

**AN EMPIRICAL INVESTIGATION ON STUDENTS' ONLINE PRIVACY
ON FACEBOOK AT NORTH-WEST UNIVERSITY (MAFIKENG)**

by

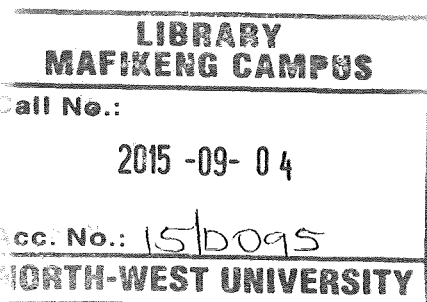
PHILLIP NYONI

23697555

A dissertation submitted to the North-West University (Mafikeng Campus), Commerce & Administration Faculty, Information Systems Department, in fulfilment of the requirements for the Masters of Commerce degree in Computer Science and Information Systems

Supervisor: Dr. M. Velempini

2014



DECLARATION

I, Phillip Nyoni, hereby declare that this dissertation submitted for the Masters of Commerce degree in Computer Science and Information Systems at North-West University, has not been previously submitted by me either at this or any other university. In addition, I declare that the research was carried out by me and only me and the literature consulted has been appropriately acknowledged.

Signature..........

Phillip Nyoni

ACKNOWLEDGMENTS

I would like to acknowledge the following individuals for their contribution towards the successful completion of this study. I am highly indebted to my supervisor, Dr. M. Velempini, who provided ideas, encouraging words and a solid positive attitude when I encountered setbacks. Special mention is due to other members of staff in the department - Prof. N. Mavetera, Prof. S. Lubbe and Mrs. C. Mavetera. Your knowledge and timely interventions made all the difference.

Gratitude is also due to my family, my parents and siblings, who were there to me as and when it was necessary. Thank you. I pray that the Lord continues to bless you in all things.

Lastly, to my colleagues and other associates who assisted me at various times, I say thank you. Be of good cheer for your reward awaits you for all your benevolence.

ABSTRACT

Online privacy is becoming increasingly important in today's world of hyper-connectivity, which is established through online media such as social networks. Sites such as Facebook, Twitter and LinkedIn have massive amounts of personal information about people and have become treasure troves to those who could misuse such personal data. Personal privacy needs to be protected now more than ever due to the risks of being targeted by third-party entities that aggregate user data. This study sought to add a meaningful insight into key user behaviour when they are online and the potential privacy violations they may be most prone to.

Users need to be made aware of the risks of disclosing personal information online as well as the tools that are in place to protect them, especially site privacy policies or legal instruments. Such information may go further in protecting their privacy and safety while they are online. The result of this would be a safer social network experience for all users. This study identified students at the North-West University (Mafikeng Campus) as a suitable population for evaluating user awareness regarding online privacy.

The study reveals that users' privacy is only partially protected by default when users create an online social networking account. The findings also show that users are not aware of their privacy rights as they should. Their awareness of privacy laws is little and the Facebook policy is lengthy with most users never having looked at the policy. This has lead Facebook users to operate at a level of trust and not a level of security. Consumers have less privacy protection on the Internet and this has a significant influence on the way these sites should be run. Based on these findings, privacy awareness can be achieved through training and increasing knowledge about how to fully utilise privacy settings on social media. Users must be taught the different ways to secure their personal information.

Keywords: Privacy, Privacy law, Personal Information, Online Self-disclosure, Social Networks, Facebook, Cyber Security, Profiling, Online Advertising, Trust.

TABLE OF CONTENTS

DECLARATION	i
ACKNOWLEDGMENTS	ii
ABSTRACT	iii
CHAPTER ONE: INTRODUCTION TO THE RESEARCH	1
1.1 INTRODUCTION	1
1.2 PROBLEM STATEMENT	2
1.3 RESEARCH QUESTIONS	3
1.4 RESEARCH OBJECTIVES	3
1.5 RESEARCH METHODOLOGY AND DESIGN	4
1.6 SIGNIFICANCE OF THE STUDY	5
1.7 SCOPE OF THE STUDY	6
1.8 LIMITATIONS OF THE STUDY	6
1.9 CONCLUSION	7
CHAPTER TWO: LITERATURE REVIEW	8
2.1 INTRODUCTION	8
2.2 PERSONAL INFORMATION ON SOCIAL MEDIA	8
2.3 STUDENT ONLINE DISCLOSURE ON SOCIAL MEDIA	9
2.4 SOCIAL MEDIA SITES: FACEBOOK	12
2.4.1 FACEBOOK PRIVACY POLICY	15
2.5 THIRD PARTY CONTENT ON FACEBOOK	16
2.6 PRIVACY	18
2.6.1 Information Privacy Model	19
2.7 LEGISLATIVE FRAMEWORK	21
2.7.1 The Need for Privacy Legislation	21
2.7.2 Overview of International Development of Privacy Legislation	22
2.7.2.1 Development of Privacy Legislation in the United States of America (USA)	22
2.7.2.2 Development of Privacy Legislation in the European Union (EU)	23
2.7.2.3 Development of Privacy Legislation in the South Africa (RSA)	24
2.7.3 Challenges faced in Implementing Privacy Laws	24
2.8 CONCLUSION	25
CHAPTER THREE: RESEARCH METHODOLOGY	26
3.1 INTRODUCTION	26
3.2 METHODOLOGY	26
3.3 DESIGN	29
3.4 POPULATION	31
3.5 SAMPLING TECHNIQUE AND SAMPLE SIZE	31

3.6 DATA COLLECTION INSTRUMENT	33
3.6.1 Reliability and Validity	34
3.6.2 Ethical Requirements	35
3.7 DATA ANALYSIS AND PRESENTATION	35
3.8 CONCLUSION	36
CHAPTER FOUR; RESULTS AND ANALYSIS	37
4.1 INTRODUCTION	37
4.2 DEMOGRAPHICS	37
4.3 USER PERSONAL INFORMATION AND SELF-DISCLOSURE	38
4.4 USER ACTIVITIES	44
4.5 THIRD-PARTY CONTENT	47
4.6 FALSE-CALL	51
4.7 SURVEY	53
4.8 SUMMARY OF RESULTS	54
4.9 CONCLUSION	55
CHAPTER FIVE: CONCLUSION	56
5.1 INTRODUCTION	56
5.2 SUMMARY	56
5.3 RECOMMENDATIONS	60
5.4 CONCLUSION	63
REFERENCES	65
Annexure A: POLLING CHECKLIST	
Annexure B: SURVEY	

LIST OF TABLES

Table 4.1: Frequency of user activity	46
Table 4.2 Time Response	52

LIST OF FIGURES

Figure 2.1: Facebook Statistics as of 2012	14
Figure 2.2: User perceptions of Facebook after reading privacy policy	15
Figure 2.3: Information Privacy Model	20
Figure 3.1: Sample Size Table	32
Figure 4.1: User Gender	37
Figure 4.2: Age	37
Figure 4.3: Place of Residence	38
Figure 4.4: Place of Work	38
Figure 4.5: Availability of user details	39
Figure 4.6: Number of Friends	40
Figure 4.7: Geo-Location Sharing	40
Figure 4.8: Geo-Location Example	40
Figure 4.9: Geo-Location Example II	41
Figure 4.10: Majority of User Likes	42
Figure 4.11: Method of Access	43
Figure 4.12: Frequency of User Activity	44
Figure 4.13: Sharing of Events	45
Figure 4.14: Frequency User Tagging	46
Figure 4.15: Programs used on Facebook	47
Figure 4.16: Facebook Program asking for Permissions	48
Figure 4.17: Frequency of Program Usage	49
Figure 4.18: Program Posting	50
Figure 4.19: Recommending Products	51
Figure 4.20: Response Rate	52
Figure 4.21: Privacy Legislation Awareness	53
Figure 4.22: Use of Privacy Tools	54
Figure 4.23: Facebook Improvements	54

CHAPTER ONE

INTRODUCTION TO THE RESEARCH

1.1 Introduction

Social networks have revolutionised the way people communicate and keep in touch. However, as these new technologies advance, users become more exposed to cyber security threats (Mansfield-Devine, 2008:18). There is a need to explore and evaluate these threats to determine their potential harmfulness. The main theme for this research is an examination of the privacy issues that users are exposed to when they make use of social networks such as Facebook (Mansfield-Devine, 2008:18).

The nature of the content of the Internet has changed as it is now mostly user-generated content, so much so that the owners of websites are not always in total control of what content their sites are displaying at specific moments in time (Mansfield-Devine, 2008:18). The information that social networks now generate is currently utilised for purposes other than the original reason for its collection (Mansfield-Devine, 2008:18). It is important to remember that social media generates a treasure trove of personal information about every individual who uses these sites (Mansfield-Devine, 2008:18). This information includes the person's location, marital status, age, gender and so much more sensitive information that users may not realise its potential threat. The current model for information exchange also employs applications that enable anyone to view a user's online profile data, which can allow an association (through data-mining) of user data to gain some insight into the users' lives (Gartrell, Han & Beach, 2008:7).

Privacy is the state of being free from intrusion or disturbance in one's private life or affairs: the right to privacy (The Oxford English Dictionary, 2002:564). It can also be defined as the ability of an individual to exercise control over the collection, use, and dissemination of his or her personally identifiable information (McEwen, 2006:10). The American Heritage Dictionary of the English Language (2006:325) defines it as "The quality or condition of being secluded or concealed from the presence or view of others." The focus of this study is on what privacy rights social networking sites, such as Facebook, violate as they amass large amounts of personal data about users. Analogous to this are the different threats that users face as they use social media to communicate with other users (McEwen, 2006:10).

Social networking websites continue to be extremely popular (Gartrell et.al., 2008:7). Facebook alone has grown to 800 million users who spend a considerable time on social networks each day (Infographic, 2012). These sites are part of the larger trend on the web of Web 2.0 based sites. Web users have an increasing concern about what personal data they should reveal when they are on these sites and when they make use of these social networks (Gartrell et.al., 2008:7).

New technology is a constant due to the Internet continuing to evolve. Simultaneously these new technologies present concerns to users, which need to be explored and evaluated for potential harmfulness (Mansfield-Devine, 2008:18). A number of users see privacy as a valuable interest (Mansfield-Devine, 2008:18) and feel it is threatened, now more than ever, by these technological advances. Currently, databases and Internet records of private data on specific financial statements, medical records, and mobile calls, for example, exist and users have no knowledge about what data is stored about them or who can access that data (Gartrell et.al., 2008:7). This lack of awareness of what information is stored about people and how it is used has led many people to question Facebook's approach towards privacy (Gartrell et.al., 2008:7).

This study focuses on the online privacy issues encountered by users when utilising social media sites such as Facebook. In order to view the effect of these issues, the researcher identified undergraduate students at the North West University to be participants in this study.

Important keywords for the study are: Privacy, Online Advertising, Social Networks, Personal Information, Profiling, Information disclosure, Facebook, Self-disclosure, and Trust. Academic search engines used for the research are: Scirus.com, Sciverse.com and ScienceDirect.com.

1.2 Problem Statement

Users of Facebook often have to register their personal details in order to access the full services they have to offer. As they disclose these details, users unknowingly put themselves at risk due to posting personal information online (Gunatilaka, 2007). Users are often unaware of the kind of implications that sharing their information online can have upon their daily lives (Hoadley, Xu, Lee and Rosson, 2010:3). For example, it may be sold to third parties who can use that information for commercial purposes and in some cases the information is exposed to cyber

security threats (Gunatilaka, 2007). Although Facebook has a privacy policy, it does not always reflect the privacy norms of a particular country or region. Data protection laws that are in place differ from country to country and are not universally applicable to large Internet companies such as Facebook, which operate across international boundaries (Gunatilaka, 2007).

1.3 Research Questions

The main question behind the research is: what are the privacy violations that arise out of social media usage and what is the security awareness of its user base? In order to determine this, the following research questions are formulated:

- Are users leaving their personal information unprotected in the public domain of Facebook and what is the specific nature of this personal information?
- What are the common ways in which Facebook is utilised by its users? Does this usage lead to serious security risks?
- Are the different types of third-party content on Facebook making user personal information vulnerable?
- Is Facebook's privacy policy regarding user information sufficient to protect users?
- How security-conscious are Facebook users?
- Is privacy legislation regarding personal information on cyberspace protecting social media users?

1.4 Research Objectives

The main purpose of this study is to determine the privacy violations that arise out of social media usage as well as the awareness of its user base. In order to determine this, the following objectives are formulated:

- To determine if personal information of users is freely available on Facebook and the nature of this information;
- To assess the common ways Facebook is utilised by its users and whether this presents a security risk;
- To explore the types of third-party content on Facebook for vulnerabilities.

- To examine the Facebook privacy policy regarding personal information;
- To determine the security awareness of users of Facebook.
- To investigate privacy legislation regarding personal information on cyberspace.

1.5 Research Methodology and Design

Methodology

This research utilised a quantitative approach in the form of a descriptive study. The aim with this approach is to determine the relationship between an independent variable and another (dependent or outcome variable) in a population (Kothari, 2004:35). The major purpose of this is to discover the state of affairs as it exists at present. The main characteristic of this study is that the researcher has no control over the variables; he can only report what has happened or what is happening (Kothari, 2004:35).

Design

To investigate the users' online privacy on social media, the study focuses on Facebook. The population selected is derived from the North-West University official Facebook page that currently has 5, 701 likes from students, lecturers and other stakeholders within the Facebook community. North-West University was chosen as it contains the population most active on social media like Facebook, mainly young adults between the ages of 18 – 30 (Pempek et.al., 2009:230). It was also selected due to the ease of access to the population for the researcher. For data collection, three instruments were employed, the polling checklist, fake call and a short survey.

Data Collection

A polling checklist has been developed to collect the data (please see appendix A). Polling is used to get information from a smaller subset of a group of people and use it to learn about the larger population. The advantage of a checklist based on survey research is that they can be generalised and have wide applicability (Kothari, 2004:35).

The research will also employ the use of a false call which is a targeted attack online that was used to assess user's awareness and vulnerabilities to any possible attacks. A survey questionnaire was developed based on the questions used in the poll to confirm the results of the

framework – the checklist instrument. Questionnaires are simple to administer and relatively inexpensive to analyse making them ideal for this study (Kothari, 2004:35). The survey was based on convenience sampling in which students who were free and willing to participate were targeted for a quick response.

Data Analysis

The poll, false call and short survey data which was gathered from the profile pages of users who are stakeholders at North-West University was analysed. Descriptive statistics which include measures of central tendency as well as measures of spread have been used to present the data (Kothari, 2004:39).

Using a combination of tabulated and graphical illustrations as well as statistical commentary following the illustrations, the findings were summarised into separate sections (Kothari, 2004:39). Researchers also use procedures that allow them to interpret or infer the meaning of data. These procedures are called inferential statistics (Kothari, 2004:39).

Ethical Requirements

In order to fulfil the research ethical requirements, the information to be used and citations will be acknowledged. No private information of the users such as their names or other personal data will be included within the study to maintain users' anonymity.

1.6 Significance of the Study

This study is very appropriate for South Africa as the country has young people within tertiary institutions who make use of websites such as Facebook on an almost daily basis. Many different types of activities take place on these online activities. Some of these have the potential to ruin the reputation of a user if they are careless. It would be beneficial for them to understand what the pitfalls of engaging in risky behaviour are.

Research also helps in informing the process of decision-making for policy makers. As such, it is important to hold service providers accountable by creating better laws to govern the activities of sites that amass large amounts of personal data.

1.7 Scope of the Study

The researcher focuses on the privacy aspects of the social networking site Facebook. The population chosen for this study are the students at the North-West University in Mafikeng. The social networking site Facebook was selected for its popularity and easy access to the students who have links to the North-West University Facebook page. To complement this, the researcher also looks at online advertising in relation to the effects that privacy violations have on users of social media. A call was issued to the students in the form of a false spoof attack to test user awareness of privacy. No sensitive data was collected.

1.8 Limitations of the Study

It is very difficult to get an adequate response rate when dealing with a target population such as students. Questionnaires have a low return rate as the forms are not filled in for months, leaving a researcher with no data to analyse. This issue becomes particularly challenging when the amount of time that a researcher can operate within is limited, thus a polling checklist was used to collect data for this study. A polling checklist is a special data collection instrument developed by the researcher (in consultation with other experienced researchers) that can be used to collect data that is publicly about a target population without having to consult each member of that population.

As this study is built around a polling checklist-based data collection instrument and false attack, as opposed to an administered questionnaire, some generalisations are inevitable in the results that were obtained. To compensate for this, the researcher had to assess a larger sample of users (357 users) using the polling checklist. The researcher searched through the whole population of users to ensure that a viable population of users was used.

The researcher also had limited amounts of time and finances with which to conduct this research. The constraint of these precious resources led to the researcher having to work as quickly and efficiently as possible to conclude this research.

1.9 Conclusion

This chapter provided the background and concepts used in this study. Chapter two includes a comprehensive review of all the literature necessary for this study. Chapter three explicates the method of research used for the study and covers the data collection method used as well as the data analysis technique. Chapter four is the presentation of the collected data and a subsequent interpretation of the results. Chapter five is the final summary of the study with recommendations and guidelines.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

Technology continuously advances and this makes it easier to generate and manipulate personal data in various fields, such as the movements of individual users and their location. This has brought about a number of challenges for service providers who try to protect their users' privacy and personal information. It is necessary to identify comprehensive studies that highlight and explain the key issues of the theme of this study. The importance of privacy, as it relates to the online presence of users, has to be understood and appreciated for one to value its capacity and potential. Thus, this chapter seeks to show areas of convergence and divergence between this research, current theoretical concepts and other findings based on previously published research.

2.2 Personal Information on Social Media

Personal information can be identified as any personally identifiable data that can be linked to an individual, for example, credit card details or utility bill statements. With the advent of Web 2.0 as well as businesses moving to e-commerce based systems, we have seen user-generated content taking over the web. This has led to an enormous amount of personal information, which is now available online. Blogs, micro-blogs, wikis and social networks have allowed us to be the content providers over the Internet, which allows for the sharing of ideas and the fostering of better communication.

Facebook is one of the social networks that heavily promote personal information disclosure. This is a by-product of the way the site operates. When a user registers for this service, they typically have to fill in details about their age, gender, place of birth as well as what their interests are and who they are in a relationship with. One might consider all this to be quite invasive considering the fact that this information will be available for public use whenever a user's name is entered in a search.

Furnell (2010:3) states that the loss of personal information by users can lead to some undesirable consequences:

- Snooping and cyber-stalking. Making personal information easily available online can lead to unsolicited attention from unstable or malicious entities. Simply put, it is

easier for people to stalk you when you are always updating your online status as to your activities. The different kind of data as well as the amount, which is generated with a simple search of a person on a social media site, is particularly worrying (Furnell, 2010:3).

- Social engineering. Information that is easily available can be used in targeting a user. What a person posts on their profile or information that other users post about them can give attackers insights into their lives and movements, which could subsequently be used in tricking them to accept a false request or even instructions from an unknown attacker. This can be done online, or by mobile phone or in a face-to-face encounter. In a world where information is power this is a concern that must be taken seriously (Furnell, 2010:3).
- Identity theft. Sufficient information about a user can be collected and pieced together thus enabling attackers to masquerade as the legitimate user, this can have disastrous consequences. In a country such as South Africa, identity theft crimes are serious and can sometimes lead to stolen funds from a bank account or lead to the beginning of a fraudster getting new credit in the unsuspecting victim's name (Furnell, 2010:3).

Evidence of user details being made available exists. For example, a case occurred in 2010 (Emery, 2010), when Facebook announced that it had 500 million active users, shortly after, reports filtered through claiming that details of 100 million users had been collected and posted online in a single unencrypted downloadable list. The list had been created by a security consultant by making use of an automated script which he used to illustrate the privacy risk of some social media sites (Emery, 2010). The data was from what was publicly available on people's profiles and it showed how at risk users actually are.

2.3 Student Online Disclosure on Social Media

Social media, as previously stated, offers users a platform where users can create and share information with others online. It provides us with key insights into how young adults interact with each other and the type of information they reveal in the information age (Pempek, Yermolayeva & Calvert, 2009:230). It is fair to say that a number of young adults with access to either desktop or mobile computing devices are participating in these social media websites on a regular basis.

Previous studies (Pempek et.al., 2009:230) have focused on the usage patterns of university students on Facebook in order to understand the motivation they have for using social media and how they go about using those services. One of these studies entitled 'College Students' Social Networking Experiences on Facebook' (Pempek et.al., 2009:230) is a fascinating report, which offers insights for researchers as well as social media site owners. Here are some of the preliminary findings:

- Students utilise Facebook for about 30 minutes throughout the day as a part of their daily routine (Pempek et.al., 2009:230).
- Students mainly communicated on Facebook using a one-to-many style, in which they were the creators disseminating content to their friends. Even so, they spent more time observing content on Facebook than actually posting content (Pempek et.al., 2009:230).
- Facebook was used most often for social interaction, primarily with friends with whom the students had a pre-established relationship offline (Pempek et.al., 2009:230).

From these findings one can see that Facebook is indeed entrenched in the daily lives of students. The report (Pempek et.al., 2009:230) goes so far as to say that it is as part of their daily routine as much as eating or drinking is. With social media holding such a coveted spot with students, it is no wonder that they are willing to divulge personal information on these sites as they spend so much of their time on the Internet (Pempek et.al., 2009:230).

When it comes to online self-disclosure on these sites, users who post information containing their details tend to think only of the reasons why they wish to share their information and the users with whom they wish to share it (Furnell, 2010:4). The outcome of their actions remains unanticipated as users fail to realise that there is potential for their data to be exploited if it somehow falls into the hands of another party (Furnell, 2010:4). This type of risky online behaviour has cost many a lucrative job offer as employers search for prospective employees online (Furnell, 2010:4). In fact, many companies seek to dissuade employees from commenting on company matters online as it may compromise the employee in question or the organisation (Furnell, 2010:4). Furnell states that:

"Some people not only put too much information online, they also do things that increase their own risk of exposing it. For example, many users on social networking sites will admit to having accepted friend requests from relative (or total) strangers; and having shared their full profile data with them in the process. The practice is perhaps most pronounced amongst young people, where the objective is often not to maintain or re-

establish contact with friends, but rather to collect more online acquaintances than their peers. Thus, issuing or accepting friend requests with strangers, is in no way unusual and helps to enhance their apparent popularity rating.” (2010:4)

The fact that people continue to engage in this behaviour may be one reason why laws about privacy are not effective as users still have not changed their behaviour concerning their online activities on social media sites (Warren, 2008:4). The legislation is mostly reactive, only seeking to punish offenders of Data Protection laws once they have transgressed (Warren, 2008:4). This is inadequate as more proactive laws would encourage site administrators to moderate all activity on social media sites more seriously (Warren, 2008:4).

The next section seeks to explicate the activities that typical users engage in when they are online in social media sites.

In 2010 a study (Balduzzi, Platzer, Holz, Kirda, Balzarotti & Kreugel, 2010:9) utilising a specially devised attack which was launched against a number of most used social networking websites - Facebook, MySpace, Twitter, LinkedIn, Friendster, Badoo, Netlog, and XING - it went on to collect a list of 10.4 million email addresses, which allowed them to easily identify more than 1.2 million user profiles linked with the email addresses (Balduzzi et.al., 2010:9). As they were going through the profiles, they collected information that was freely available in the public domain of each user, which was then used for automated profiling (thus enriching the data they got from every targeted user). This study (Balduzzi et.al., 2010:9) revealed that indeed there are critical vulnerabilities within the systems on which these sites are built. In particular, the information that users provide when registering for an account with these sites is often utilised to provide extra functionality within the social networking service, such as discovering which users might know each other through performing a graph search, which tries to find similarities between users and connect them to each other through that linked data (Balduzzi et.al., 2010:9).

This research (Balduzzi et.al., 2010:9) was particularly focused on automated user profiling based on email addresses used to register for the social media sites. It did not go further to investigate what other personally identifiable information was divulged by unsuspecting users of these sites. It is quite worrying though that with a small piece of information such as a user's email address, he/she can be profiled by trained attackers on these sites.

2.4 Social Media Sites: Facebook

According to Gunatilaka (2007:10), social media can be described as:

Web applications that allow users to create their semi-public profile for example a profile that some information is public and some is private, communicate with those who are their connections (friends) and build an online community. (2007:10)

Web applications have allowed users to be connected to many other groups of individuals, making these applications critical to modern communications. The internet has allowed for the creation and existence of online social networks or social media sites (Warren, 2008:2). Social media offers specific benefits to participants of these sites by enabling them to communicate across various geo-locations and different time zones at any point in the day, thus eliminating any need for people to meet in person (Warren, 2008:2). This description also shows how the expansion of the Internet has led to the popularity of social networking activities online (Warren, 2008:2).

Facebook was created in 2004 to facilitate exclusive interaction in an online social environment for college students (Warren, 2008:2). Facebook functions by enabling users to select one or more groups to which they feel they will belong, for example a high school or university they attended, or a city they are from or once lived in, or an organisation they once worked for (Warren, 2008:2). Every user maintains an online profile which contains basic to detailed personal information such as their name, address, place of residence and work place (Pempek et al., 2009:227). Users can post online to notify other users about what their current activities are by changing their status update, which appears at the top of the newsfeed (Warren, 2008:2). This is the way in which Facebook works to connect individuals.

Facebook members can also upload pictures into virtual photo albums onto their profiles (Pempek et al., 2009:229). Any user can be tagged to these pictures so that his or her name appears underneath the images (Pempek et al., 2009:229). If a particular user wishes not to be associated with the image, they can un-tag themselves from it, thereby removing the name and the link (it must be noted, however, that this does not remove the picture) (Pempek et al., 2009:229). Facebook users can post comments on any photo they view and these appear as messages underneath the image (Pempek et al., 2009:229). Infographic Labs (2012) have an annual statistical analysis of Facebook and other social media sites and have released interesting

facts about Facebook. These statistics illustrate the type of impact it has on the way people communicate. Some highlights of Infographic Labs (2012) research are as follows:

- There are 845 million active users of which 57% are female and 43% male.
- Currently Europe has the largest population of users (223,376,640 representing 27.5% of the total population) this is closely followed by Asia (with 183,963,780 representing 4.7% of the population), Asia may very well overtake Europe within the next few years. Africa has only 3.6% of the Facebook population with a meagre 37,739,380 users.
- 250 million photos are uploaded daily and there are 2.7 billion likes generated daily. There are also 37 million pages with 10+ likes.

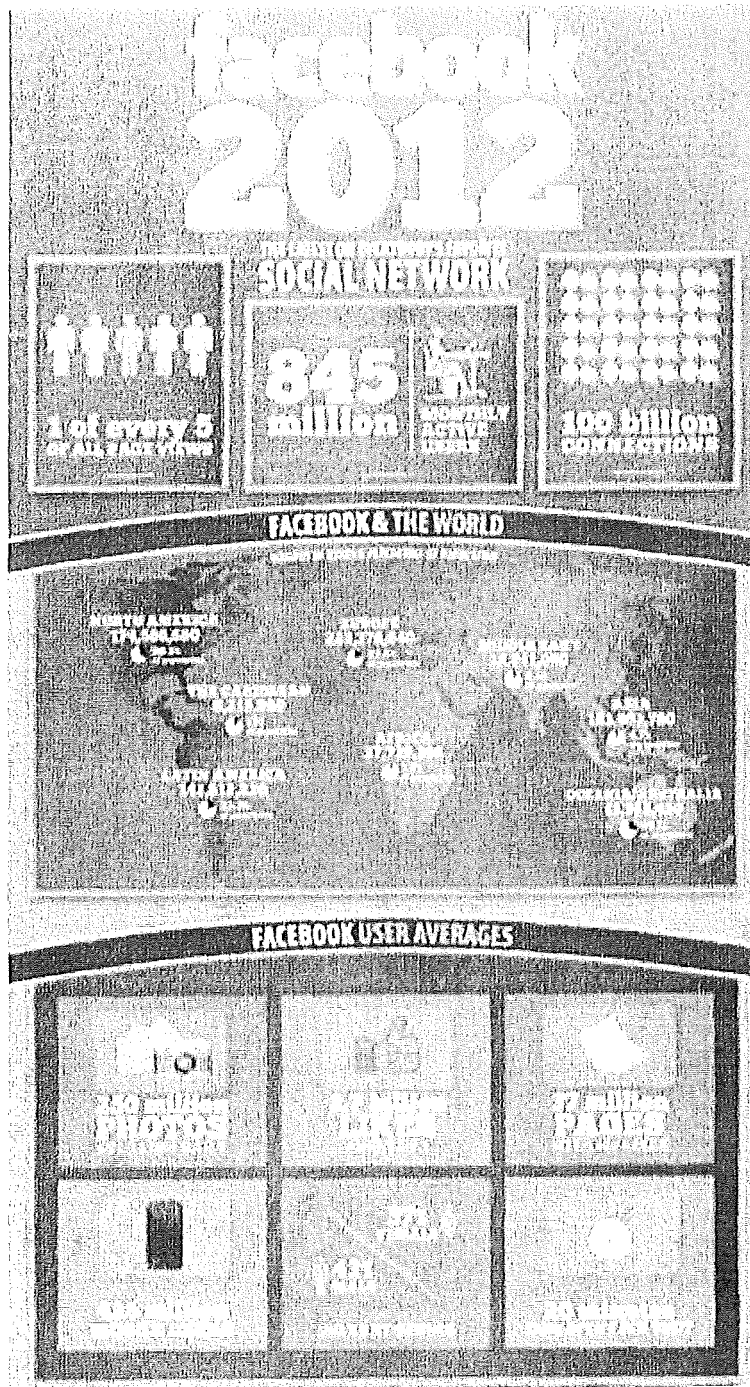


Figure 2.1: Facebook statistics as of 2012 (Infographic Labs, 2012)

These statistics on Facebook (Figure 2.1 above) have been included to show how pervasive a technology this social media platform has become. As Facebook is the most widely used social site (and thus the biggest store of personal information of web users), Facebook possesses the highest probability for privacy violations of all the social sites that are currently operating.

2.4.1 Facebook Privacy Policy

Privacy policies are supposed to explain what information is collected, how it's collected, stored and shared, and how a person might manage such activities (SimplicityLab, 2012:2). Facebook has a comprehensive privacy policy in place to help users understand how the platform operates and how their data is ensured by Facebook. It is comprehensive and covers a wide range of subjects such as the information Facebook receives; information user's share with third parties and how users can view, change, or remove information (Facebook, 2012).

Facebook regularly solicits feedback from users concerning the policy in order to be able to do revise it to make it more effective (Facebook, 2012). This unfortunately does not seem to be making the policy any easier to read and understand. In 2012, a consumer research survey conducted by SimplicityLab was done to assess Facebook's privacy policy. The survey was aimed at evaluating comprehension and perception.

Change in user perceptions of Facebook after reading its privacy policy

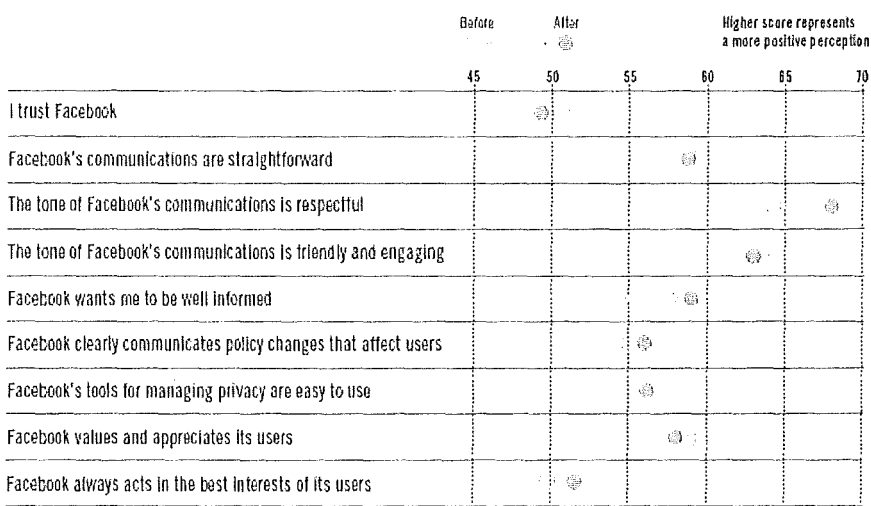


Figure 2.2: User perceptions of Facebook after reading privacy policy (SimplicityLab, 2012)

The survey results illustrate that users experience discomfort with how their information is shared with third parties and affiliates (SimplicityLab, 2012:4). Some highlights of those findings are:

- Only 30% of users understood that their Facebook username is always publicly available, regardless of privacy settings.

- Less than 40% of Facebook users knew how an Application Programming Interface (API) can be used to access and view their public information.
- More than 80% didn't understand that even if a user deletes their Facebook account, information is scrubbed of anything personally identifiable, but remains on Facebook servers permanently.

SimplicityLab (2012:7) findings indicate that the policy is indeed a long technical document written in legal language that will confuse most people who attempt to read through it (SimplicityLab, 2012:4). The survey does outline that the responsibility of personal information is a shared one between the service provider and the user. SimplicityLab (2012:7) state that, "Multiple parties shoulder the responsibility of preserving privacy and increasing user literacy on this topic". They believe that both parties should work towards protecting information. However, most users are not aware of this social contract they have entered into with the service provider and often disregard common advice to go through their personal privacy settings and manually set them to block information leakage.

2.5 Third Party Content on Facebook

Facebook Programs

Facebook has become a platform for different developers (Mansfield-Devine, 2008:5) to create their own programs that users can install. This is one of the ways in which users' personal data has become vulnerable to all kinds of attacks (Mansfield-Devine, 2008:5). The threats these programs pose to users is that they are mostly designed by developers who are not officially a part of Facebook (Mansfield-Devine, 2008:5). As the programs are not part of the service provider's organisation there are no standards to which these programs are developed (Mansfield-Devine, 2008:5). The producers may also have malicious intent as they produce their programs or they may be technically incompetent in designing secure programs that cannot be hacked into (Mansfield-Devine, 2008:5). Facebook has attempted to address this in their privacy policy (Facebook, 2012), as there are restrictions that are supposed to control the way in which these programs work.

One example of how this has backfired in the past is documented in the case of the Secret Crush Application (Mansfield-Devine, 2008:5). Targeted users received messages implying that they had secret admirers (thus playing on their love interests) and in order for them to find out who

these supposed secret admirers are, they had to install the program on Facebook and allow it full access to their data (Mansfield-Devine, 2008:5). What was interesting was the further requirement for users to pass on an invitation-to-install to any other five users before proceeding (Mansfield-Devine, 2008:5). Once installed, users were prompted to download and install an extra component called the Crush Calculator, which turned out to be the Zango application (Mansfield-Devine, 2008:5). It is described as adware as well as spyware (Mansfield-Devine, 2008:5). This is an example of a Facebook program that was designed to be a malicious attack on users by violating their privacy.

Another example is the Superwall program, which was popular on the social network. It used a simple HTML form to get users to leave comments on another user's profile (Mansfield-Devine, 2008:5). The user ID's of both users were held in standard 'hidden' <input> elements. However, with the aid of a tool like Firebug, it was possible to easily insert another ID so that the message would seem to come from another user (Mansfield-Devine, 2008:5). A lack of security know-how on the side of the software developers left the program vulnerable to skilled social engineering attacks (Mansfield-Devine, 2008:5). Third party programs are often poorly coded and this can be exploited to mine personal data (Mansfield-Devine, 2008:5).

Personalised Advertising

Personal data is a valued commodity that can help businesses with a way to strategically target and segment their markets (Mishra & Mishra, 2008:7). Producers of both information goods and services find it beneficial to segment their customers based on observable traits or revealed consumer behaviour/patterns that can be used to increase profits (Mishra & Mishra, 2008:7). The financial value of this information could explain why so many websites gather personal data (Mishra & Mishra, 2008:7). This is a common business practice that is well within the boundaries of the law (Mishra & Mishra, 2008:7). The problem arises when these businesses engage sites such as telecommunications service providers or social media sites for customer data (Tucker, 2010:5). These sites possess an enormous amount of personal information about users and offer advertisers complete, proprietary advertising opportunities to engage in personalised advertising (Tucker, 2010:5). The fact that the future of advertising has become personal is now obvious as the drive for customised marketing has become the tendency in the industry (Tucker, 2010:5).

Social networking sites allow advertisers to engage in sophisticated targeting techniques and actually personalise advertising content (Tucker, 2010:9). As a result, users are worried about what personal data they may unintentionally reveal when they go online and where that information might end up (Tucker, 2010:9). If an organisation selects fans of Microsoft on Facebook as potential customers, it will include a reference to company personnel within the organisation or some Microsoft product in a personalised advert copy in order to get people to buy its products (Tucker, 2010:9).

The information that a user provides to register for an online service (such as a social networking website or search engine) might later be used for telemarketing or sold to another data aggregation company (Mishra & Mishra, 2008:11). Seemingly anonymous information about a user's surfing habits tends to be merged with a user's personal information for the sake of a more personalised and customised service (Mishra & Mishra, 2008:11), which will result in better provision of information services. Apart from gathering data from social media, advertisers can also use adware and cookies and combine these methods for data mining purposes (Mishra & Mishra, 2008:11).

2.6 Privacy

Privacy can be generally defined as "The state of being free from intrusion or disturbance in one's private life or affairs" (The Oxford English Dictionary, 2002:564). In addition to this is another definition which posits that it is "The quality or condition of being secluded or concealed from the presence or view of others" (The American Heritage Dictionary of the English Language, 2006:325). These definitions see privacy as a state of not being visible to unwanted parties, thus it is implied that privacy no longer exists when personal information is made available to others.

Westin (1967:15) has a classic definition describing it as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others". His approach to privacy sees it as the active protection of information about individuals or organisations. The definition views privacy as the user's control over their personal information, including access to it.

The Information Security Group of Africa (2011: 27) states the following with regard to privacy:

“The appropriateness of the use of personal information depends on a number of factors such as context, regulatory requirements, the individual’s expectations as well as the right of an individual to control how their personal information is used or processed.” (2011: 27).

Privacy, thus, includes the element of control that individuals have over information related to them. This element of control is linked to the ability of users to decide what amount of visibility and online presence they wish to have.

Control can be ensured in various ways for example, users can be granted the right (through legal channels) to be informed when personal information about them is collected, the right to decide if this information can be used and for what purposes and by whom (Information Security Group of Africa, 2011: 27). Control over information is something that many users are without when they are online (Information Security Group of Africa, 2011: 27). Privacy will be ensured only when the usage, release and circulation of personal data can be controlled (Information Security Group of Africa, 2011: 27).

Yet, there are other approaches to privacy. A related approach is that of informational self-determination which defines privacy as “the right to determine who accesses person-related data” (Stalder, 2002:8). This interpretation is wide-spread in continental Europe (Stahl, 2000:2). Another related way of dealing with privacy is seeing it in terms of property, where personally-identifiable information can be viewed as a form of personal property, which lead to privacy issues being reduced to more established intellectual property laws (Spinello, 2000:14). As a form of property, users should be entitled to legal rights regarding privacy (Spinello, 2000:14). It is, after all, a way of generating value, not only for the generators of the information, but also for those who collect it and sell it to other parties (Spinello, 2000:14). Using the metaphor of information as property, it becomes clear that it requires legal protection in the form of comprehensive legislation from regulators from the public sector (policy makers and advocates) as well as the private sector (businesses and consumers) (Spinello, 2000:14).

2.6.1 Information Privacy Model

An information privacy model developed by Conger (2005:239) seeks to show the types of relationships that exist between users and the content providers as well as third parties and other members of the broader online ecosystem. She explains how personal information is transacted

between the user and a typical website that processes personal information (and subsequently from the site to third parties or fourth parties without consent from users to whom the personal information belongs) (Conger, 2005:239).

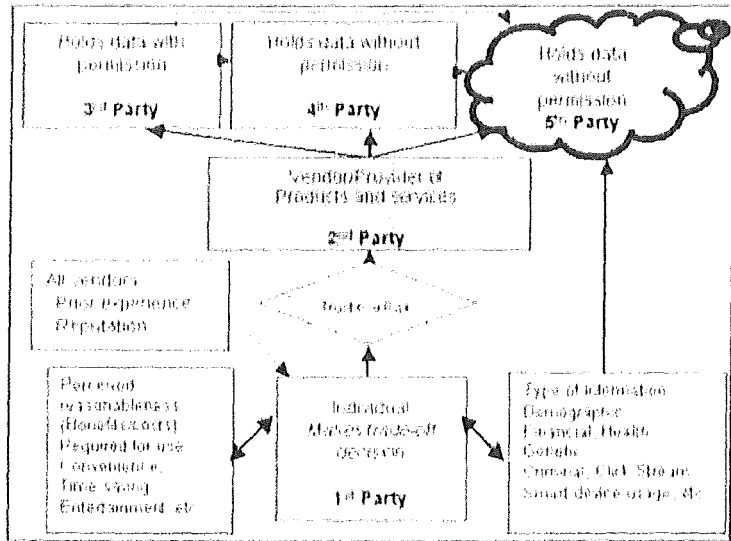


Figure 2.3: Information privacy model (Conger, 2005)

In her model (Figure 2.2 above), part of the individual's decision involves what data to provide to a second party (social media site i.e. Facebook) based on “the expected life and use of that data, perceived reasonableness of the data collected, expected benefits, and expectations of corporate use of the collected data” (Conger, 2005:239). When a transaction is completed, information is shared with any legal data-sharing entities, for example the third party data user (i.e. online marketer) who is an established data-sharing partner (Conger, 2005:239). Third party organisations would then sell this information or provide it, through legal requests, to fourth parties. Major problems begin to arise when these so-called fourth parties use this information without user and/or Facebook permission (Conger, 2005:239).

Conger (2005:239) believes that sparse research exists concerning users' risk perception of online self-disclosure and what happens to personal information when third or fourth parties get it from service providers. Hence, the darker shaded boxes in the illustration show when information is passed on from second to third, fourth or fifth parties. This study does not seek to directly address what takes place when information is passed along these channels (Conger, 2005:239). It is more concerned with user perceptions regarding such transacting, which often

takes place behind the scenes with these sites. This model is useful in showing the areas where users are unaware of what happens to their personal information (Conger, 2005:239).

2.7 Legislative Framework

2.7.1 The Need for Privacy Legislation

The Internet is a constantly evolving tool that affects the way in which we live our lives (Stahl, 2000:2). It is a technology that has brought about many challenges. One of these challenges is a threat to personal privacy, which is generally considered as one of the big issues of computer science ethics (Stahl, 2000:2). New technology always has the potential to create a number of concerns for privacy protection (Stahl, 2000:2). When users participate in these social networks, where their actions can be tracked without their awareness or permission, it is seen as a real threat to the concepts of openness and freedom, which the Internet has always tried to exemplify (Stahl, 2000:2). Without sufficient regulation, this can cause the online environment to become very dangerous with many pitfalls that users will need to watch out for (Stahl, 2000:2). The most important Internet privacy concern comes from the secondary use of information, this is defined as personal information collected for one purpose and used, subsequently, for a different purpose (Mishra & Mishra, 2008:6). Studies suggest that

- (a) users are more willing to provide personal information when they are not identified,
- (b) some information is more sensitive than other information, and
- (c) the most important factor is whether or not the information will be shared with other companies. Users overwhelmingly disliked unsolicited communications and any form of automatic data transfer (Mishra & Mishra, 2008:6).

Many governments have begun to recognise that this is a particularly sensitive issue for their citizens (Mishra & Mishra, 2008:6). As such, governments have created laws and regulations which seek to address the issue of privacy (Mishra & Mishra, 2008:6). Supporting those regulations, however, are principles of privacy that are not always easily identifiable, but have importance in recognising how and why privacy is legally protected (Stahl, 2000:2). Privacy concerns are making users nervous about going online. There are a clear set of activities commonly seen as definite privacy invasions:

- collecting and analysing user data without the user's knowledge/consent or authorization (Mishra & Mishra, 2008:6),
- employing user data in a way other than was authorized, and (Mishra & Mishra, 2008:6)
- disclosing or sending user data to others without the user's knowledge and authorisation (Mishra & Mishra, 2008:6).

Consumers wish to be regularly informed about what personal data is being collected from them, how that data will be utilised and if the information will only be used in an aggregate form (Mishra & Mishra, 2008:6). Users will be less suspicious if they view information collected about them in the context of an existing on-going business relationship, or as if it is needed for a transaction, or as if it will be used to make reliable and valid inferences, and as if they have the ability to control its future use (Baker, 1991:42).

2.7.2 Overview of the International Development of Privacy Legislation

2.7.2.1 The Development of Privacy Legislation in the United States of America (USA)

Privacy is recognized as an important issue affecting businesses and consumers and its significance has continued to escalate as the value of information continues to grow (Mishra & Mishra, 2008:6). Many feel that it should be the responsibility of government to protect the individual from corporate abuses by implementing and enforcing legislation (Mishra & Mishra, 2008:6).

Privacy legislation in America had its beginnings in Congressional hearings held in the 1970's, where privacy advocates sought to ban credit bureaus from using centralized computer databases (Mishra & Mishra, 2008:6). A need was soon realised that organisations have certain responsibilities and that individuals have certain rights, regarding information collection and use (Mishra & Mishra, 2008:8). Since 1973, the Fair Information Practice principles have served as the basis for establishing and evaluating U.S.A. privacy laws and practices (Mishra & Mishra, 2008:8).

These principles consist of:

- 1) notice/awareness;
- 2) choice/consent;

- 3) access/participation;
- 4) integrity/security;
- 5) enforcement/redress (Mishra & Mishra, 2008:9).

The above principles have led to is a general consensus that organisational privacy policies should reflect these very principles (Mishra & Mishra, 2008:8). Privacy violations that still occur today prove, however, that this is not always the case (Mishra & Mishra, 2008:8). America has had a relatively business-friendly, minimal intervention approach that encourages organisations to provide self-regulated privacy protections (Turner & Dasgupta, 2003:10). This may explain why most social media sites are not held accountable for violations as they are registered companies in the United States.

2.7.2.2 The Development of Privacy Legislation in the European Union (EU)

During the early 1980's the Organisation for Economic Cooperation and Development (OECD) issued guidelines similar to the ones the U.S.A. produced on the protection of privacy and trans-border flows of personal data (Mishra & Mishra, 2008:8). The OECD guidelines are the current best practice global standard for privacy protection and are the recommended model for legislation in member countries (Mishra & Mishra, 2008:8). Although not legally binding, the guidelines are recognized by all OECD members, especially the European Union (EU) and America (Mishra & Mishra, 2008:8). They are implemented differently in individual nations, suggesting that approaches to privacy differ between countries (Baumer, Earp & Poindexter, 2004:405).

As the EU developed their privacy legislation in 1995, they produced their own legal document – The Directive on Data Privacy (Mishra & Mishra, 2008:10). The legislation places the onus on companies and organisations—not individuals—to seek permission before using personal information for any purpose (Mishra & Mishra, 2008:10). The European Union has taken a pro-consumer approach with tough regulations that ban the use of personal information until consent is obtained from users (Turner & Dasgupta, 2003:8). EU directives, which are based on the OECD guidelines, are noted to be stricter and are even more comprehensive with respect to privacy than similar guidelines in America (Mishra & Mishra, 2008:9).

The EU restricts the operation of American companies, unless they fall in line with the EU guidelines and it is estimated that 90 percent of US companies have not addressed the EU directive (Turner and Dasgupta, 2003:8). An example of one of the directives is that companies are required to inform customers when they plan to sell their personal information to other firms (Kruck, Gottovi, Moghadami, Broom & Forcht, 2002:6). Hence the occasional anti-Trust lawsuits that the EU files against search engines like Google.

2.7.2.3 The Development of Privacy Legislation in South Africa (RSA)

In South Africa, a relatively new law, enacted in August 2013 was approved by cabinet (Information Security Group, 2011:30). Known as the Protection of Personal Information Act of 2013 (PoPI), it seeks to give effect to the right to privacy as explained in the Constitution by introducing measures to make sure that organisations process personal information in what can be said to be a fair, responsible and secure manner (Information Security Group, 2011:30). This law protects many individuals as it punishes organisations and third parties that fail to take sufficient steps to secure private and personal information such as identity and contact details (Information Security Group, 2011:30). While it is laudable to have this law in place, the challenge of enforcing it on international companies such as Facebook is difficult as these operate across borders where different privacy laws exist (Information Security Group, 2011:30). It is yet to be evaluated for its effectiveness in dealing with privacy and businesses as it is still a relatively new piece of legislation (Information Security Group, 2011:30).

2.7.3 Challenges faced in Implementing Privacy Laws

Any government's approach to how personal information is handled becomes a challenge when one considers that most Internet companies operate outside the borders of their host nations and have a global reach (Mishra & Mishra, 2008:12). It is not easy to find an immediate solution to this challenge of policing international cyberspace. A central problem is that behaviour on the Web can't be controlled (Mishra & Mishra, 2008:12). This has traditionally been seen as a good thing. It is also difficult to reach international consensus on Web privacy because the privacy concept is heavily dependent on widely variable cultural and political issues (Mishra & Mishra, 2008:12). For example, the self-regulatory approach adopted by the U.S.A. is in direct contrast with the government-mandated approach adopted by the European Union (EU). This has to do with the region-specific attitudes towards state intervention in online activity (Mishra & Mishra, 2008:12).

Governments have a mediocre track record for developing laws as well as policing online privacy, due to the fact that designing appropriate laws for data protection is a lengthy process because industry specialists, practitioners, advocates and users need to be consulted (Mishra & Mishra, 2008:12). Various international countries have implemented varying degrees of privacy legislations (such as the OECD guidelines) which are designed to control how companies access and utilise information of potential customers (Mishra & Mishra, 2008:12).

Certain sectors of the online community oppose government involvement and believe that privacy and protecting their personal data is the responsibility of individuals who enter into contracts with companies (Smith, 2004:201). If one considers what Smith (2004:201) is saying, then it can be argued that he is advocating for users to put pressure on service providers in order for them to effectively manage personal information. This pressure usually manifests itself in the form of the general populace lobbying the specific companies via civic groups and non-governmental institutions, which will raise their concerns about protecting their information online (Smith, 2004:201).

Until privacy laws are really enforced, however, companies will find few incentives to protect and respect privacy mainly because most users don't even realise that their privacy can be violated. The challenge of getting government to be proactive about the privacy of users when they formulate legislation may be the key to achieving success in this area.

2.8 Conclusion

This chapter provided a comprehensive review of the related literature, it includes views from other scholars concerning privacy, the law, social media and students who frequently utilise these sites. Privacy and its relation to the law was a particularly important area. Literature concerning the challenges faced in implementing privacy legislation is also discussed. The researcher sought to provide a link between such views and the reality online, i.e. as users experience it. How privacy relates to the common user is fundamental when considering the platforms within which social media sites operate. The next chapter looks at the methodology that was employed in the research.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

This chapter examines the research design that was used for this study. The focus is on the methodology, the data collection instrument, the population and sample size for the study as well as the sampling procedures that were used. The manner in which data were analysed, interpreted and presented is outlined in detail as well.

3.2 Methodology

Research methodology can be defined as a description of a proposed study designed to investigate a given problem (Kothari, 2004: 5). There are two main types of methodology, qualitative and quantitative research approaches.

Qualitative Research

Qualitative research aims at discovering the underlying motives and desires, using in depth interviews for the purpose. Qualitative research is characterised by the fact that the researcher works on the basis of an open question (Jonker & Pennink, 2010:92). It is research in which the researcher makes an attempt to understand a specific organisational reality and occurring phenomena from the perspective of those involved (Jonker & Pennink, 2010:92).

The researcher does not start his research by means of theoretical notions, or a model or concepts that needs to be tested, but with several sensitising concepts (Jonker & Pennink, 2010:92). Sensitising concepts are pre-theoretical by nature and serve to steer observations (Jonker & Pennink, 2010:92).

The essence of the research is, 'a systematic search for the unknown' (Jonker & Pennink, 2010:92). In order to achieve this, the researcher will try to become one with the situation that is being examined (Jonker & Pennink, 2010:92). In this approach research is a continuous process (Jonker & Pennink, 2010:92).

Quantitative Research

Quantitative research is based on the basic approach that knowledge about reality can be obtained 'through the eyes of the researcher (Jonker & Pennink, 2010:85). By means of a careful and consistent study of literature, accepted concepts and current findings by others, which are then used to help formulate the problem definition, research objective and research question (Jonker & Pennink, 2010:85).

The researcher conducts research in 'the' reality (the empirical situation to be examined) by means of carefully chosen instruments (Jonker & Pennink, 2010:85). The researcher observes 'through his own eyes', in other words, by designing and realising the research he determines what is observed or measured – and what is left out (Jonker & Pennink, 2010:85). The researcher pays great attention to methods and techniques; this care determines to a great extent the quality of the research (Jonker & Pennink, 2010:85). The attitude of the quantitative researcher implies that he tries to be an objective observer (Jonker & Pennink, 2010:85).

Quantitative research is an investigation into a recognised problem, measured with numbers and analysed using statistical techniques (Kothari, 2004:5). It involves numerical data gathered through tests, surveys, observations, interviews. The variables are not manipulated but are measured as they occur (Kothari, 2004:5).

For this study, the quantitative approach was chosen. The major strength of this method is to discover the state of affairs as it exists at present (Kothari, 2004: 7). This made it ideal for this research as the researcher has no control over the variables, with only the ability to report what has happened or what is happening (Kothari, 2004: 7). It therefore allows for an objective reporting of facts as there are (Kothari, 2004:7).

Research Paradigms

A paradigm is a set of beliefs about the nature of social reality, that is, the nature of the "world" and the individual's place in it (Shanks & Parr, 2003:12). Mack (2010:4) also defines a paradigm as "a loose collection of logically related assumptions, concepts or propositions that orient thinking and research."

Positivist Paradigm

The positivist paradigm is also called the scientific paradigm (Mack, 2010:55). The purpose of research in this paradigm is to prove or disprove a hypothesis (Mack, 2010:35). Other characteristics of positivist research include an emphasis on the scientific method, statistical analysis, and generalisable findings (Mack, 2010:5). Furthermore, positivist research usually has a control and experimental group and a pre/test post method (Mack, 2010:5).

Positivism maintains that the scientist is the observer of an objective reality (Mack, 2010:6). From this understanding of ontology, the methodology for observation in natural science was adopted for social science research (Mack, 2010:6). The positivist paradigm asserts that real events can be observed empirically and explained with logical analysis (Mack, 2010:6).

Interpretive Paradigm

The interpretivist paradigm can be also called the “anti positivist” paradigm because it was developed as a reaction to positivism (Mack, 2010:7). It is also sometimes referred to as constructivism because it emphasizes the ability of the individual to construct meaning (Mack, 2010:7). Interpretivism’s main tenet is that research can never be objectively observed from the outside rather it must be observed from inside through the direct experience of the people (Mack, 2010:7).

The role of the scientist in the interpretive paradigm is to, “understand, explain, and demystify social reality through the eyes of different participants” (Cohen, Manion & Morrison, 2007:19). Researchers in this paradigm seek to understand rather than explain (Mack, 2010:7).

Critical Paradigm

The critical paradigm stems from critical theory and the belief that research is conducted for “the emancipation of individuals and groups in an egalitarian society” (Cohen et. al., 2007:26). Critical theory originated from the criticism that educational research was too technical and concerned with only efficiency and rationality of design, neglecting social inequalities and issues of power (Gage, 1989:5). According to the critical theorists, researchers should be looking for the “political and economic foundations of our construction of knowledge, curriculum, and teaching.” (Gage, 1989:5)

The critical researcher aims not only to understand or give an account of behaviours in societies but to change these behaviours (Cohen et. al., 2007:26).

3.3 Design

A research design is the arrangement of conditions for collection and analysis of data in a manner that aims to combine relevance to the research purpose with economy in procedure (Kothari, 2004:4). In fact, the research design is the conceptual structure within which research is conducted; it constitutes the blueprint for the collection, measurement and analysis of data (Kothari, 2004:4).

This study utilised the mixed-method approach for the research design data collection. Mixed-method studies use different methods of data collection and analysis within a single research methodology (Hesse-Biber, 2010: 12). This approach was chosen as it allowed for the subject matter to be viewed from a variety of angles (Hesse-Biber, 2010: 12). It also allowed for the collection of pertinent and precise information concerning the current status of phenomena used to draw valid general conclusions from the facts discovered (Kothari, 2004: 37).

Data Instrument Procedure

Due to the mixed nature of this research it must be clearly stated that each instrument utilised a different data collection procedure and sample size for each instrument. For example the polling checklist had a total of 357 participants while the false call (a false call is an attack done online to get people to reveal their personal information by creating a fake message requesting them to respond with their private details) 237 participants and the short survey had 70 participants (please see the sample technique and size section of this chapter for further explanation).

Polling Checklist

A polling checklist (see appendix A) was designed to profile users by capturing the details of users on Facebook. It was designed to cover the privacy and data protection concepts of the research. The checklist is further explained under the Data Instrument section of this chapter.

The profile pages of each participant (who has a Facebook profile) were compared against a set checklist that covers different aspects of the user's activities on the social media platform which

are sensitive. These sensitive activities may be violated in the absence of privacy laws. In total, 357 user profiles were targeted for this study based on the convenience sample. Data collection took a little over 2 months as each page required a minimum of 15 minutes with some taking longer than that.

False Call

As a test to see whether user data is secure on Facebook and whether users are informed and knowledgeable, a false-call was carried out to evaluate user awareness to online privacy and security issues on social networks. An experimental user account was created and users were invited to accept friend requests. The acceptance of the call meant that their details were now available for analysis. The users targeted were friends to the researcher. A total population of 237 users had been selected for this second method of data gathering which was also employed to validate the results of the first instrument, the framework.

The second method was aimed at proving that users rarely try to check the authenticity of friend requests and the identity of the requesters (callers).

Survey

Furthermore, a short survey was developed based on the questions used in the poll to confirm and validate the results of the checklist instrument (see appendix B). Surveys enable the researcher to obtain data about practices, situations or views at one point in time through questionnaires or interviews (Davison, 1998:44). Quantitative analytical techniques are then used to draw inferences from this data regarding existing relationships (Davison, 1998:44). The use of surveys permit a researcher to study more variables at one time than is typically possible in laboratory or field experiments, whilst data can be collected about real world environments (Davison, 1998:44).

The survey utilised a short questionnaire with few questions that covered Facebook's privacy policy, user awareness of privacy legislation and their attitudes regarding regulation. The survey had a few questions and it was distributed to 70 participants because it was designed to support and confirm the findings of the main research instrument, the checklist.

3.4 Population

Polling Checklist

The population for the research consisted of students doing their studies at the North-West University. In order to investigate online privacy on social media, the study has set its focus firmly on Facebook. This is because Facebook is the largest social media site available with a staggering 845 million users (as of 2012), a number which is steadily growing (Facebook, 2012). The population was selected from the students who have 'liked' or added the official North-West University (NWU) Mafikeng Campus Facebook page that currently has 5, 701 likes from students, lecturers and other stakeholders from the university. Students were chosen due to their very active online activities and the abundance of information they generate online which make them targets of online privacy violations.

False Call

The False call made use of the researcher's own social circle. An experimental Facebook account, using a particular user's name, was created. The first step was to copy the targeted user's information from Facebook. The personal information copied varied from the person's name, address, email address, hometown and so forth. The account had to be credible so it had to contain the selected person's likes and interests. Lastly, their profile photo was also copied to allow other people to see that it was the selected person.

Survey

For the survey, the population is made up of students doing their studies at the North-West University. They were targeted due to their activeness on Facebook (Pempek et.al., 2009:230), which happens to be one of the widely used social network platform at the university.

3.5 Sampling Technique and Sample Size

Polling Checklist

The sample population was obtained by assessing how many stakeholders have 'liked' the official North-West University (NWU) Facebook page that currently has 5, 701 likes from students, lecturers and other people from the university. According to Krejcie and Morgan (1970:56), it is within the acceptable range of sample size to use 357 participants when your total

population is between 5, 000 to 6, 000 people (see Figure 3.1). The minimum accepted sample size was also chosen by researcher due to the length of time required to go through each profile page (it took 15 minutes per profile).

North-West University was chosen as it contains the population most active on social media like Facebook, mainly young adults between the ages of 18 – 30 (Pempek et.al., 2009:230). It was also selected due to the ease of access to the population for the researcher.

Convenience sampling was used here due to the accessibility and proximity of the target population. All participants were currently enrolled at the university and have their personal data available on Facebook.

N	S	N	S	N	S	N	S	N	S
10	10	100	100	1000	1000	10000	10000	100000	100000
15	15	150	150	1500	1500	15000	15000	150000	150000
20	20	200	200	2000	2000	20000	20000	200000	200000
25	25	250	250	2500	2500	25000	25000	250000	250000
30	30	300	300	3000	3000	30000	30000	300000	300000
35	35	350	350	3500	3500	35000	35000	350000	350000
40	40	400	400	4000	4000	40000	40000	400000	400000
45	45	450	450	4500	4500	45000	45000	450000	450000
50	50	500	500	5000	5000	50000	50000	500000	500000
55	55	550	550	5500	5500	55000	55000	550000	550000
60	60	600	600	6000	6000	60000	60000	600000	600000
65	65	650	650	6500	6500	65000	65000	650000	650000
70	70	700	700	7000	7000	70000	70000	700000	700000
75	75	750	750	7500	7500	75000	75000	750000	750000
80	80	800	800	8000	8000	80000	80000	800000	800000
85	85	850	850	8500	8500	85000	85000	850000	850000
90	90	900	900	9000	9000	90000	90000	900000	900000
95	95	950	950	9500	9500	95000	95000	950000	950000

Figure 3.1: Sample Size Table (Krejcie & Morgan, 1970)

False Call

The researchers total social circle contact list was included for the false call. This included family, close friends and work colleagues. The total number of participants from that social circle was 237. They were chosen for ease of access to the researcher, availability on a social media platform (Facebook) and the quickness of their response to the false call.

Survey

As mentioned before the survey was based on convenience sampling in which students who were free and willing to participate were targeted for a quick response. The survey utilised a short questionnaire with a few questions and it was distributed to 70 participants because it was designed to support and confirm the findings of the main research instrument, the checklist. 70 respondents were chosen as a smaller sample size meant a higher chance of collecting data from students on campus as well as limited time constraints within which to acquire adequate.

3.6 Data Collection Instrument

Polling Checklist

A research instrument is a scale by which data for the study is gathered for further analysis. For this study, the researcher chose to collect data using a polling checklist (please see appendix A). For the profiling, a polling checklist was utilised to capture the details of users on Facebook. This guide was developed to cover the privacy and data protection concepts of the research.

The polling checklist was developed by the researcher (in consultation with other experienced researchers) to cover the main thematic areas of the research. These areas are derived from the research questions, originally outlined in chapter one. All of the 357 user profiles on Facebook required 15 minutes per profile. The polling checklist are filled in and then matched to ensure that the information that is observed correlates with the questions that the polling checklist poses. The polling checklist was designed to gather information about the activities of users on Facebook, the privacy options available to them and whether they are being targeted by third parties on social media.

This instrument is appropriate as it generates numerical data and gathers data that can be processed statistically as well as providing descriptive, inferential and explanatory information. The method is good for manipulating key factors and variables so as to derive frequencies such as the most common demographic information (age, ethnicity or gender). It gathers standardised information as the researcher uses the same instrument with the same questions for all the members of the target population and this allows the researcher to make generalisations about the population. In particular, the advantage of polling checklist based on survey research is that they can be generalised and are widely applicable.

False Call

A false call is an attack done online to get people to reveal their personal information by creating a fake message requesting them to respond with their private details. In this study it has been used to assess whether users do indeed respond to user profiling and online enticements from falsified accounts. False impersonation of an entity, organisation or another person's identity with the intent to commit fraud is used in the real world every day to carry out crimes (Smith, 2004:213). In this study, the false call is used in a more practical way to confirm and validate the generalisations derived from the findings of the polling checklist, thus providing the study with more data concerning the online behaviour of users. Therefore it is vital to the overall research design.

Survey: Questionnaire

A survey is an investigation of the opinions or experiences of a target population by asking the population questions (Kothari, 2004:17). The purpose of survey investigations is to provide scientifically gathered information to work as a basis for the researchers for their conclusions (Kothari, 2004:17).

A questionnaire consists of a number of questions printed or typed in a definite order on a form or set of forms. The respondents have to answer the questions on their own (Kothari, 2004:100). The advantage of the questionnaire is low cost even when the universe is large and is widely spread geographically and large samples can be made use of with the results can be made more dependable and reliable (Kothari, 2004:100).

For this study, the questions were asked in person with the aid of a short questionnaire which was aimed at investigating user awareness regarding privacy legislation, regulation and Facebook policies regarding privacy. When used in combination with the checklist and false call, the survey confirms and validates the findings of the other instruments.

3.6.1 Reliability and Validity

Reliability can be defined as an indication of the extent to which an instrument contains errors that may impact upon the study while validity refers to the extent to which an empirical measure adequately reflects the extent to which a test measures what it purports to measure. In order to

ensure these, the researcher conducted a short trial of the instrument - a pilot study using a smaller sample than the one outlined above in order to refine the polling checklist and ensure that it posed relevant questions that it would answer the research questions outlined in chapter one.

3.6.2 Ethical Requirements

In order to fulfil ethical research protocols, the literature used in this study is acknowledged and rightfully cited. In addition, no private information of the users, such as their names or other personal data, is included in the study so as to maintain users' anonymity.

University regulations dictate that all research studies must be cleared by its established ethical committee, which evaluates the validity of each potential research study before it commences. This research was cleared by the university and an ethical clearance number was issued (NWU-00212-13-A9).

3.7 Data Analysis and Presentation

Descriptive statistics are procedures used to summarize, organize, and make sense of a set of scores or observations (Munro, 2005:2). Descriptive statistics are typically presented graphically, in tabular form (in tables), or as summary statistics (single values) (Kothari, 2004:39). Descriptive statistics summarize data to make sense or meaning of a list of numeric values (Munro, 2005:2).

Descriptive Statistics include basic numerical summaries and graphical summaries in the format of bar graphs and pie charts (Kothari, 2004:39). These graphs seek to display data accurately and clearly. Descriptive Statistics are specifically used to describe or summarize numeric observations, referred to as data (Munro, 2005:2). Researchers use descriptive statistics to summarize sets of individual measurements so they can be clearly presented and interpreted (Kothari, 2004:39). Coding procedures such as calculating frequency distribution, measures of central tendency-mean, median and mode calculating percentiles and percentile ranks as well as establishing norms were also used for the analysis of data (Singh, 2006:224).

Inferential statistics have also been used for this study. Inferential statistics are procedures used that allow researchers to infer or generalize observations made with samples to the larger population from which they were selected (Kothari, 2004:39).

3.8 Conclusion

A quantitative research design is employed for this study as it allows for an adequate sample to be chosen from a target population of students who form the basis of this study. Its ability to allow the researcher to make generalisations about the broader population makes it invaluable to a study of this nature. A polling checklist was developed to collect the data in conjunction with a spoof attack that aims to test users' privacy awareness when they are online. Data were analysed, interpreted and presented using the readily available Microsoft Excel and IBM Statistical Package for the Social Sciences software packages.

CHAPTER FOUR

DATA ANALYSIS

4.1 Introduction

This chapter presents the results of data collection as well as analysis to ensure that conclusions can be drawn from this study. Data has been analysed using descriptive statistics. Descriptive statistics describe a sample from a target population in terms of numerical measures that are computed from data (Katznelson, 2006:1). Standard coding and editing procedures such as the calculation of percentiles and percentile ranks, frequency distribution of items under study and the calculation of central tendency-mean, median, mode and establishing range were used for statistical analysis (Singh, 2006:224). Data collected is presented primarily in the form of tables and figures with an interpretation of the results below each figure.

4.2 Demographics

Gender and Age

From the 357 respondents, 55% ($n = 198$) were female, while 45% ($n = 159$) were male (Figure 4.1). This correlates with the statistics released by Infographic Labs (2012), which were mentioned in the literature review in chapter two. According to Infographic Labs (2012), Facebook has more female than male users. The greatest age group represented was between 18 and 25 ($n = 214$). This was to be expected considering the fact that the majority of students using Facebook are undergraduate students.

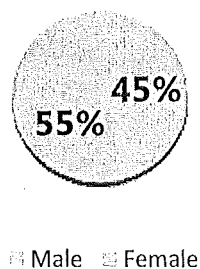


Figure 4.1: User Gender

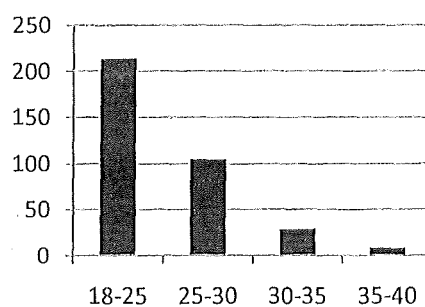


Figure 4.2: Age groups

Most users are female between the ages of 18 and 25 with general likes, which include entertainment and celebrities. A good portion of them access social networks through their

mobile devices as this allows them to stay in touch and communicate on a daily basis. This means that on a daily basis they generate personal information about where they go, what they do and who they spend their time with. This rich treasure trove of information can be utilised by any number of interested parties.

Place of Residence and Place of Work

The majority of users are from Mafikeng as the University campus is located in Mafikeng, this was to be expected as well. The rest are from the surrounding cities located in the North-West Province. About 69% ($n = 246$) of them are unemployed while a combined 31% ($n = 111$) stated that they were employed either at the university or elsewhere.

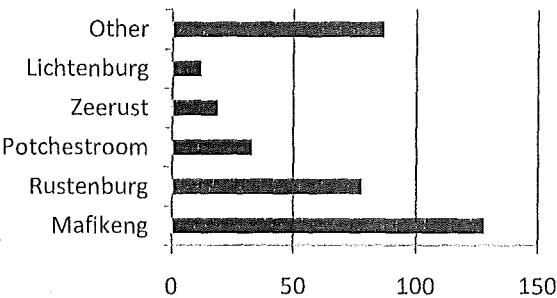


Figure 4.3: Place of Residence

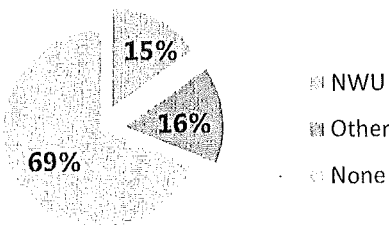


Figure 4.4: Place of Work

4.3 Users' Personal Information and Self-Disclosure

Of the Facebook users selected for this study, 67% ($n = 240$) have personal information partially available online, while 33% ($n = 117$) have their full personal details available. This is because Facebook does not put a default block on new users' personal information when they sign up to be a member on the site. This might be because Facebook wishes to encourage users to find friends and view other people's information. Unfortunately, this makes it easier to view each other's information and, thus, makes it possible for those with malicious intent to get hold of sensitive data. The biggest challenge that users face is changing their perception of themselves as being part of a group to being individuals. They believe that no one would bother attacking them. There is however, a good reason for them to be victims of cyber attacks. The information that users willingly supply is highly valuable. Attackers are after user ID's and passwords for

Facebook accounts and they use data mining to obtain those credentials. These attackers have figured out that people hardly ever change their user names and passwords, so if they could

figure out what their usernames and passwords are for Facebook, it is likely that they could do the same thing with the victims' banking details as well. This is the basic form of social engineering, a potential attacker uses specific information, such as a birthday, a pet's name, a spouse or lover's name, or a high school. Things which people often use for passwords or for the security questions to recover an online account with a bank or email account.

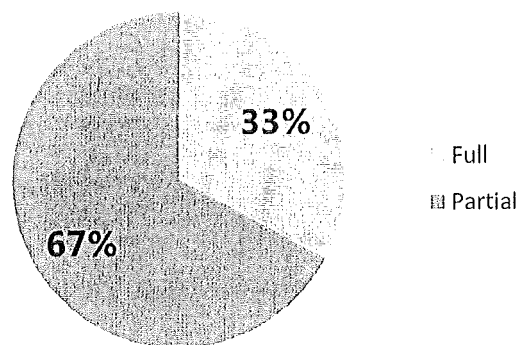


Figure 4.5: Availability of users' details

Most users have their data partially available on Facebook. This could be due to the fact that Facebook needs user profiles to be semi-accessible to the public in order for people to find new friends with who they could possibly have common interests (Likes). The unfortunate consequence of this is that not everyone wants to be a friend on Facebook.

Number of User Friends and Location Sharing

From the findings, 28% ($n = 101$) of students have more than 100 friends with the next significant figure being 25% who have between 300 - 400 friends (Figure 4.6). Only 7% ($n = 26$) have friends in excess of 500. This indicates that most users engage in a moderate amount of networking. Most users only accept friend requests from people that they already know as opposed to adding anyone who wishes to be their friend.

The fact that only 7% of the sample have Facebook friends in excess of 500 could indicate that they are weary of adding more people or connecting with total strangers on Facebook, which is an unsafe practice that should be discouraged on social networks in any case. In the same category, they are not interested in using software programs on Facebook. These programs may be too difficult to use or may not be in-line with their interests.

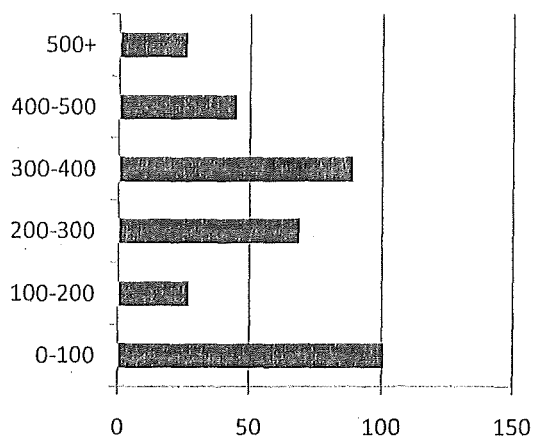


Figure 4.6: Number of Friends

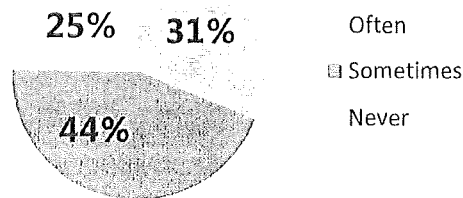


Figure 4.7: Geo-Location Sharing

Location Sharing

Interestingly, 75% ($n = 269$) either often share or sometimes share their geo-location with their friends on Facebook. Most of them indicated that they share their location when they travel far for a holiday trip or when they are at a restaurant, for example, spending time with other friends (Figure 4.7). This must be based on the level of trust that these users have with their peers on the social network, which enables them to share their location on a regular basis. To a skilled and seasoned social engineer, location sharing is integral in tracking movements and establishing patterns of an individual. This information is quite easy to obtain from the profiles of this set of users. Attacks launched on social networks would not be possible were it not for this high level of trust that people place in these sites (Pempek et al., 2009:229)..

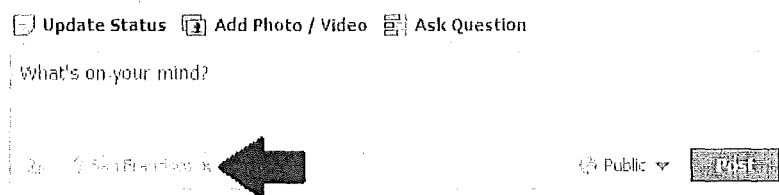


Figure 4.8: Example of Geo-Location Sharing on Facebook (Blair, 2011).

Figure 4.8 shows how users have every post 'tagged' with their location (by default unless they turn off this option) at the bottom, which acts as a signature to every post or upload they do on Facebook. In as much as users share their location, it seems they are also willing to share events they attend (about 22% ($n = 77$) and 14% ($n = 50$)). This is generally considered an unsafe

practice, but on social networks it is subtly encouraged as Facebook allows users to ‘check-in’ and promote what they are doing (Pempek et al., 2009:231). Blair (2011), states that if someone wanted to plan to rob the place of residence of one of these users, it would not take too long to establish a pattern of that individual's movements and to decide on a day to initiate the malicious scheme. For example figure 4.9 clearly shows a user post where the location of that particular user is and who is with him. An informed attacker will study such details along with the time and date of the post to begin tracking the user (Blair, 2011). This is just one of the negative consequences of this occurrence on Facebook.

Some users even tag, or include who they are with, when they post these location sharing updates as can be seen in Figure 4.9. This can be dangerously revealing as the user’s close relationships are exposed to anyone who knows how to use the information and link it with other information data mined from the social network.

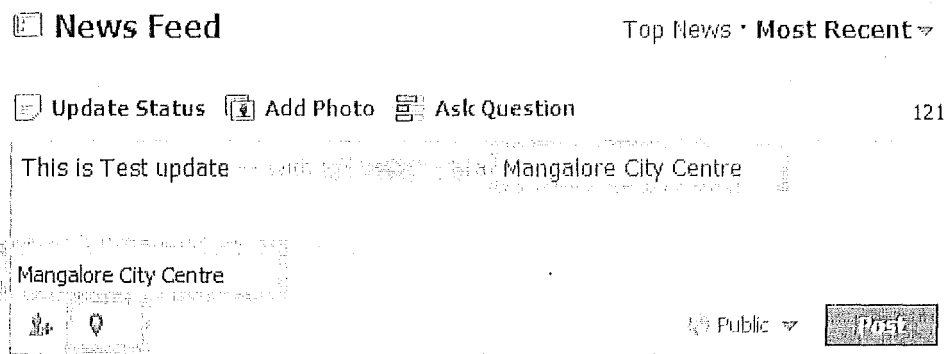


Figure 4.9: Example of Geo-Location Sharing with Friend Tag (Blair, 2011)

It can also lead other people, who a user just added to their list of friends and who are unknown to the user, to track and associate their activities with the friends they spend time with in the real world.

User Likes

For the category of Likes, an overwhelming majority, 65% ($n = 231$ users) have general entertainment as their Likes. This includes television shows, movies, music and books. Considering the demographics of users who make up the majority of this study (young female users between the ages of 18 and 25), it is quite clear what their main interests are (see Figure 4.2). Celebrity personalities are at 14%, this might be due to the fact that most users follow famous personalities through the official Facebook pages of their favourite TV shows, books or

music. This differs from other social networks (for example Twitter) where these celebrities are more active and are followed by thousands of users. Only 15% ($n = 53$) made up the next significant number, which was an interest in sports. Religious ($n = 13$ or 3%) and Game ($n = 10$ or 3%) pages had very low interest levels from the users. This can all be seen in the figure below:

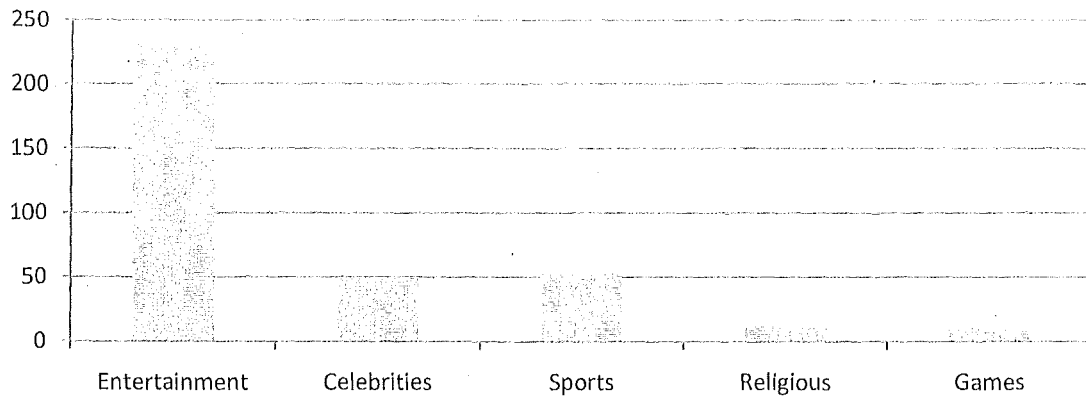


Figure 4.10: Majority of User Likes

The privacy implications of being able to track a user's Likes is that they can be profiled easily by online marketers whose job it is to segment markets in order to mass advertise to them (Cheung, Chan and Limayem, 2005:9). These companies try to solicit a user's personal information as well. It also makes it easier to track users in cyberspace as well as in the real world. For example, a user who states that he likes a certain football team will post that they are attending a game which can be traced to a specific location in the city (Cheung et.al., 2005:9).

Method of Access

According to the findings, 57% ($n = 205$) of users access Facebook from desktop computers and 43% ($n = 152$) use mobile devices (smart-phones or tablets) to access Facebook (Figure 4.11). This could be because Internet access is now more affordable, which makes it easier for users to get online more frequently and contact other users. The current generation of users prefer to log onto Facebook and 'inbox' (send messages to) each other in order to communicate with the added advantage of being able to share media such as photographs, audio and video (Pempek et.al., 2009:232)..

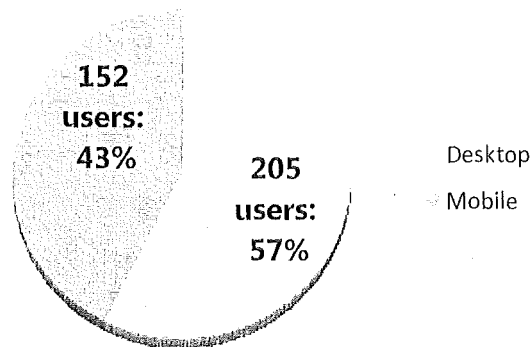


Figure 4.11: Method of Access

This could also explain why their geo-location is automatically updated and loaded onto Facebook as meta-data (Clookey, 2013). Most smart-phone operating systems now incorporate GPS software that allows smart-phone owners to share their location with applications like Facebook Messenger (Clookey, 2013). While these applications inform users that this is how they work, most users may not be aware of how this makes them vulnerable. If users go online and post a comment or upload a picture, their location immediately becomes a part of that post or upload (Clookey, 2013). If the users simply feel like checking in (a term Facebook uses for those who wish to simply state where they are) then they can do so and that is seen by other users as a post (see figure 4.9).

The sharing of geo-location (Figure 4.7) makes users vulnerable as they can be tracked. A log of an individual's movements and activities can be created by a potential attacker who will begin to see patterns in the user's activities and who can then easily determine when the user is at their place of residence or not (Blair, 2011).

4.4 User Activities

The data in Figure 4.12, indicates that 56% ($n = 202$) of the users post daily on Facebook, while 38% ($n = 135$) post at least once or twice a week. This number confirms Facebook's popularity among young users (Facebook, 2012). It also shows that a good number of users access Facebook with their mobile devices which one can assume they make use of everyday, thus allowing them to check in a few times a day on their profiles. Only 6% ($n = 20$) post monthly.

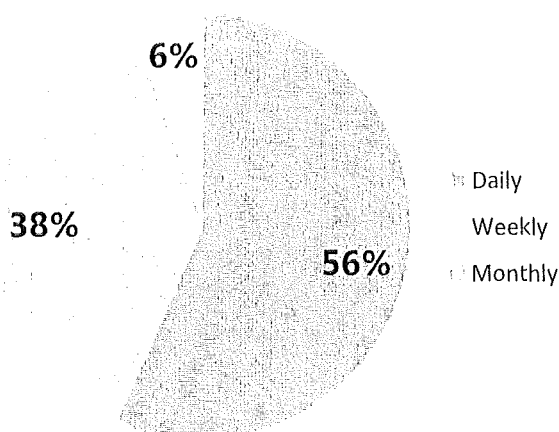


Figure 4.12: Frequency of User Activity

This particular group of users is always connected to their peers as the data indicates that an overwhelming amount check in on Facebook to post, upload or comment on something on Facebook. When personal information is generated daily and at this rate, it makes it a lot easier for those who want to track and profile users, particularly if users are constantly sharing their location and uploading pictures of themselves (Blair, 2011).

Event Sharing

Findings from the study show that 64% ($n = 230$) of users hardly ever post events they attend on Facebook. This is interesting considering that they are willing to share their location readily with their friends (see figure 4.7). Their apprehension may be due to them self-censoring and not wanting every detail of their personal lives to be known. About 22% ($n = 77$) and 14% ($n = 50$) do actually mention that they will be attending a specific function ahead of time and then go on in detail about when it will be held and who else will be in attendance.

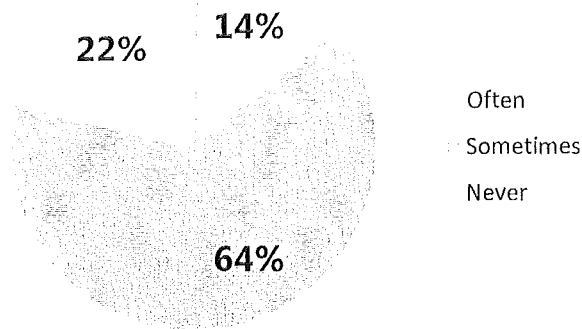


Figure 4.13: Sharing of Events

These functions include weddings, concerts and theatrical performances. The risk users face when they share information about events they are attending is that they become vulnerable to those who might be tracking their activities and look for information of this nature (Clooche, 2013). If users post images of themselves at an event standing in front of their vehicle which has registration plates in clear view, they have exposed themselves. They could be standing by their place of residence with their house number in the background, this as an example of exposing security data (Blair, 2011).

Majority of User Activity

For the sample, the major activity (47%) on Facebook is posting statuses (Table 4.1). This includes statements from the user, jokes and opinions. This is followed by users commenting on other users' posts (20%) and Liking different pages on Facebook (19%).

The pages fall under the categories explained earlier (entertainment, celebrities, sports or religious pages).

Finally, uploading pictures onto Facebook is the last activity (14%). These pictures tend to be personal in nature and often times of the users themselves, but in some cases the photos are of products the users like, such as a brand of designer apparel and shoes. An ethical issue that tends to come up is whether to post a picture of another user without their permission. These pictures can be digitally altered using Photoshop to depict that user in a negative light (a form of cyber-bullying or propaganda in the case of a public figure) (Hoadley, 2010:3). This can leave

undesirable impressions on those who view these pictures on Facebook. This vulnerability can be countered by the user un-tagging him-/herself in that image, but the damage to their reputation will be done as it may take time for the user to realise they are tagged in an offensive image (Hoadley, 2010:3).

Activity	Frequency
<i>Posting</i>	169 (47%)
<i>Commenting</i>	70 (20%)
<i>Liking</i>	68 (19%)
<i>Uploading</i>	50 (14%)

Table 4.1: Frequency of user activity

User activities mostly comprise posting comments on Facebook. This generation believes in communicating and expressing itself using various electronic mediums. It is definitely cheaper for them to communicate with each other and canvass their peer groups for opinions about what interests them. Users who are on social media every day (see figure 4.12 where 56% of users are on Facebook everyday) are generally willing to share information about their location (see figure 4.7), events they are attending (see figure 4.13) as well as photographs of themselves or their interests (see figure 4.10). Anyone with Facebook access from the outside can analyse these usage patterns and profile the user.

Frequency of User Tagging

Figure 4.14 shows the frequency with which users are tagged in photographs that are uploaded onto Facebook.

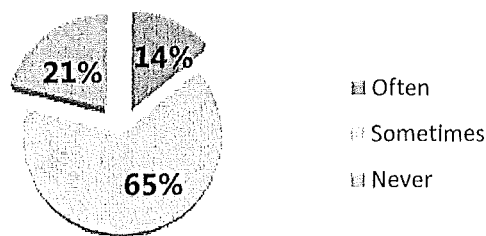


Figure 4.14: Frequency of User Tagging in Photographs

About 65% ($n = 233$) are sometimes tagged by other users in different photographs while 14% ($n = 49$) are often tagged by friends. Most users enjoy sharing their photos with their friends and select specific individuals to view their pictures in their News Feed or wall posts when they log onto Facebook. The challenge with being tagged is that users can be tagged in some offensive material that might be racist, xenophobic or graphic in nature. These images are then seen by all their friends as fresh updates on their News Feed. This is an undesirable outcome of being tagged. Fortunately, Facebook allows users to un-tag themselves from such images if they wish to do so.

The last significant figure here is the 21% ($n = 75$) of users who are never tagged in photos. It could be that these users simply remove these tags themselves to ensure that any pictures that they deem unsavoury are not associated with them.

4.5 Third-Party Content

Program Usage

According to the data, 20% ($n = 71$) use Facebook-related programs such as ‘Who’s viewed your profile?’ and 20% ($n = 60$) use social programs like ‘Meet your Mate!’ Only 16% ($n = 59$) play online games on Facebook (Figure 4.15). These programs are Liked and utilised as they are supposedly endorsed by the site. However, the truth is that these programs are from third party vendors and the way they work is not necessarily regulated by Facebook (Mansfield-Devine, 2008:4). These programs often need access to a user’s profile, this means that they access the user’s personal information in order for them to function. If these programs contain malicious software like worms then the user’s profile will be infected (Mansfield-Devine, 2008:4).

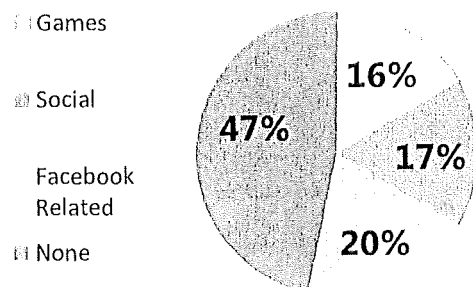


Figure 4.15: Programs used on Facebook

It is questionable whether users are aware of the fact that these programs are not programs produced or endorsed by Facebook. The developers of these programs and where they are hosted are clearly also not known by users (Mansfield-Devine, 2008:4). It may be that the developers are not malicious but that the quality of the coding behind the programs will leave users vulnerable to sniffers who may steal the data from these programs (Mansfield-Devine, 2008:4). Users give permission to these programs before thinking about the implications of their actions. 47% ($n = 167$) of users do not utilise the programs available on Facebook. A lack of interest in these applications or a general inability to use them may be the reason behind this high figure.

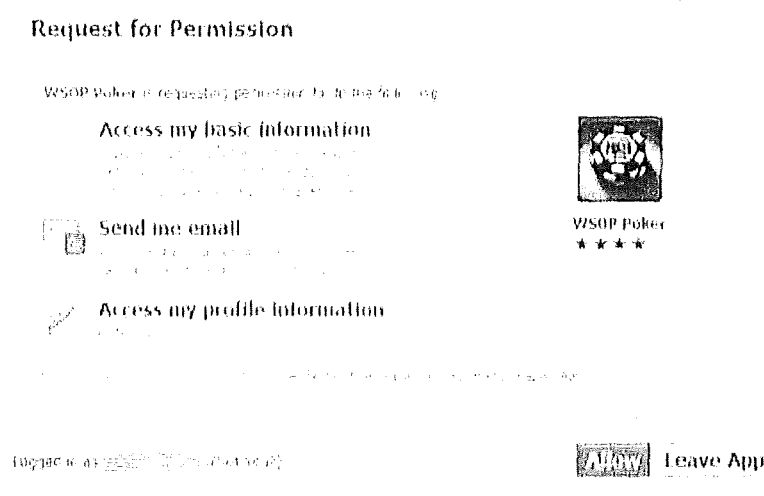


Figure 4.16: Facebook Program asking for Permissions (Mansfield-Devine, 2008).

From the figure above it is clear that these programs by nature invade the privacy of a user's personal information by requesting access to it. The programs even send emails (spam) to the mail box of the user to try and promote other related products that the parent company may be offering (Mansfield-Devine, 2008:4).

Frequency of Program Usage

Figure 4.17 shows the frequency of usage of these programs. Only 41% use these programs frequently or some of the time. 59% ($n = 211$ users) still do not make use of these applications on Facebook.

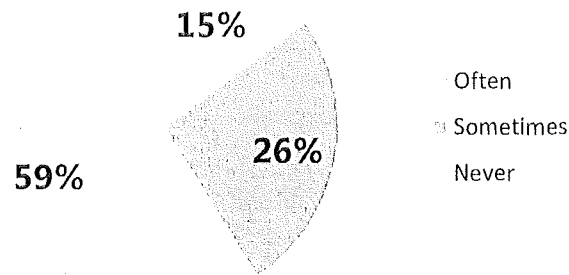


Figure 4.17: Frequency of Program Usage

It could be that the programs are not merging with their main interest areas or are complex to utilise. The relevance of this data is that it affects a user's privacy as these Facebook programs often post on a user's profile page (and thus their friends' News Feed) using the user's name. These programs advertise themselves and affiliated products, thus promoting themselves, oftentimes without the user being aware of what is happening (Mansfield-Devine, 2008:5). This is another example of how technology goes beyond the scope of what some users may think it does.

Program Posting

Figure 4.18 shows that 93% ($n = 334$) of users do not have programs assuming their identity and posting on their behalf. 6% ($n = 20$), however, do experience this and 1% ($n = 3$) often have their identities used without their permission. Quite frequently these programs post links to websites that spread dangerous malware, which can easily be posted to user profile pages and as soon as the user clicks on the link, they have infected their personal computer or work computer (Mansfield-Devine, 2008:5).

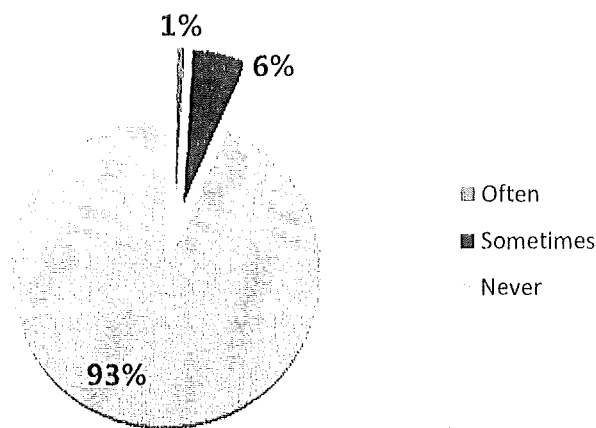


Figure 4.18: Program Posting

Posting has often taken on malicious forms in the past, e.g. as worms on the Internet. These worms, dubbed Koobface.A and Koobface.B, once attacked Facebook (Mansfield-Devine, 2008:5). A user on the site with an infected machine often found that they were posting messages to their friends, which encouraged them to visit sites where they would become infected as well. These attacks were only so effective due to the trust generated by the social network.

Fortunately, though 93% of users in the population do not use these programs which may assume their identity and post on their behalf, they seem not to be interested in these. That, however, does not mean they do not actively promote products that they like or have an attachment to. They play the role of brand ambassadors as they advocate for others to purchase these or Like them indirectly.

Product Recommendations

Interestingly, 41% of users on Facebook ($n = 145$) recommend a brand or product in a number of ways. Some post direct references to their favourite brand, while others upload pictures theirs. Additionally, other users have it on their Likes page, which is prominently displayed on the new Timeline Profile that Facebook rolled out for every user during the middle of 2012 (Facebook, 2012). Only 19% ($n = 68$) often make references to products while 40% ($n = 144$) never promote anything on their profiles (Figure 4.19).

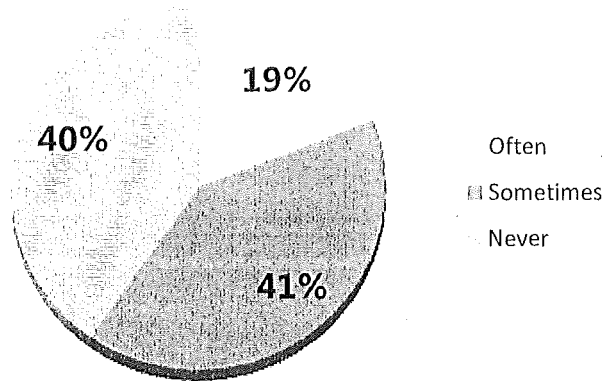


Figure 4.19: Recommending Products

Users recommending brand products on social media is an incentive for online marketers to get the user to become a brand advocate (Mansfield-Devine, 2008:7). This means that if an online marketer can profile a target user based on of his/her Likes and personal details, then they can be targeted for mass advertising by these marketers (Mansfield-Devine, 2008:7).. Privacy can be violated in the form of the user being overwhelmed by unwanted spam mail in the form of digital adverts for products that they do not want to buy or recommendations from their friends to buy these products.

4.6 False-Call

Most calls fail to ensure that each and every detail is correct and this was the case with this call. The name of the user was slightly modified as well as the interests so that the original profile and this one were not completely similar. The idea behind this was that, hopefully, the friends of this user would pick up on this and reject any friend requests or any communication from the experimental profile. The best case scenario would involve them alerting the user or Facebook about this experimental profile that is claiming another individual's online identity.

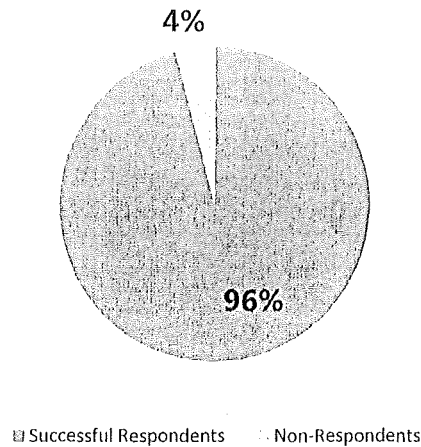


Figure 4.20: Response Rate

Out of a population of 237 individuals, 10 (4%) could not be added as friends due to them blocking any new friend requests (Figure 4.20).

Within 7 days, the profile managed to attract 32% ($n = 76$) who responded to this experiment. The low response rate may have been due to a number of individuals not checking their Facebook profiles every day and would certainly increase if more time was allocated to this online impersonation. The number, though, is sufficient for the fake profile to have more credibility and solicit more connections. After a period of 30 days the experiment managed to attract a further 33% ($n = 78$) in total.

Days	Number of Respondents	Response Rate
0 - 10	76	32%
10 - 20	83	35%
20 - 30	78	33%

Table 4.2: Time Response

The people who did respond did not check the personal details thoroughly to assess whether this was a true profile account or not. Even though the profile name was modified, it was taken as a common practice that takes place on Facebook as many individuals misspell their names purposely on social media. This occurs sometimes out of fun or to hide themselves from people they do not want to find them.

With these new friends and some patience, the experimental profile could assume this identity and with the access to individuals on the Internet, try to scam them into doing something illegal. This attack proved that most users lack the habit of verification before they take a course of action on social media. It is quite simple to impersonate another user on Facebook.

4.7 Survey

The survey consisted of a couple of questions focusing on the privacy awareness of the users about privacy legislation, what they believe and feel about Facebook’s privacy policy and the features of Facebook they would like to see improved.

Privacy Legislation

The study surveyed 70 respondents who participated in an online survey. Figure 4.21 shows that 57 of them (81%) agreed that they did not know there was any legislation in place to towards privacy. They simply believed that they were communicating online with no need to have their privacy advocated for in the law. Only 19% (13) were aware of some data protection laws but were unsure if they were also applicable to Facebook and other social media.

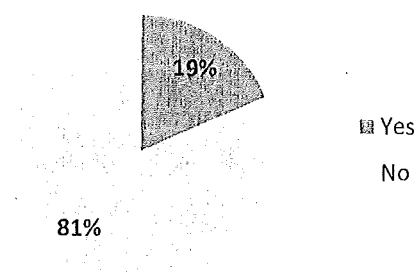


Figure 4.21: Privacy Legislation Awareness

Facebook Privacy Policy

The findings of the survey also showed that a good majority of the users did not implement privacy controls that Facebook provides. Figure 4.22 shows that 61 (88%) agreed that they have never used privacy tools on the site. Only 12% (9) have actually used those controls in order to prevent any privacy loss. It could be that these don’t believe their data to be worth keeping safe or they simply do not know how to implement the controls due to never having read nor understood the Facebook privacy policy. The results show to what extent are users exposed.

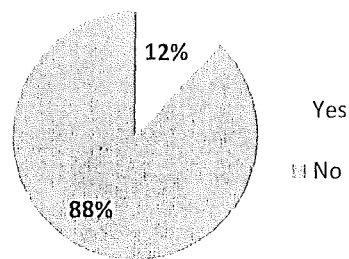


Figure 4.22: Use of Privacy Tools

Improvements

When asked which feature they believed would benefit the most from improvement on Facebook, users stated that they would like to see their News Feed improve. 60 users (Figure 4.23) would like to control more of what they see from other users as well as what other users see from them via the News Feed feature on Facebook. 20 would improve the way users can be tagged on unsavoury material on Facebook while only 7 were concerned with location sharing needing to be changed on Facebook.

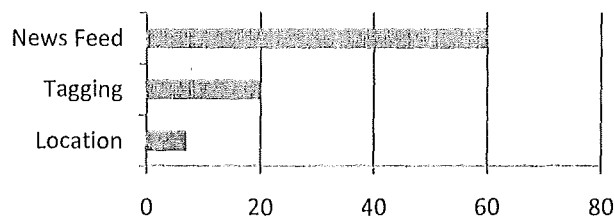


Figure 4.23: Facebook Improvements

4.8 Summary of Results

Highlights from the findings show that users post enough information on their profiles, which can be used to track their movements, location and activities. The majority of users believe that information posted on their Facebook profiles is not viewable by anyone outside of their social circle on Facebook. This study has proven that there is more than enough information available in the public domain about a user to create a profile about them and track their online habits.

In order to reap the benefits offered by Facebook, users have to trade in their privacy to become part of the online communities that exist on this site. Users need to be made aware of the large amount of personal data that is collected on Facebook and what it is subsequently used for. Users

tend to have a false sense of security as they use Facebook to post information without thinking about the implications of what they are doing. Facebook is user-friendly and available on mobile devices and this makes it easier to post things online that may be potentially harmful.

4.9 Conclusion

The purpose of this chapter was to present the results obtained in this study in a clear and logical manner. Accompanying the results are incisive interpretations of each of the results to make them meaningful. The results were organised logically in order to facilitate analysis and a brief discussion was offered to enhance the understanding of the context of the issues affecting privacy on social networks. From the data it is clear that most users believe the Internet to be a safe space for them to engage in all kinds of activities (such as uploading personal photographs). This, however, is not the case as the Internet has individuals who seek out personal information for their own gain. The false spoof attack showed this as a great number of friends responded to a false profile without questioning its authenticity or investigating further. This casual attitude towards online privacy is what has led to the difficulties experienced by those who are targeted. Most users are unaware of the settings that exist on these sites to help protect their privacy.

CHAPTER FIVE

CONCLUSION

5.1 Introduction

This chapter concludes the study by providing a brief overview of the study. Findings from the polling checklist were presented and discussed in the previous chapter enabling pertinent conclusions to be drawn. Thus, this chapter seeks to reflect incisive conclusions and recommendations in the context of online privacy in social media.

5.2 Summary

The purpose of this research has been to assess the online behaviour of users and their privacy when using the popular social networking site Facebook. The study focused on students based at the Mafikeng Campus of the North-West University. Social media has given the world a new and more efficient means of connectivity and has enabled people across the world to stay in touch and reach out to new people. The new technology has, however, led to a new threat to privacy because the availability of personal information online can result in it being used in negative ways. For example, when the data is online it can be used by third parties (most often online advertising firms) for various purposes for which it was not originally intended. Another example is that a social engineer can use the information for malevolent purposes.

The study made use of a mixed-method approach to assist in the investigation. It allowed for data to be collected from users who have their personal information open to be accessed by the public on Facebook, as well as the researcher's social circle and students on campus.. The population sample for the polling checklist was 357 students sampled conveniently because they Liked the university's official Facebook page. The population sample for the false call was 237 participants, the total number of the researcher's circle. The sample for the short survey was 70 participants from those who were willing to be part of the survey. Once data were collected, analysis was done using descriptive statistics and standard coding procedures. Data was presented via tabulation and illustrations such as pie charts and bar graphs. Some findings confirmed what exists in literature already about online privacy, but some new interesting facts (such as smart-phones automatically posting geo-locations) were revealed.

Below are some broad conclusions that were drawn from the study:

Personalised Services

It is highlighted in the study (see chapter 4, figure 4.11, method of access) that mobile access to social networks enables even more personal information to be made available. This information includes users' geo-locations (see chapter 4, figure 4.7, geo-location sharing) as well as the fact that they are accessing Facebook through a Blackberry device, Android or Windows Mobile tablet. This meta-data accompanies the posts, comments and uploads those users generate when they are online, increasing their digital footprint (Clooke, 2013). The personal information, which can be in the form of geo-location, is then used by Facebook – an advertising business, to make sure adverts that are shown to a particular user are location specific and relevant to their Likes. Criminal opportunists can harm users by gaining access to a user's residential address or noting where they will be on a specific day and at a specific time (Blair, 2011). Facebook utilises this data to create more personalised adverts with the aim of generating more revenue for the clients advertising through them. It is unlikely that users are aware that this is how all their information is used or that it is accessible to other people who have their own agendas (Clooke, 2013). Social networks should not trade user privacy for personalised service as a lack of trust from the users' side can damage the goodwill and reputation of these sites.

Privacy

The study reveals (see chapter 4, figure 4.5, availability of users' details) that users' privacy is only partially protected by default when users have created an online social networking account. Most users' data are partially available on their profiles (67%, see chapter 4, figure 4.5). This can lead to any number of information leakages occurring. Anyone masquerading as one of the users' friends can get a hold of sensitive data by logging on and searching for this data (Blair, 2011). Consumers have less privacy protection on the Internet and this has a great influence on the way these sites should be run. Based on these findings, privacy awareness may be achieved through training and an increase of the knowledge on how to fully utilise privacy settings on social media. Users must be taught the different ways to secure their personal information.

This lack of safety was highlighted in the study "Privacy as information access and illusory control" (Hoadley et.al., 2010:3). The researchers noted that service providers needed to develop privacy enhancing features that are easy to use for average users. This study has found (see

chapter 4, figure 4.22, use of privacy tools) this to still be a challenge as most users are not sealing their data from outside viewing by anonymous people on Facebook. This could be because for average users the implications of sharing personal information online still seems to be low risk, therefore they are not moved to change their online behaviour.

Privacy Policy

Another conclusion is that the Facebook policy is lengthy and it is likely that most users have never looked at the policy (see chapter 4, figure 4.21, privacy legislation awareness) due to it being long and a bit time consuming to go through (Simplicity, 2012:2). It is not user-friendly to people who are not technology literate or knowledgeable about security policies. From the findings of the survey (see chapter 4, figure 4.22, use of privacy controls), it was clear that users are not fully implementing privacy controls on Facebook (88% had never used the tools available on Facebook) which could be due to them not understanding the policy. If users don't understand these components of a privacy policy, how could users even begin to execute the remaining, and possibly most important, portion of the policy—managing privacy (Simplicity, 2012:3)? The technical jargon contained in the policy is because it is written by lawyers and computer engineers and as a result it is difficult to understand. The policy though, does cover the basic demands that users have concerning their privacy. What good is a policy that most users are unable to understand though, and how can users challenge the service provider to change their policy when they are unaware of what is contained in it?

Profiling

Most users are female between the ages of 18 and 25 (see chapter 4, figure 4.1, user gender and figure 4.2, age groups). As such, their general Likes include entertainment and celebrities (see chapter 4, figure 4.10, majority of user likes). A fair number of them (43%) access social networks through their mobile devices giving them the ability to stay in touch and communicate on a daily basis (see chapter 4, figure 4.11, method of access).

Most (93%) users do not have programs that assume their identity and post on their profile, which then features on the News Feed of others (see chapter 4, figure 4.18, program posting). They seem not to be interested in these. That however, does not mean they do not actively promote products they like or have an attachment to. They often advocate for others to purchase these or Like them indirectly (see chapter 4, figure 4.19, recommending products). The

personalised nature of the subtle marketing done on Facebook makes users play the role of brand ambassadors and they therefore market a company's products for them (Smith, 2004:213).

Legal Issues

Users are not aware of their privacy rights. This was established through the survey which sought to uncover user knowledge of various laws protecting their privacy (see chapter 4, figure 4.21, privacy legislation awareness). The majority, 81% were not aware of any laws in place to protect their privacy. With the movement towards cloud computing gathering momentum it is now feasible to say that most organisations will use data warehouses to store their data as well as individuals as the cost of storage decreases (Information Security Group of Africa, 2011: 20). It may be at this point when enough people are on these platforms that governments around the world will begin to create legislation governing these new privacy aspects.

South Africa has been in the process of developing suitable security laws such as the Protection of Personal Information for nearly a decade now. This was necessary to keep up with the pace of technology and e-commerce (Information Security Group of Africa, 2011:18). There has been a need for separate and more adequate legislation on data protection. It however is not clear about data that is produced on social media sites.

There is as yet no current research on the effectiveness of this new Protection of Personal Information act, here in South Africa. News stories reporting on the application of privacy laws across the world are widely available online. For example Google was fined 150,000 Euros in France as they violated privacy laws and did not inform people what they were doing with user data (Bodoni, 2014). This shows that it is possible to fine an international internet company for violating user privacy as long as specific clauses that punish violations exist within legislation.

User Trust

Facebook users often operate at a level of trust and not a level of security. The false call (see chapter 4, figure 4.20, response rate) proved that if an attacker can successfully duplicate another user account, they can have full access to their social circle and thus the personal information of the contact list. The vast majority (96%) of users targeted responded within a 30 day period (see chapter 4, table 4.2, response rate). None of the respondents sought to verify the authenticity of the account or even compare it with the original and thus raise suspicion of it being a duplicate account.

5.3 Recommendations

Based on the findings of the study the following recommendations are suggested to enable social networks to be safer and users to be secure when operating online.

5.3.1 Privacy Legislation

An effective way to combat privacy violations should be the introduction of legislation by governments or Internet governing bodies to ensure that user privacy is not subject to violation. It is important to understand that organisations have certain obligations when processing personal information and individuals have certain rights. These may be established in laws, regulations and organisational policies. The value of privacy legislation will also become evident in its application.

Governments will need to take care to ensure that the laws governing privacy do not become irrelevant. As these laws apply to a dynamic technology, they will need constant updating as people's attitude towards personal privacy evolves along with the technology. These laws will need the following components to make them effective:

- Specificity

The development of specific laws dealing with this aspect of online privacy is necessary. As this technology continues to integrate people's daily lives, the opportunity for privacy to be violated becomes an ever increasing risk. Privacy violations will be dealt with through existing legal structures. As it stands, privacy violations are not punishable using legal instruments and this should not be the case. The only punishment that a company can face is the loss of goodwill. The introduction of privacy legislation will be a timely addition to the fight against these violations. Advocates and users should be willing to engage and discuss policy matters that will ensure that user privacy is not subject to violation. Subsequent punishments and deterrents should be devised to protect user rights.

- Enforceable

There will be a need for laws that are enforceable when it comes to international Internet companies. The biggest challenge will be creating a jurisdiction for cases of privacy violations to be investigated. Claims that are made against privacy violators should be supported by the highest law institutions across the world. It would not be out of the

question to suggest that the International Criminal Court (ICC) should have a smaller division that looks after cyber security under which a social network taskforce can be established. It is becoming clearer that cyber crime needs an active response from our institutions that have the means to correct these violations.

5.3.2 User Awareness

As mentioned before, a shared model for privacy protection would include users showing more awareness about responsible online behaviour. Users should regulate their own behaviour by employing safe practices such as having their profiles completely locked from being viewed by non-friends. Also, they should not accept friend requests from people who they do not know or who seem suspicious.

5.3.3 Service Provider Changes

The truly most efficient mechanism for ensuring that the law is observed is for service providers, such as Facebook, to be a self-regulating social network and to create robust enough privacy policies that are not only comprehensive, but easy enough to understand for all types of users, like the ones social networks often attract. If service providers want to create greater trust between them and the users, then they should try to enforce a standard set of safety policies that are beneficial to their user base. Firstly, the privacy policy should be simpler and be required reading before any one signs up for Facebook. Profiles should by default be locked as it is

presumptuous to assume that users can do this for themselves. Some people on these networks may not be savvy enough in terms of computers and therefore they fail to protect themselves.

The privacy policy needs to be updated more frequently to reflect the dynamic nature of this type of technology and the challenges it creates. These measures should be based on empirical researches on privacy, which can inform service providers about how to protect privacy.

Facebook also needs to be actively involved in vetting the types of applications that are allowed to run on Facebook. It may be a risk to their user base for them to allow most developers to simply upload their programs on Facebook without first evaluating how they work. Programs need to be tested to ensure that they do not contain vulnerabilities that may expose users to unwanted social engineering.

5.3.4 Change of Business Model

The fault may lie in the current business model that has been employed by the social network as it seeks to monetise the services it provides to users. Any reputable business understands that having goodwill between them and their customers will enable the business to achieve its objectives of steady growth and profitability. There are already signs that users are migrating away from having Facebook as their primary social network provider. While the site still enjoys new users being added to it every day, those who have been on Facebook for a period of time are now making use of Google+ and other social networks that have ethical values driving their business model. A different business model would see users paying for varying levels of privacy offered by the social networking site to protect their data in legally binding contracts enforceable in a court of law. In this way the contract between the service provider and user is protected by the laws of the country and are recognised by a court of law. It will also allow the site to raise the revenue they desire for their shareholders. Of course, the challenge of creating a means for policing the contracts obtained will arise. This, however, can be achieved by creating new and separate laws regarding the contracts between social sites and users. This solution may seem cumbersome, but it will ultimately ensure that there is someone who is responsible for any violation that takes place.

5.3.5 Orient new users

New members to social networking sites should be oriented by the service provider with regard to how to manage their privacy settings. Currently, users are only guided in terms of how to look for new friends or upload pictures. There needs to be a long term commitment to privacy and security from these sites. The new users should be taught how to navigate the basic privacy settings to ensure that they can perform activities such as locking their account, creating different lists of friends by sorting them from close friends, acquaintances and colleagues as well as how to un-tag themselves from photographs which they were tagged in without their permission.

5.3.6 Training Programmes

Colleges and schools can have active programmes that inform young people of the dangers of irresponsible behaviour on social media and to watch out for the negative elements it attracts. It is important also that elderly users be trained as well as they tend to lag behind in terms of the latest trends affecting users on social media. Rural users must also be considered as the

proliferation of the Internet envelopes rural and peri-urban areas. As such, it is imperative that these programmes be made user-friendly, informative and empower participants with skills to allow them to navigate the complex tools that Internet sites such as Facebook employ to ensure privacy.

These programs can be run and sponsored by local educational institutions with the financial backing of the appropriate government departments. The government should be seen as involved in relevant matters affecting citizens by sponsoring short workshops in cyber crime and privacy protection.

5.3.7 Online Security and Privacy Information Resource Centres

Websites that teach users how to protect their own privacy when they are online would be exceptional in protecting user privacy. These sites can provide 24 hour information resources for people to consult at their own convenience and pace. They can be manned by trained security consultants who can answer questions from users who need to know how to handle a specific privacy matter. These sites will act as online repositories that users can refer to whenever they are in doubt. Newsletters from the site can be emailed every 2 weeks or monthly to update people on their mailing list about current trends affecting privacy.

5.3.8 Privacy-Enhancing Technologies

A broad investigating into current privacy-enhancing technologies that can be employed to protect users' privacy can be done to come up with creative solutions to these violations of personal information. Software tools can be used to provide a pseudonym proxy for logging on to a site, giving users consistent access to registration based systems without revealing personal data. A technology that can disguise a user's IP address and supply a dynamic IP address each time it is required, would be exceptional. One such solution may be found in web anonymisers which provide the ability to sanitize packet headers passed from the client to the server or web filters. The disadvantage of such software would be the loss of access to all personalised services, including those from trustworthy sites.

5.4 Conclusion

This chapter provides conclusions based on the findings of the research. The conclusions encompassed all the main points of the research. From these, relevant guidelines were suggested

to solve the challenges facing users. As technology continues to evolve as new features are added, such as geo-tagging and face-recognition, it needs to be revised periodically to ensure that it covers any new ways through which privacy can be violated. Self-regulation, legislation, training and technological applications can be used to accomplish this. The best solution will be to combine these guidelines to create a holistic approach towards privacy that will better serve the Internet community in the future. The digital symbiosis of each of these guidelines will empower the user and hold the service provider accountable (something which is not currently taking place).

The relationship between privacy and security continues to be an evolving one. How much users will need to give up in order to be part in the new digital age will depend on how the various stakeholders of these sites react to the current losses in privacy. These companies will be expected to safeguard data and prevent their systems from being hacked into.

As future studies in this area will seek to widen our understanding of privacy, it will be important to factor in the new changes that will affect those generations when it comes to new technologies. One prediction of networking in the future will see the combination of mobile, location services and social networks coming together to provide even more personalised services for users. Users will receive automatic updates on their phones concerning the availability of a product they Liked on Facebook. This update will inform the user of where they can buy the product (based on their location which they willingly provided on Facebook). The invasiveness of this technology will continue to be a challenge.

LIST OF REFERENCES

Acts *see* SOUTH AFRICA.

BAKER, J. 1991. *Personal Information and Privacy*. Proceedings of the First Conference on Computers, Freedom, and Privacy. Los Alamitos, CA: IEEE Computer Society Press.

BALDUZZI, M., PLATZER, C., HOLZ, T., KIRDA, E., BALZAROTTI, D. & KRUEGEL, C. 2010. Abusing Social Networks for Automated User Profiling. *Vol. 6307 of Lecture Notes in Computer Science*. Springer. p. 7-9.

BAUMER, D.B., EARP, J.B., & POINDEXTER, J.C. 2004. Internet Privacy Law: A Comparison between the United States and the European Union. *Computer Security*, (23):400-412.

BLAIR, K. 2011. New Survey: Burglars Use Social Media to Plan Crimes.

http://socialtimes.com/new-survery-burglars-use-social-media-to-plan-crimes_b79475

Date of Access: 18 June 2012

BODONI, S. 2014. Google fined maximum French penalty for privacy violations.

<http://www.bloomberg.com/news/2014-01-08/google-fined-maximum-french-penalty-for-privacy-violations.html> Date of Access: 30 Jan 2014

CHEUNG, C.M.K., CHAN, G.W.W. & LIMAYEM, M. 2005. A Critical Review of Online Consumer Behaviour: Empirical Research. *Journal of Electronic Commerce in Organizations*, 3(4):1-19.

CLOOKE, R. 2013. Facing the Risks of Location Sharing.

<http://www.mobilesecurity.com/articles/526-facing-the-risks-of-location-sharing#sthash.gO0eDEGi.dpuf> Date of Access 2 November 2013

COHEN, L. MANION, L. & MORRISON, K. 2007. Research methods in education. London: Routledge.

CONGER, S. 2005. *Emerging Technologies, Emerging Privacy Issues*. Dallas: University of Dallas.

- DAVISON, R.M. 1998. An Action Research Perspective of Group Support Systems. University of Hong Kong. Hong Kong.
- EMERY D. 2010. Details of 100 m Facebook Users Collected. BBC News Online.
<http://www.bbc.co.uk/news/technology-10796584> Date of Access: 5 Aug 2012.
- FURNELL, S.M. 2010. *Online Identity: Giving it all away?* Information Security Technical Report. Place of Publication: Plymouth.
- GAGE, N.L. 1989. The paradigm wars and their aftermath: A “historical” sketch of research on teaching since 1989. *Educational Researcher*, 18 (7), 4-10.
- GARTRELL, M., HAN, R., & BEACH, A. 2008. Solutions to Security and Privacy Issues in Mobile Social Networking. Colorado: University of Colorado.
- GRIMMELMANN, J. 2009. Saving Facebook. *Iowa Law Review*, (94):1197.
- GUNATILAKA, D. 2007. A Survey of Privacy and Security Issues in Social Networks.
<http://www.cse.wustl.edu> Date of Access: 25 Aug 2012.
- HESSE-BIBER, S. N. 2010. Mixed methods research: merging theory with practice. New York: Guilford.
- HOADLEY, C., XU, H., LEE, J. & ROSSON, M. 2010. Privacy as information access and illusory control: the case of the Facebook news feed privacy outcry. *Journal of Electronic Commerce Research and Applications*, 13(9):3.
- INFOGRAPHIC LABS. 2012. *Social Media Statistics for 2012*.
<http://www.digitalbuzzblog.com/social-media-statistics-stats-2012-infographic.htm>
 Date of Access: 31 Aug 2012.
- INFORMATION SECURITY GROUP OF AFRICA. 2011. *Revealing Privacy in South Africa: What You Need to Know*. Pretoria: Information Security Group of Africa.
- JONKER, J. & PENNINK, B. 2010. The Essence of Research Methodology: A Concise Guide for Master and PhD Students in Management Science. Heidelberg, Springer.
- JOSS, M. 2001. *Do you need a CPO?*
<http://www.computeruser.com/articles/2006.1.2.0601.01.htm> Date of Access: 1 Sep 2012.

- KATZNELSON, Y. 2006. A (brief) Introduction to Inferential Statistics. University of California. Santa Cruz.
- KOTHARI, C. 2004. Research Methodology: Methods & Techniques. New Delhi: New Age International.
- KREJCIE, R.V. & MORGAN, D.W. 1970. Determining Sample Size for Research Activities. *Journal of Educational and Psychological Measurement*, 30(608):56.
- KRUCK, S.E., GOTTOVI, D., MOGHADAMI, F., BROOM, R. & FORCHT, K.A. 2002. Protecting Personal Privacy on the Internet. *Information Management & Security*, 10(2):6.
- MACK, L. 2010. The philosophical underpinnings of educational research. *Polyglossia*, 19, 5-11.
- MANSFIELD-DEVINE, S. 2008. Anti-Social Networking: Exploiting the Trusting Environment of Web 2.0. *Journal of Network Security*, 23(5):4-7.
- MCEWEN, J. 2006. *Connecting Privacy and Security Efforts in the Incident Response Process*. Bedford, MA: MITRE Corporation.
- MILES, M.B. & HUBERMAN, A. M. 1994. *Qualitative Data Analysis: An Expanded Sourcebook*. 2nd ed. Thousand Oaks: Sage.
- MISHRA, A. & MISHRA, D. 2008. *Web Privacy: Issues, Legislations and Technological Challenges*. Hershey, PA: IGI Global.
- MUNRO, B. H. 2005. Statistical methods for health care research. (1)1. Lippincott Williams & Wilkins.
- PEMPEK, T., YERMOLAYEVA, Y. & CALVERT, S. 2009. College Students' Social Networking Experiences on Facebook. *Journal of Applied Developmental Psychology*, 30(12):227-238.
- SCHOEMANN, F. 1984. *Philosophical Dimensions of Privacy: An Anthology*. New York: Cambridge University Press.
- SHANKS, G. G., & PARR, A. N. 2003. Positivist single case study research in information systems: a critical analysis. *ECIS*, 5(25):1760-1774.

- SIMPLICITYLAB. (2012). Knowing more about privacy makes users share less with Facebook and Google. Siegel+Gale; New York.
- SMITH, H. 2004. Information Privacy and its Management. *MIS Quarterly Executive*, 3(4):201-213.
- SINGH, Y.K. 2006. Fundamentals of Research Methodology and Statistics. New Age International; New Dehli.
- SPINELLO, R. 2000. Cyber-Ethics: Morality and Law in Cyberspace. London: Jones and Bartlett.
- SOUTH AFRICA. 2005. Privacy and data protection discussion paper. 2005. 109(124).
- SOUTH AFRICA. 1996. Constitution Act 108 of 1996.
- SOUTH AFRICA. 2010. Protection of State Information Bill.
- SOUTH AFRICA. 2012. Protection of Personal Information Bill.
- SOUTH AFRICA. 2013. Protection of Personal Information Act 4 of 2013.
- STAHL B.C. 2000. *The Impact of the UK Human Rights Act 1998 on Privacy Protection in the Workplace*. Hershey, PA: IGI Global.
- STALDER, F. 2002. Privacy is not the Antidote to Surveillance. *Surveillance & Society*, 1(1):8.
- THE AMERICAN HERITAGE DICTIONARY OF THE ENGLISH LANGUAGE. 2006. Washington: Houghton Mifflin.
- THE OXFORD ENGLISH DICTIONARY. 2002. Oxford: Clarendon Press.
- TURNER, E.C. & DASGUPTA, S. 2003. Privacy on the Web: An Examination of User Concerns, Technology, and Implications for Business Organizations and Individuals. *Journal of Information System Management*, 20(1):8-18.
- WARREN, J. 2008 . *Self-Imposed Violations of Privacy in Virtual Communities*. San Antonio: University of Texas.
- WESTIN, A. 1967. Privacy and Freedom. New York: Atheneum.

Annexure A: POLLING CHECKLIST

Research Question	Polling checklist Question	Response
1. Demographics	1.1 What is the user's gender?	Male (1), Female (2)
	1.2 What is the user's age?	18 – 25 (1), 25 – 30 (2), 30 – 35 (3), 35 – 40 (4)
	1.3 What is the user's hometown?	Mafikeng (1), Lichtenburg (2), Potchefstroom (3), Zeerust (4), Other (5)
	1.4 Where does the user work?	NWU (1), Other (2), None (3)
2. What private details are available on a user's profile?	2.1 What level of detail has the user placed in their profile?	Full Details (1), Partial Details (2), None (3)
	2.2 How many friends does a user have on their profile?	0 – 100 (1), 100 – 200 (2), 200 – 300 (3), 300 – 400 (4), 500 + (5)
	2.3 Does the user share their geo-location with friends?	Often (1), Sometimes (2), Never (3)
	2.4 What category of likes does the user have?	Entertainment (1), Technology (2), Automobile (3), Fashion (4), Food (5), News (6), Sports, Religious
	2.5 What is the user's primary choice for accessing Facebook?	Desktop (1), Mobile (2)
2. What are the Timeline activities of users on Facebook	2.1 What is the frequency of the user posting on their wall?	Daily (1), Weekly (2), Monthly (3)
	2.2 Does the user share events they are attending regularly?	Often (1), Sometimes (2), Never (3)
	2.3 What is the major activity of the user?	Posting (1), Commenting on other profiles (2), Liking comments-pages (3), Uploading pictures (4)
	2.4 How often does the user get tagged in others photographs?	Often (1), Sometimes (2), Never (3)
3. What type of 3 rd party content do users make use of	3.1 What type of programs does the user utilise on Facebook?	Games (1), Social (2), Facebook-related Programs (create a football jersey or who's been viewing my profile?? application) (3)
	3.2 How often does a user utilise these programs on Facebook?	Often (1), Sometimes (2), Never (3)
	3.3 How often do Facebook programs (games, etc) post using the user's identity to promote themselves?	Often (1), Sometimes (2), Never (3)
	3.4 How often do users recommend or praise a product, store or interest of theirs (i.e football team)?	Often (1), Sometimes (2), Never (3)

Annexure B: SURVEY

1. Do you believe your profile cannot be accessed by other Facebook users who are not your friends?	☐ Yes ☐ No ☐ Don't Know
2. How often do you share personal photos, geo-location and other sensitive information on Facebook?	☐ Very Often ☐ Occasionally ☐ Not Often
3. Has the following ever happened to you on Facebook?	☐ Tagged on appropriate material ☐ Strangers write on wall on Facebook ☐ Photos uploaded without your permission ☐ None of the above
4. As a Facebook user are you aware of your privacy rights?	☐ Yes ☐ No
5. Have you ever used Facebook privacy tools?	☐ Yes ☐ No
6. Do you know of the existence of the Protection of Personal Information Act?	☐ Yes ☐ No
7. Which privacy feature would benefit the most from being improved on Facebook?	☐ Location Sharing ☐ Tagging ☐ NewsFeed