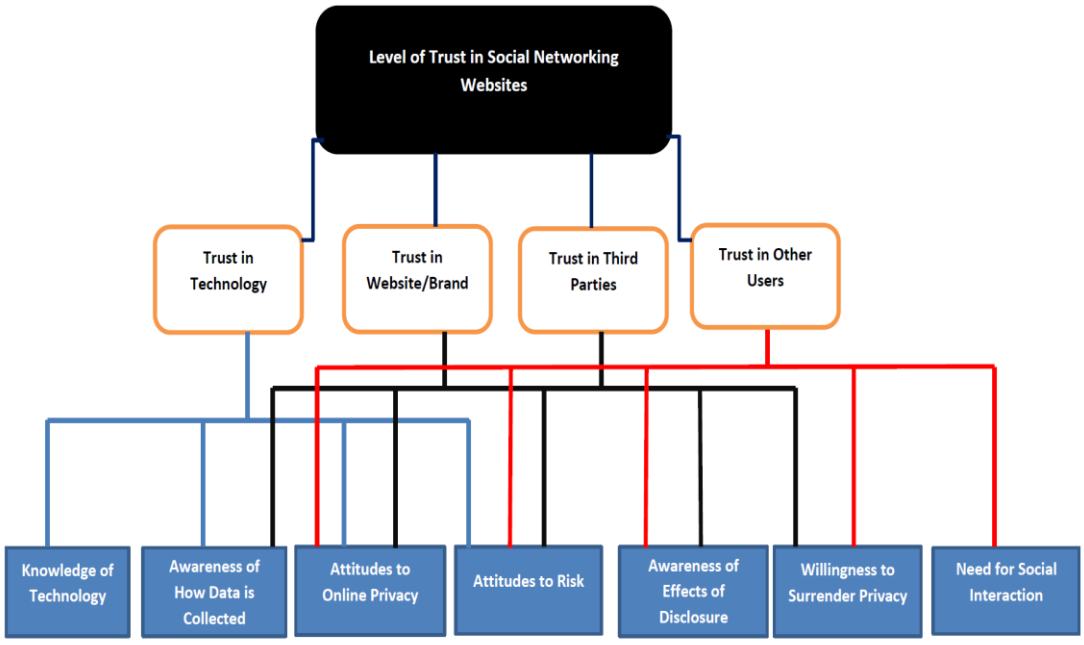
The level of awareness about how social networks share users' information with third parties was found to be high among participants in this study. The media

attention surrounding privacy of information on social networking websites in recent months may be contributing to this heightened awareness. There is evidence that Irish social network users are concerned about government monitoring of online social networking websites, something which was not mentioned in the questionnaire, but can be attributed to recent news coverage surrounding US government practices in relation to online social networking. While findings show there is a lack of trust and a high level of concern surrounding privacy on social networking websites Irish users, who took part in this study, do not foresee this affecting their future use of social networks. These results combined suggest this is a topic which requires further research.

Chapter 6: Proposed Conceptual Model

As a result of the findings outlined in the previous chapter, the researcher revised the conceptual model outlined in chapter three. Although the results of this research indicate that trust is not a vital requirement for Irish people to use social networking websites, the research findings demonstrate that the themes identified in the literature review are still reflective of social network users' attitudes to privacy. While these factors do not necessarily lead to trust in social networking websites, the level of trust users have in these websites is affected in some way by these themes. A new element; trust in third parties, has also been added to the model to reflect the issue of government monitoring of social networking websites which was identified following the data analysis. Following these findings the researcher proposes a new conceptual model of trust and privacy on social networking websites. This new model is shown in figure 6.1. The following chapter will further discuss the elements of this new model in relation to the findings and previous literature on the topic.

Figure 6.1: Proposed Conceptual Model of Trust & Privacy in Social Networking Websites



Chapter 7: Discussion

7.1 Introduction

The aim of this research was to identify what level of trust Irish internet users have in social networking websites and to examine their attitudes to privacy on these websites. The research also sought to establish what level of awareness Irish users had about how their data is handled by social networks. A total of 150 responses were received following the distribution of the questionnaire, which the researcher deemed acceptable given the time constraints. The results indicate that there is a lack of trust in social networking websites among Irish users who participated in the research. In this section, the results of this study and the elements of the proposed conceptual model will be discussed in relation to previous literature on this topic.

Contrary to findings by Pitkänen and Tuunainen (2012) that the majority of Facebook users in Finland trusted the website with their personal information, the findings of this study indicate that social network users in Ireland lack trust in social networking websites and are more aware of how their data is shared with third parties by these websites. However, when it comes to level of information disclosure, the findings of this study are consistent with similar studies carried out by Acquisti and Gross (2006) and Debatin et al (2009) in the US, which found that Facebook users revealed huge amounts of personal information on their profiles, despite stating they had concerns about their privacy online.

7.2 Information Disclosure

One of the most worrying findings of this study was the vast amounts of personal information Irish users are posting on their social networking profiles. The majority of Irish users are disclosing their full name, date of birth, work and educational information and photographs of themselves and others. This is exactly the type of information required by criminals to steal someone's identity and the type of information that would traditionally be classed as private (Levin and Abril, 2009). These results support Rosenblum's (2007) theory that users of social networking websites are quite comfortable to live their lives online. The problem here is that it is not only their own privacy they are threatening but also that of others as one of the most common things users include on their profile are photographs of others. Even though someone may not be a member of a social network or may be cautious in what they upload to their own profiles, they have very little control over what others may upload e.g. photographs or check-ins.

Large amounts of personal information are being disclosed despite the fact that by and large, Irish social network users have concerns about their privacy online and how their personal information is treated by social networks. The evidence in this research is in line with that of Barnes (2006) who refers to this phenomenon as the *"privacy paradox"*. According to Berendt et al (2005) web users do not necessarily act in accordance with their own privacy concerns and often divulge information without any pressure on them to do so, which based on the results of this research seems to be the case with Irish social network users.

The majority of users claim they are concerned about their privacy on social networking websites, yet include large amounts of personal data on their profiles.

Therefore it seems that Irish users' need for social interaction is stronger than their need to protect their personal information. This is consistent with the findings of O'Brien and Torres (2012) which focussed on information disclosure among Facebook users. Studies by Debatin et al (2009) have also found that while users may know the dangers associated with uploading personal information on social networks the benefits associated with social networking outweigh the risks involved.

It is not only the amount and type of information Irish users are disclosing on social networks which is a cause for concern it is also who they are sharing this information with. While most users, who took part in the research, were aware who could see their profile and many have selected the "friends only" option there are still quite a significant number unaware who can see their information. Taking a closer look at these results it would appear that even those users, who are taking steps to protect their personal information, may still be putting their privacy at risk. Even though they are only allowing "friends" to see their profiles they are still displaying their information to a broad range of people, as the majority of users are connected to more than 100 people on their online social network. These findings are supported by Debatin et al (2009) who found that social network users are providing very detailed information to a "*loosely defined group*" which is leaving them open to significant threats online (Acquisti & Gross, 2006).

7.3 Protection of Privacy

The majority of those who took part in this study are using social networks to stay connected with existing contacts, with the most common connections requested and accepted by Irish users being friends, close friends and family. This is in line with studies by Dwyer et al (2007) and Ellison, Steinfield and Lampe (2007) who found

that members tend to use social media to reinforce relationships made in an offline environment. However, 7.5% of Irish social network users admitted to requesting connections with people whom they had never met and 20% had requested people they had met just once. These figures were higher than expected in comparison with those of Pitkänen & Tuunainen (2012), who found that only 3% of users had requested people they had never met; while 12% sent requests to people they had met just once. This difference may be due to the fact that this study examined a range of different networks, whereas Pitkänen & Tuunainen's (2012) research only focussed on Facebook users. The nature of the different networks may explain why these figures were higher than previous studies. Twitter is more focussed on the members' interests and therefore people are more likely to "follow" people whom they have never met and members of LinkedIn are usually interested in new employment opportunities and may accept or request connections with recruiters they have never met in order to achieve this. However, this statistic is still worrying given the amount of information being disclosed by participants.

The vast majority of participants stated that they had adjusted their privacy settings on at least one occasion, which is consistent with the findings of previous studies by Debatin et al (2009) and Govani and Pashley (2005). O'Brien and Torres (2012) attribute this familiarity with privacy settings to controversy in the media about Facebook's privacy policy in 2009. Although the majority of Irish users have changed their privacy settings, only 18% change their settings on a regular basis with just over 6% admitting to changing their settings when amendments had been made to their social networks privacy policy. This can be linked to the fact that almost two thirds, of those who participated in this research, had not read the privacy policy of the social networks they are members of, which is supported by the findings of

previous studies in this area (O'Brien & Torres, 2012; Pitkänen & Tuunainen, 2012; Levin & Abril, 2009 and Govani & Pashley, 2005).

Bilton (2010) argues that the length of privacy policies on these websites may contribute to users' reluctance to read them and this may be the case among Irish users as one participant in this study commented that social networks *"do not make it easy"* for their members to read privacy documents and terms of use. It may also be as Kuzma (2011) suggests that these websites do not promote their privacy policies in case they deter people from joining the network.

7.4 Trust in Social Networking Websites

The results from this study imply that a large number of Irish users do not trust the social networking websites of which they are members with their personal data. These results are in contrast to studies carried out by Pitkänen & Tuunainen (2012) and Dwyer et al (2007) which found that users in general trusted social networking websites. A possible explanation for this difference is the increased knowledge people now have about social networks and how they operate. When the studies mentioned were first conducted social networks were a relatively new phenomenon (Pitkänen & Tuunainen's data was collected 5 years prior to publication) and privacy issues surrounding these websites have attracted a lot of media coverage in recent years and especially in the last number of weeks when the questionnaire for this study was being distributed.

It could be argued that the findings surrounding trust in social networking websites is worrying for social media companies as there is a substantial body of work which suggests trust is central to gain loyalty in an online environment. However, from the results of this research this does not seem to be the case when it comes to social

networking websites. Despite the fact that users did not trust social networks many were still active users of these websites. This contradicts the theory put forward by Hoffmann, Novak and Peralta (1999) and Metzger (2004) that trust is a central concept to information exchange in an online environment. O'Brien and Torres (2012) suggest that trust may be less important on social networking websites due to the need for social interaction among users and the findings of this research support this. Olivero and Lunt (2004) also argue that trust is less important if people perceive they will gain social benefits.

These findings are further supported by the fact that even when participants were informed of the threats to their privacy when using social networks approximately 60% reported that it would not affect their future use of social networks, thus reinforcing the point that the social benefits of being a member of one of these websites far outweigh the risks to user privacy. It may be that it will take a real and substantial threat to their privacy or for social network activity to have a negative impact on their lives for users to change their habits.

The results of this research indicate that levels of trust differ between age groups with younger users in the 18-24 category the most trusting group. This contrasts with findings by Madden and Smith (2010) who found younger age groups to be the least trusting of social networks. The level of trust younger Irish users have in social networking websites is worrying as they seem to be the users who share the most information leaving them vulnerable to threats on these websites (O'Brien & Torres, 2012).

Given the differences between these results and the findings of previous studies on this topic the researcher believes this is an area which warrants further study.

7.5 Trust in Other Users

Many participants were concerned about other users posting incorrect information which would embarrass them, however they were not so worried as to refrain from posting items to their "friends" profiles which is public to all those whom both they and their "friends" are connected to. This is also reflected in findings by Pitkänen & Tuunainen (2012) who suggest the reason for this is that users do not see their social network "friends" as threats to their privacy. The concern users have may stem from the fact that their connections are made up of such a varied group with many Irish users accepting requests not only from those they consider friends in an offline environment but also people they do not know very well or perhaps not at all. Boyd (2004) suggests that in an online social networking environment users may accept people as "friends" without knowing or trusting them.

Again the level of trust Irish users have in other members of social networks differs with age. While there is concern among all users about what other members may post about them this concern was higher among older users, which supports findings by O'Brien and Torres (2012) that older users are the least trusting on social networking websites.

7.6 Awareness of How Data is Collected

Awareness of how data is shared with third parties by social networking websites was widely acknowledged by participants in this study. 73% of users were aware that the terms in the privacy policy allow social networks to share their data with third parties for marketing purposes. This is in stark contrast to previous studies by Pitkänen and Tuunainen (2012) and Govani and Pashley (2005) where users' awareness was found to be significantly lower than the figures in this research. As

mentioned, this difference could also be linked to the fact that social networks have a much higher profile than when the data was collected for these studies. Users are becoming more knowledgeable about how these companies make their money. This difference in findings between this research and other studies on this topic is an area which is worthy of further study.

It came as no surprise that those who had read the privacy policy had a higher level of awareness about how their data is used, however, given the fact that only 36% have read the privacy policy it is clear that Irish users are gaining their knowledge from other sources. This is in line with findings by O'Brien and Torres (2012). Media interest surrounding privacy on social networking websites has gained considerable public interest in recent weeks and could explain why Irish users, who have not read the privacy policy, know how these websites are tracking and using their data.

7.7 Other Factors

Given there was no mention of government monitoring in the questionnaire, it is clear from the results that recent events have contributed to Irish users' lack of trust in social networking websites. With the revelations that governments are requesting information on users from social networking companies, the spotlight has been placed firmly on the issue of privacy on these websites. Facebook have released figures that information on 38,000 of their users was requested by government officials in 74 countries in the first half of 2013 alone (Hilliard, 2013) therefore it is unsurprising that this issue was mentioned by a number of participants in the free-text responses. One participant stated that *"social networks such as Facebook should be prevented from passing on your information to the likes of governments such as*

the US" while another commented that *"people need to be aware that the public is being watched/monitored"*. From these types of responses it is clear that these revelations are affecting Irish users' perceptions of privacy on social networks. These results are worrying for social networking companies as this issue could lead to a further fall in trust among their users, which could be detrimental to their business. These revelations are a relatively new development therefore this is an area which requires further research.

7.8 Summary

The need for social interaction is leading Irish users, who took part in this research, to disclose large amounts personal information online in some cases to people they have no relationship with in an offline context.

Irish social network users are disclosing this information despite stating that they have concerns about their privacy and do not trust social networking websites with their personal information. In general, the benefits associated with these websites outweigh the risks involved, which is in line with previous studies.

Older users are less trusting than younger users and are more cautious about who they share their information with.

There appears to be a high level of awareness about how personal information is treated by social networking companies despite the fact that the majority of users have not read the privacy policy, indicating that they are receiving their information by other means.

Recent revelations of government monitoring of social networking websites is contributing to the lack of trust which already exists amongst Irish social network users.

Chapter 8: Conclusions

At the outset the aim of this research was to explore the level of trust Irish social network users have in social networking websites, as well as determining their awareness of how their information is used by social networking companies. The study also sought to examine attitudes to privacy among social network users in Ireland and if age had any effect on users trust in social networks or attitudes to privacy. The research has successfully provided answers to these questions. In this chapter the findings of the research will be reviewed and recommendations for further study on this topic will be presented.

The findings of this research show that lack of trust in social networking websites exists among Irish social network users. However, the research also finds that this lack of trust is not having an impact on their use of online social networks. These low levels of trust are in contrast to results of Govani and Pashley (2005) which indicates a change in attitudes in the last number of years as people become more familiar with the practices of social networking companies.

This decrease in trust appears to come from awareness among Irish users about how social networking websites treat their personal information. Irish social network users are well informed when it comes to knowing how their information is used and shared with third parties; however they are not gaining this knowledge from the social network itself as the majority have not read the privacy policy or terms of use. Media attention of privacy issues on social networking websites may explain the greater awareness and seems to have negatively impacted users' trust in social networking websites.

One of the most significant findings to emerge from this research is users' attitudes to privacy on online social networks. The need for social interaction appears to be of greater importance to users than the protection of their personal information. In spite of the privacy concerns Irish users have in relation to the use of social networking websites they are still uploading a vast amount of personal information to their profiles which can be seen by a large number of people. Users are prioritising social interaction over personal privacy. The low levels of trust users have is not deterring them from actively using social networking websites and they are sacrificing their privacy for social gains.

The research also shows that although Irish people are members of a number of different types of social networking websites, no significant difference exists between the different social networks and the levels of trust that users have in them. However, the research indicates that age is a factor in the level of trust users have in social networks. While there is a general distrust of social networking websites among all users, older users are more likely to distrust social networks than younger users. As a result they are more cautious not only about the number of connections they share their information with but also the connections they request and accept.

It is clear from this research that while users have reservations about using social networking websites, the need for trust and the importance of privacy are not deciding factors in the use of social networks in Ireland. The perceived benefits of social networking mean that users are willing to put their privacy concerns aside.

Although there is strong evidence to suggest that lack of trust in social networking websites among Irish users will not deter them from actively using these websites, the limitations of the research mean that further research is required in order to

determine the full extent of this phenomenon before broader generalisations can be made.

Chapter 9: Recommendations

It is clear from this research that users of social networking websites need to be more cautious in both the level of information they disclose and also who can see this information. It is not enough users to apply privacy controls to limit who can see their profile if they do not also exercise the same control over the types of people they are requesting and accepting into their online social network.

By disclosing so much information to such a broad range of people users are leaving themselves open not only to identity theft but also to other threats such as offline crimes with criminals monitoring these websites to find potential targets or threats to their employment prospects as many companies are now reviewing potential employees social media profiles. Social network users need to recognise these threats when using online social networks and take steps to reduce the risk of these types of infringements on their privacy.

Social network users should be encouraged to read the privacy policy and terms of use of the social networking websites they use. It is clear from the failure by so many users to read the privacy policy and terms of use that they find these documents too long or complicated to read. Social networking companies need to evaluate their current privacy policies and make them more accessible for their members; otherwise users will continue to seek their information from third party sources such as media outlets which may further decrease their level of trust in social networking companies.

Social networking companies should seek to alleviate users concern by being more transparent about how they share information with third parties especially in relation government requests for information from social networking companies, which has

emerged as a new cause for concern among social network users. Facebook have already committed to publishing reports on a regular basis detailing how many requests they get from each country to keep users informed. Other social networking websites should follow suit as this may help address some of the privacy concerns users have. This would be beneficial for social networking websites as this transparency could help improve trust among users.

Chapter 10: Further Research

The results of this research highlighted a number of issues in relation to the topic of online trust and privacy on social networking websites which are worthy of further investigation and research. Firstly, due to the limitations of this research the time constraints did not allow for the gathering of a large number of people. Gathering data from a larger sample and perhaps using a random sampling method would allow for generalisations to be made.

Although the majority of users claimed that the information in the research would not affect their future use of social networking websites, there were a number of users who stated that they would be more cautious about what they uploaded and would look at their privacy settings again. An interesting study would be to carry out an experiment following the distribution of a questionnaire to monitor if users did actually follow through with these changes to their privacy settings and activity following the completion of the questionnaire.

The recent revelations of government monitoring of social networking websites and requests for user information raised further privacy concerns among users, as this is a relatively new issue a worthwhile future study would be to further examine if the knowledge that governments were monitoring profiles would affect usage of social networking websites.

The research shows that trust in social networking websites is not required in order for people to use them however much of the previous literature in the area of online trust suggests that trust is an essential requirement for people to disclose information online. This implies that trust differs across different types of websites. Future

research may identify whether significant differences in attitudes to privacy exist between different types of websites.

The results of this research also found that older users are less trusting of social networking websites and more cautious when it came to uploading information than younger users. A study into older social network users would be interesting to determine how age affects users trust in social networking websites.

It is clear from the research that lack of trust is not affecting usage of social networking websites and it may take an actual negative experience for users to alter their usage patterns. Future research could examine how user attitudes change when confronted by various types of negative impacts as a result of using social networking websites.

Chapter 11: Reference List

Acquisti, A. & Gross, R. (2006) 'Imagined Communities: Awareness, Information Sharing and Privacy on the Facebook'. *Lecture Notes in Computer Science*, Volume 4258: 36–48.

Adams, A. & Sasse, M.A. (2001) 'Privacy in Multimedia Communications: Protecting Users, Not Just Data'. In: Blandford, A. and Vanderdonckt J. eds. *People and Computers XV- Interaction without Frontiers: Joint Proceedings of HCI 2001 and IHM 2001*. London: Springer, 49-64.

Altman, I. (1977) 'Privacy Regulation: Culturally Universal or Culturally Specific?'. *Journal of Social Issues*, Volume 33(3): 66-84.

Barnes, S.B., (2006) 'A Privacy Paradox: Social Networking in the United States', *First Monday*, Volume 11(9). Available from: http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/1394/1312%23 [Accessed 24 November 2012].

Bart, Y., Shankar, V., Sultan, F. & Urban, G.L. (2005) 'Are the Drivers and Role of Online Trust the Same for All Web Sites and Consumers? A Large-Scale Exploratory Empirical Study'. *Journal of Marketing*, Volume 69(4): 133-152.

Bell, J. (2010) *Doing Your Research Project: A Guide for First-time Researchers in Education, Health and Social Science, 5th Edition*. Maidenhead: Open University Press.

Berendt, B., Günther, O. & Speikermann, S. (2005) 'Privacy in E-Commerce: Stated Preferences vs. Actual Behavior'. *Communication of the ACM*, Volume 48(3): 101-106.

Biernacki, P. & Waldorf, D. (1981) 'Snowball Sampling: Problems and Techniques of Chain Referral Sampling'. *Sociological Methods and Research*, Volume 10(2): 141-163.

Bilton, N. (2010) 'Price of Facebook Privacy? Start Clicking'. The New York Times, Technology. Available from: http://www.nytimes.com/2010/05/13/technology/personaltech/13basics.html?_r=0 [Accessed 26 August 2013].

Borna, S. & Sharma, D. (2011) 'Considering Privacy as a Public Good and Its Policy Ramifications for Business Organizations'. *Business and Society Review*, Volume 116(3): 331-353.

Boyd, D.M. (2004) 'Friendster and Publicly Articulated Social Networking', Paper presented at the *Conference on Human Factors and Computing Systems (CHI 2004).* Vienna, April 24-29.

Boyd, D.M. & Ellison, N.B. (2008) 'Social Network Sites: Definition, History, and Scholarship'. *Journal of Computer-Mediated Communication*, Volume 13(1): 210-230.

Brandenburg, C. (2008) 'The Newest Way to screen Job Applicants: A Social Networkers Nightmare', *Federal Communication Law Journal*, Volume 60(3): 597-626.

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

Bryman, A. & Bell, E. (2011) *Business Research Methods, 3rd Edition.* Oxford: Oxford University Press.

Camenisch, J., Shelat, A., Sommer, D., Fischer-Hübner, S., Hansen, M., Krassemann, H., Lacoste, G., Leenes, R. & Tseng, J. (2005) 'Privacy and Identity Management for Everyone', Paper presented at *Proceedings of the 2005 Workshop on Digital Identity Management.* Virginia, 11th November 2005: 20-27.

Caudill, E.M. & Murphy, P. E. (2000) 'Consumer Online Privacy: Legal and Ethical Issues'. *Journal of Public Policy and Marketing*, Volume 19(1): 7-19.

Collins, J.C. (2010) 'Fortify Your Facebook Privacy Settings: Don't Let the Window into Your Private Life Sully Your Professional Reputation'. *Journal of Accountancy*, Volume 209(6): 42-45.

Collis, J. & Hussey, R. (2009) *Business Research: A Practical Guide for Undergraduate and Postgraduate Students, 3rd Edition*. Houndsmills, Basingstoke: Palgrave Macmillan.

Cranor, L.F. (1999) 'Internet Privacy'. *Communications of the ACM*, Volume 42(2): 28-39.

Creswell, J.W. (2009) *Research Design: Qualitative, Quantitative and Mixed Methods Approaches*. London: Sage Publications Inc.

Culnan, M. (1993) '"How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use'. *MIS Quarterly*, Volume 17(3): 341-363.

Debatin, B., Lovejoy, J.P., Horn, A.K. & Hughes, B.N. (2009) 'Facebook and Online Privacy: Attitudes, Behaviours and Unintended Consequences', *Journal of Computer-Mediated Communications*, Volume 15(1): 83–108.

Del Riego, A., Abril, P.S. & Levin, A. (2012) 'Your Password or Your Paycheck?: A Job Applicants Murky Right to Social Media Privacy'. *Journal of Internet Law,* Volume 16(3): 1-26.

Denscombe, M. (2003) *Good Research Guide: For Small-Scale Research Projects, 2nd Edition*. Maidenhead: Open University Press.

Deutsch, M, (1958) 'Trust and Suspicion'. *Journal of Conflict Resolution,* Volume 2(4): 265-279.

De Vaus, D. (2002) *Surveys in Social Research, 5th Edition*. London: Routledge.

Dillman, D.A. (2007) *Mail and Internet Surveys 2007: The Tailored Design Method*. Chichester: John Wiley & Sons Ltd.

Dwyer, C., Hiltz, S.R. & Passerini, K. (2007) 'Trust and Privacy Concern within Social Networking Sites: A Comparison of Facebook and MySpace', Paper presented at the *Proceedings of the Thirteenth Americas Conference on Information Systems.* Colorado, August 09 – 12.

Ellison, N., 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,* Volume 12(4): 1143-1168.

Fink, A. (2003) *The Survey Handbook, 2nd Edition*. Thousand Oaks: Sage Publications.

Fisher, C.M. (2004) *Researching and Writing a Dissertation for Business Students*. Harlow: FT Prentice Hall.

Fried, C. (1968) 'Privacy', *Yale Law Journal,* Volume 77(3): 475-493.

Friedman, B., Khan, P. & Howe, D. (2000) 'Trust Online'. *Communications of the ACM*, Volume 43(12): 34-40.

Fukuyama, F. (1995) *Trust: The Social Virtues and the Creation of Prosperity*. New York: Free Press Paperbacks.

Furnell, S. & Botha, R.A. (2011) 'Social Networks – Access All Areas?'. *Computer Fraud and Security*, Volume 2011(5): 14-19.

Genova, G. (2009) 'No Place to Play: Current Employee Privacy Rights in Social Networking Sites'. *Business Communication Quarterly*, Volume72(1): 97-101.

Gill, J. & Johnson, P. (2010) *Research Methods for Managers, 4th Edition*. London: Sage Publications Ltd.

Gomm, R. (2009) *Key Concepts in Social Research Methods*. Hampshire: Palgrave Macmillan.

Govani, T. & Pashley, H. (2005) 'Student Awareness of the Privacy Implications When Using Facebook'. *Carnegie Mellon University*. Available from: http://lorrie.cranor.org/courses/fa05/tubzhlp.pdf [Accessed: 30 March 2013].

Grabner-Krauter, S. (2009) 'Web 2.0 Social Networks: The Role of Trust. *Journal of Business Ethics*, Volume 90(4): 505-522.

Hann, I., Hui, K., Tom Lee, S. & Png, I. (2007) 'Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach'. *Journal of Management Information Systems*, Volume 24(2): 13-42.

Hilliard, M. (2013) 'State Sought Data on 40 Irish Facebook Users'. The Irish Times, Technology. Available from: http://www.irishtimes.com/news/technology/state-sought-data-on-40-irish-facebook-users-1.1507620 [Accessed August 29 2013].

Hoffman, D.L., Novak, T.P. & Peralta, M. (1999) 'Building Consumer Trust Online'. *Communications of the ACM*, Volume 42(4): 80-85.

Horn, R. (2009) *Researching and Writing Dissertations: A Complete Guide for Business and Management Students*. London: CIPD.

Ipsos MRBI (2012) 'Social Networking Quarterly Survey: August 2012' [Internet]. Available from: http://www.ipsosmrbi.com/social-networking-quarterly-survey-august-2012.html [Accessed 21 December 2012].

Ipsos MRBI (2013) 'Social Networking Quarterly Survey: February 2013' [Internet]. Available from: http://www.ipsosmrbi.com/social-networking-quarterly-survey-februar-2013.html [Accessed 16 August 2013].

Jankowicz, A.D. (2005) *Business Research Projects, 4th Edition*. London: Thomson Learning.

Joinson, A.N., Reips, U., Buchanan, T. & Schofield (2010) 'Privacy Trust and Self-disclosure Online'. *Human-Computer Interaction*, Volume 25(1): 1-24.

Karvonen, K. (2007) 'Users and trust: The New Threats, the New Possibilities'. *Universal Access in Human-Computer Interaction: Applications and Services Lecture Note in Computer Science*, Volume 4556: 893-902.

Koehn, D. (2003) 'The Nature of and Conditions of Online Trust'. *Journal of Business Ethics*, Volume 43: 3-19.

Kuzma, J. (2011) 'Empirical Study of Privacy Issues among Social Networking Sites'. *Journal of International Commercial Law and Technology*, Volume 6(2): 74-85.

Lauer, T.W. & Deng, X. (2007) 'Building Online Trust Through Privacy Practices'. *International Journal of Information Security*, Volume 6(5): 323-331.

Levin, A. & Abril, P.S. (2009) 'Two Notions of Privacy'. *Vanderbilt Journal of Entertainment & Technology Law*, Volume (11): 1001-1051.

Lewicki, R.J., McAllister, D. & Bies, R. (1998) 'Trust and Distrust: New Relationships and Realities'. *Academy of Management Review*, Volume 23(3): 438-458.

Lewicki, R.J., Wiethoff, C. & Tomlinson, E. (2005) 'What is the role of trust in organizational justice?' In Greenberg, J. & Colquitt J.A. eds. *Handbook of organizational justice: Fundamental questions about fairness in the workplace*. Mahwah, N.J.: Lawrence Erlbaum Associates.

Liu, C., Marchewka, J.T., Lu, J., Yu, C.S. (2004) 'Beyond Concern: A Privacy-Trust-Behavioural Model of Electronic Commerce'. *Information and Management*, 42(2): 127-142.

Madden, M. & Smith A. (2010) 'Reputation Management and Social Media: How People Monitor Their Identity and Search for Others Online'. Report of Pew Research Center. Available from: http://www.pewinternet.org/~/media//Files/Reports/2010/PIP_Reputation_Management_with_topline.pdf [Accessed 24 August 2013].

Mayer, R.C., Davis, J.H. & Schoorman, F.D. (1995) 'An Integrative Model of Organizational Trust'. *Academy of Management Review*, Volume 20(3): 709-734.

McGrath, L.C. (2011) 'Social Networking Privacy: Important or Not?'. *Interdisciplinary Journal of Contemporary Research in Business*, Volume 3(3): 22-28.

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

Mohamed, A.A. (2010) 'Online Privacy Concerns Among Social Networks' Users'. *Cross-Cultural Communication*, Volume 6(4): 74-89.

Nielsen (2009) 'Global Faces and Networked Places: A Nielsen Report on Social Networking's New Global Footprint' [Internet], *Nielsen*. Available from: http://blog.nielsen.com/nielsenwire/wp-content/uploads/2009/03/nielsen_globalfacesmar09.pdf [Accessed 25 November 2012].

Nissenbaum, H. (2001) 'Securing trust online: Wisdom or oxymoron', *Boston University Law Review*, Volume 81(3): 101-131.

O'Brien, D. & Torres, A.M., (2012) 'Social Networking and Online Privacy: Facebook Users' Perceptions', *Irish Journal of Management*, Volume 31(2): 63-97.

Olivero, N. & Lunt, P., (2004) 'Privacy Versus Willingness to Disclose in e-Commerce Exchanges: The Effect of Risk Awareness on the Relative Role of Trust and Control', *Journal of Economic Psychology*, Volume 25 (2): 242-262.

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

Pallant, J. (2001) *SPSS Survival Manual: A Step By Step Guide to Data Analysis Using SPSS*. Buckingham: Open University Press.

Parahoo, K. (2006) *Nursing Research: Principles, Process and Issues, 2nd Edition.* Basingstoke: Macmillan.

Pitkänen, O. & Tuunainen, V.K. (2012) 'Disclosing Personal Data Socially - an Empirical Study on Facebook User's Privacy Awareness'. *Journal of Information Privacy & Security*, Volume 8(1): 3-29

Ridings, C.M., Gefen, D. & Arinze, B. (2002) 'Some Antecedents and Effects of Trust in Virtual Communities', *Journal of Strategic Information Systems*, Volume 11(3): 271-295.

Roloff, M.E. (1981) *Interpersonal Communication: The Social Exchange Approach.* Beverly Hills: Sage Publications Inc.

Rosenblum, D. (2007) 'What Anyone Can Know: The Privacy Risks of Social Networking Sites', *IEEE Security and Privacy*, Volume 5(3): 40-9.

Rousseau, D., Sitkin, S., Burt, R. & Camerer, C. (1998) 'Not So Different After All: A Cross-Discipline View of Trust'. *Academy of Management Review*, Volume 23(3): 393-404.

Saunders, M., Lewis, P. & Thornhill, A. (2012) *Research Methods for Business Students, 6th Edition*. Harlow: Pearson Education Limited.

Sekaran, U. & Bougie, R. (2009) *Research Methods for Business: A Skill Building Approach, 5th Edition*. Chichester: John Wiley & Sons.

Sim, I., Liginlal, D. & Khansa, L. (2012) 'Information Privacy Situation Awareness: Construct and Validation'. *The Journal of Computer Information Systems*, Volume 53(1): 57-64.

Squicciarini, A.C., Xu, H. & Zhang, X. (2011) 'CoPE: Enabling Collaborative Privacy Management in Online Social Networks'. *Journal of the American Society for Information Science & Technology*, Volume 62(3): 521-534.

Sundén, J. (2003) *Material Virtualities: Approaching Online Textual Embodiment*. New York: Peter Lang Publishing.

Taddei, S. & Contena, B. (2013) 'Privacy, Trust and Control: Which Relationships with Online Self-Disclosure?'. *Computers in Human Behaviour,* Volume 29(3): 821-826.

Timm, D.M. & Duven, C.J. (2008) 'Privacy and Social Networking Sites'. *New Directions for Student Services,* Volume 2008(124): 89-101.

Tomlinson, S. (2011) 'How's your social security? Burglars monitor Facebook and Twitter to see when you're away from home'. *The Daily Mail*. Available from: http://www.dailymail.co.uk/sciencetech/article-2056079/Hows-social-security-Burglars-monitor-Facebook-Twitter-youre-away-home.html [Accessed 15 December 2012].

Van Dyke, T.P., Midha, V. & Nemati, H. (2007) 'The Effects of Consumer Privacy Empowerment on Trust and Privacy Concerns in e-Commerce', *Electronic Markets,* Volume 17 (1): 68-81.

Verhagen, T., Meents, S., & Tan, Y. (2006) 'Perceived risk and trust associated with purchasing at electronic marketplaces', *European Journal of Information Systems,* Volume 15(6): 542-555.

Wang, Y.D. & Emurian, H.H., (2005) 'An Overview of Online Trust: Concepts, Elements and Implications', *Computers in Human Behaviour,* 21(1): 105-125.

Weir, G.R., Toolan, F. & Smeed, D. (2011) 'The Threats of Social Networking: Old Wine in New Bottles?'. *Information Security Technical Report*, Volume 16(2): 38-43.

Westin, A.F. (1967) *Privacy and Freedom*. New York: Athenaeum.

Williamson, K. (2006) 'Research in Constructivist Frameworks Using Ethnographic Techniques'. *Library Trends*, Volume 55(1): 83-101.

Xu, H., Dinev, T., Smith, J. & Hart, P. (2011) 'Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances'. *Journal of the Association for Information Systems*, Volume 12(12): 798-824.

Zimmer, X.J., Arsal, R.E., Al-Marzouq, M. & Grover, V. (2010) 'Investigating Online Information Disclosure: Effects of Information Relevance, Trust and Risk'. *Information and Management*, Volume 47(2): 115-123.

Chapter 12: Appendices

Appendix A: Cover Letter

Online Privacy on Social Networking Websites

Introduction

Dear Participant,

I am a post-graduate student at the National College of Ireland. This survey is part of my Masters of Business Administration degree. The survey focuses on attitudes towards and awareness of privacy on social networking websites among internet users in Ireland.

The survey contains some demographic questions and questions about your use and opinions of social networking websites.

The full survey should take approximately 15 minutes to complete. Your participation is voluntary, anonymous and entirely confidential. The findings of the research will be included in my final thesis. The results of this research will be available to you on request. All data collected will be stored securely and destroyed once no longer required for the purposes of the research.

I would be grateful if you could pass the survey onto others in your online social network to take part in the research.

If you have any queries regarding this survey please contact me at:
patricia.greene@student.ncirl.ie

Thank you very much for your participation.
Patricia Greene

Appendix B: Questionnaire

Online Privacy on Social Networking Websites

Background Information

1. What is your age?

- ◯ Under 18
- ◯ 18 to 24
- ◯ 25 to 34
- ◯ 35 to 44
- ◯ 45 to 54
- ◯ 55 to 64
- ◯ 65 or older

2. What is your gender?

- ◯ Female
- ◯ Male

3. How would you rate your level of technical knowledge of the internet?

- ◯ Poor
- ◯ Basic
- ◯ Average
- ◯ Above average
- ◯ Highly proficient

***4. Which of the following social networking websites are you a member of? (Check all that apply)**

- ☐ Facebook
- ☐ Twitter
- ☐ LinkedIn
- ☐ Google+
- ☐ Myspace
- ☐ Bebo
- ☐ Instagram
- ☐ Other (please specify)

5. If you are a member of more than one of the above, which social networking website do you use most often?

Online Privacy on Social Networking Websites

6. How long have you been a member of this social networking website?

- ◯ Less than 1 year
- ◯ 1-2 years
- ◯ 3-5 years
- ◯ More than 5 years

7. Tick all of the below reasons for joining a social networking website which apply to you

- ☐ "Everyone I know has a social networking profile"
- ☐ A friend suggested it
- ☐ To keep in touch with existing friends & family
- ☐ To track down old friends & family
- ☐ To find people who share my interests
- ☐ To meet new people
- ☐ To find a job
- ☐ To find a date
- ☐ To express opinions
- ☐ To promote my business

Other (please specify)

Online Privacy on Social Networking Websites

Participants' use of socail networking websites

8. How often do you log onto your social networking profile?

- ◯ More than once per day
- ◯ Once per day
- ◯ More than once per week
- ◯ Once per week
- ◯ Less than once per week
- ◯ Once per month
- ◯ Less than once per month
- ◯ Rarely
- ◯ Never

9. Please indicate what personal information you include on your social networking profile (check all that apply)

- ☐ Full Name
- ☐ Date of Birth
- ☐ Hometown
- ☐ E-mail Address
- ☐ Contact Number
- ☐ Street Address
- ☐ Education information
- ☐ Work information
- ☐ Relationship status
- ☐ Political views
- ☐ Religious views
- ☐ Skills & expertise
- ☐ Family members
- ☐ Photographs of you
- ☐ Photographs of friends & family

Other (please specify)

Online Privacy on Social Networking Websites

10. What do you normally do when you log onto your social networking profile? (check all that apply)

- [ ] Update my profile information
- [ ] Upload new photographs
- [ ] Look at profiles and photographs of friends
- [ ] Look at profiles of people I don't know
- [ ] Look for more friends to add to my friends list
- [ ] Contact new people
- [ ] Play games
- [ ] Send private messages to my friends
- [ ] Update my status
- [ ] Write messages on my friends's profiles
- [ ] Add new applications
- [ ] Create a new event

Other (please specify)

11. How often do you update your status?

- ◯ More than once per day
- ◯ Once per day
- ◯ More than once per week
- ◯ Once per week
- ◯ More than once per month
- ◯ Once per month
- ◯ Occasionally
- ◯ Never

12. Approximately how many contacts/friends do you have on your social networking profile?

- ◯ 0-50
- ◯ 51-100
- ◯ 101-150
- ◯ 151-200
- ◯ More than 200

Online Privacy on Social Networking Websites

13. What type of friends have you requested to join your online social network? (check all that apply)

- [ ] Close friends
- [ ] Friends
- [ ] Family
- [ ] People you know
- [ ] People you have met just once
- [ ] People you have never met

14. What type of friends have you accepted requests to join your online social network from? (check all that apply)

- [ ] Close friends
- [ ] Friends
- [ ] Family
- [ ] People you know
- [ ] People you have met just once
- [ ] People you have never met

15. Have you ever looked at the profile of someone you do not know?

- ◯ Yes
- ◯ No

Online Privacy on Social Networking Websites

Privacy Control

16. Do you know who can see your profile and the information contained in it?

- ◯ Yes
- ◯ No
- ◯ I don't know

17. Are you aware that you can change your privacy settings?

- ◯ Yes
- ◯ No

Online Privacy on Social Networking Websites

18. Have you ever used your privacy settings?

- ◯ Yes
- ◯ No

Online Privacy on Social Networking Websites

19. How often do you change your privacy settings?

20. How important is it for you to be able to control who can see your social networking profile?

Extremely unimportant	Unimportant	Somewhat unimportant	Neither important nor unimportant	Somewhat important	Important	Extremely important
◯	◯	◯	◯	◯	◯	◯

21. Who can see your profile and information?

- ◯ My networks & friends
- ◯ Only my friends
- ◯ No one
- ◯ Everyone
- ◯ I don't know

22. Are you aware that if you have joined some network or group and you haven't changed your privacy settings all members of the same network can see your profile?

- ◯ Yes
- ◯ No

Online Privacy on Social Networking Websites

General privacy & data security concerns

Using a 1-7 scale, please indicate your agreement with each of the following statements by clicking on the appropriate circle.

23. I worry about my privacy and data security while using the internet

Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
◯	◯	◯	◯	◯	◯	◯

24. I worry that if I use my credit card to buy something online my credit card number will be obtained/intercepted by someone else

Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
◯	◯	◯	◯	◯	◯	◯

25. I worry about people online not being who they say they are

Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
◯	◯	◯	◯	◯	◯	◯

26. I feel that identity theft could be a real privacy risk

Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
◯	◯	◯	◯	◯	◯	◯

27. I worry that if I use the internet on my mobile phone and it is stolen he/she can find my personal information.

Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
◯	◯	◯	◯	◯	◯	◯

28. I am familiar with data protection and security while using the internet in general.

Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
◯	◯	◯	◯	◯	◯	◯

Online Privacy on Social Networking Websites

Social network privacy & data security concerns

Using a 1-7 scale, please indicate your agreement with each of the following statements by clicking on the appropriate circle.

29. I worry about my privacy and data security while using online social networking websites

Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
◯	◯	◯	◯	◯	◯	◯

30. I feel that social networking websites protect the privacy of my personal information

Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
◯	◯	◯	◯	◯	◯	◯

31. I trust that social networking websites of which I am a member will not use my personal information for any other purpose

Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
◯	◯	◯	◯	◯	◯	◯

32. I feel comfortable writing messages on my friends' profiles

Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
◯	◯	◯	◯	◯	◯	◯

33. I worry that I will be embarrassed by wrong information others post about me on social networking websites

Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
◯	◯	◯	◯	◯	◯	◯

Online Privacy on Social Networking Websites

Privacy policy on social networking websites

34. Have you read the privacy policy of any of the social networking websites which you are a member of?

- ◯ Yes
- ◯ No

35. Have you read the terms of use of any of the social networking websites which you are a member of?

- ◯ Yes
- ◯ No

36. Are you aware that social networking websites can share your information with people or organisations for marketing purposes?

- ◯ Yes
- ◯ No

37. Are you aware that when you add a new application to your social networking profile you give the organisations who supply the application the right to access your profile information?

- ◯ Yes
- ◯ No

38. I am concerned about providing my personal information (including photographs) to social networking websites because it could be used in a way I did not foresee

Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
◯	◯	◯	◯	◯	◯	◯

39. Do you think this questionnaire will affect your future use of social networking websites?

- ◯ Yes
- ◯ No

If yes how?

40. Please give any feedback on the questionnaire or subject you may have

Online Privacy on Social Networking Websites

Thank you for completing the survey!

Appendix C: Codebook

Full Variable Name	SPSS Variable Name	Coding Instructions
Identification Number	Participant	Participant Identification Number
Age	Age	1=Under 18; 2=18-24; 3=25-34; 4=35-44; 5=45-54; 6=55-64; 7=65 or Older
Gender	Gender	1=Female; 2=Male
Level of technical knowledge	Tech	1=Poor; 2=Basic; 3=Average; 4=Above Average; 5=Highly Proficient
Network Membership	Network1 to Network8	1=They Checked this
Network used most often	Popular	1=Facebook; 2=Twitter; 3=LinkedIn; 3=Google+; 5=MySpace; 6=Bebo; 7=Instagram; 8=Other
Length of membership	Time	1=Less than 1 year; 2= 1-2 years; 3=3-5 years; 4=More than 5 years
Reasons for joining	Reasons1 to Reasons11	1=They Checked this
Frequency of logon	Freq	1=More than once per day; 2=Once per day; 3=More than once per week; 4=Once per week; 5=Less than once per week; 6=Once per month; 7=Less than once per month; 8=Rarely; 9=Never
Information included on profile	Info1 to Info16	1=They Checked this
Activities when logged on	Task1 to Task13	1=They Checked this
Frequency of Status updates	Activity	1=More than once per day; 2=Once per day; 3=More than once per week; 4=Once per week; 5=Less than once per week; 6=Once per month; 7=Occasionally; 8=Never
Number of Contacts	Contacts	1=0-50; 2=51-100; 3=101-150; 4=151-200; 5=More than 200
Types of friends requested	Request1 to Request6	1=They Checked this
Types of friends accepted	Accept1 to Accept6	1=They Checked this
Viewed strangers profile	Unknown	1=Yes; 2=No
Who can see profile	PC1	1=Yes; 2=No; 3=I don't know
Knowledge of privacy settings	PC2	1=Yes; 2=No

Usage of privacy settings	PC3	1=Yes; 2=No
Frequency of changes to privacy settings	PC4	1=Rarely; 2=Once; 3=Never; 4=Regularly; 5=Once per month; 6=After changes to privacy policy; 7=Occaisionally; 8=Weekly; 9=When I need to; 10=I don't know
Importance of Control	PC5	1=Extremely unimportant; 2=Unimportant; 3=Somewhat unimportant; 4=neither important nor unimportant; 5=Somewhat important; 6=Important; 7=Extremely important
Knowledge of who can see profile	PC6	1=My networks and friends; 2=Only my friends; 3=No one; 4=Everyone; 5=I don't know
Awareness of joining networks	PC7	1=Yes; 2=No
General privacy	GP1 to GP6	1=Strongly disagree; 2=Disagree; 3=Somewhat disagree; 4=Neither agree nor disagree; 5=Somewhat agree; 6=Agree; 7=Strongly Agree
Social network privacy	SNP1 to SNP5	1=Strongly disagree; 2=Disagree; 3=Somewhat disagree; 4=Neither agree nor disagree; 5=Somewhat agree; 6=Agree; 7=Strongly Agree
Read privacy policy	PP1	1=Yes; 2=No
Read terms of use	PP2	1=Yes; 2=No
Awareness of sharing information	PP3	1=Yes; 2=No
Awareness of adding new applications	PP4	1=Yes; 2=No
Concern about uploading information	PP5	1=Strongly disagree; 2=Disagree; 3=Somewhat disagree; 4=Neither agree nor disagree; 5=Somewhat agree; 6=Agree; 7=Strongly Agree
Future use	PP6	1=Yes; 2=No