User perspective of privacy and surveillance on social networks
Abstract

Social networks have integrated into people’s daily lives and they became a powerful medium for effective marketing and communication worldwide. Problem raise when governments and special agencies violate users’ information privacy under the pretext of protecting national security or something as, furthermore, when information became the source of income for social networks it became necessary to investigate users concerns about informational privacy on social platforms, if there are. The main purpose of the thesis is to understand what level of privacy awareness users on social networks have and how much relevant knowledge about surveillance on social networks they recognize. Moreover, the thesis aims to present users’ opinion about surveillance on Facebook and if they accept to be surveyed in certain scenarios. As results, the study has identified ambiguity in Facebook terms and data policy, while there has been clarity that Facebook applies massive surveillance in terms of data collection on all users on the network. 71% of the participants had concerns about their privacy on social networks, two-thirds of the participants didn’t read Facebook terms and 76% did believe that social networks sell users information for own benefits. The majority of the interview participants showed lack of knowledge about data collection on social networks, and didn’t know if governments do surveillance on social platforms or not. However, 37% of the survey participants claimed that they have nothing to hide and governments can look into their activities online, and almost similar percentage supported such an action. Further, most of the interview participants protect their informational privacy on social networks by having good privacy settings, controlling who have access to certain posts or managing friends list. However, 1/3 of the participants who had good privacy settings didn’t know all their friends on FB. Through personal observations on data analysis and literature review, I concluded the thesis with some suggestions of possible approaches to enhance information privacy, these recommendations present my own thoughts and weren’t derived in academic way rather personal notes during the thesis study.

Keywords

Informational privacy, data collection, social networks, Facebook, surveillance.
Acknowledgements

First and above all, I praise Allah, the almighty for providing me this opportunity and granting me the capability to proceed successfully.

To my Parents, for their encouragement and support in all aspects of life.

A sincere appreciation to my examiner Anita Mirijamdotter and supervisors Jiff Winter and Sisse Finken. Thanks for the warm encouragement, thoughtful guidance, critical comments and for assisting me in learning and growing as a student.

A special thanks for Christina Mörtberg, one of the most amazing professors I’ve ever met. I’ll never forget your kind words and your support during my study.

I would also like to thank Swedish Institute for awarding me the prestigious scholarship “Swedish Institute Study Scholarship”. Thanks for investing in my education, without this support I would have not been able to pursue my masters’ degree in Sweden.
Contents

1. INTRODUCTION ............................................................................................................. 1
   1.1. PRESENTATION ............................................................................................................. 1
   1.2. MOTIVATION ................................................................................................................ 1
   1.3. RESEARCH AIM AND RESEARCH QUESTIONS .......................................................... 2
   1.4. SCOPE AND LIMITATION .......................................................................................... 2
   1.5. THESIS ORGANIZATION ............................................................................................ 3

3. LITERATURE REVIEW ..................................................................................................... 4
   3.1. PRIVACY ...................................................................................................................... 4
      3.1.1. Privacy Meaning, Types and Frameworks ............................................................... 4
      3.1.2. The Controversy over Informational Privacy ......................................................... 5
      3.1.3. Privacy on Social networks .................................................................................... 6
         3.1.3.1. Overview of social networks ............................................................................. 6
         3.1.3.2. Why Facebook? ................................................................................................ 6
         3.1.3.3. Previous Studies on Privacy and Disclosure on Facebook ............................. 7
   3.2. SURVEILLANCE .......................................................................................................... 9
      3.2.1. Definition, History and Examples ......................................................................... 10
      3.2.2. Surveillance on Facebook ..................................................................................... 11

4. STUDY ON FACEBOOK TERMS AND DATA POLICY ................................................... 13
   4.1. INTRODUCTION .......................................................................................................... 13
   4.2. STATEMENT OF RIGHTS AND RESPONSIBILITIES ................................................. 13
   4.3. DATA POLICY ............................................................................................................. 15

5. METHODOLOGY ............................................................................................................. 20
   5.1. METHODOLOGICAL TRADITION (PARADIGM AND RESEARCH TYPE) ................... 20
   5.2. METHODS/TECHNIQUES FOR DATA COLLECTION AND ANALYSIS ....................... 20
      5.2.2. Sampling Method .................................................................................................. 20
      5.2.2. Interviews .............................................................................................................. 21
      5.2.3. Survey ................................................................................................................... 22
      5.2.4. Why Two Methods .............................................................................................. 23
      5.2.5. Data & Analysis ................................................................................................... 24
   5.3. VALIDITY AND RELIABILITY .................................................................................... 26
   5.4. ETHICAL CONSIDERATION ....................................................................................... 26

6. EMPIRICAL FINDINGS ..................................................................................................... 28
   6.1. ANALYZING INTERVIEWS ......................................................................................... 28
   6.2. ANALYZING SURVEY .................................................................................................. 32
   6.3. SUMMARY OF THE CRITICAL FINDINGS ................................................................. 38

7. DISCUSSION .................................................................................................................... 39
   6.1. REFLECTION AND INTERPRETATION ON PRESENTED RESULTS .......................... 39
   6.2. SUGGESTION OF POSSIBLE APPROACHES TO ENHANCE PRIVACY ................... 41
      6.2.1. Suggestions for users on SNs .............................................................................. 41
      6.2.2 Suggestions for SNs and governments ................................................................. 41

8. CONCLUSION .................................................................................................................. 43
   8.1. CONCLUSION OF MAIN ARGUMENTS AND FINDINGS ........................................... 43
   8.2. FUTURE RESEARCH SUGGESTIONS ....................................................................... 44

BIBLIOGRAPHY .................................................................................................................. 45

APPENDIX A ....................................................................................................................... 49
APPENDIX B ....................................................................................................................... 50
APPENDIX C ....................................................................................................................... 52
Table of Figures

Figure 1- Disclosure Patterns in the CMU FB Network ........................................ 8
Figure 2- Application Settings on Facebook (Others Use) ..................................... 17
Figure 3- Interview Participants ........................................................................... 22
Figure 4- Phases of Thematic Analysis ................................................................ 25
Figure 5- Participants have read FB terms ............................................................... 33
Figure 6- Amount of Reading ................................................................................ 34
Figure 7- Knowledge about a specific statement in the terms ............................... 35
Figure 8- Opinions if SN sells users’ info ............................................................... 35
Figure 9- Comp. who read the terms and think SN sell users’ info ....................... 36
Figure 10- Sharing personal info & friends list ..................................................... 36
Figure 11- Concerns about privacy in SN .............................................................. 37
Figure 12- Participants’ opinion about surveillance on SN .................................. 37

List of Abbreviations:

FB   Facebook
SN   Social Network
SM   Social Media
IS   Information Systems
1. Introduction

1.1. Presentation

In the 21st century, the way of communication between people around the world have changed to become more web-dependent or in another phrase Apps-dependent. Nowadays, social networks have become powerful marketing and communication tools. According to the statistics published in 2015 by Facebook and Twitter, more than 1.2 billion of users on Facebook while 288 million monthly active users on Twitter. These statistics for only two platforms that individuals use, so how is the situation for all social platforms? In fact, the high functionality with the multiple services provided by social network’s vendors, make individuals and corporations more attractive to use them than ever.

Rising concerns about the huge load of personal data on social media, and due to the increased violations against informational privacy, many debates in Europe particularly and in the world generally have been conducted to highlight and discuss this matter, e.g. the European Parliament Committee Debate on the EU-U.S (European Parliament, 2016). Privacy Shield in 2016, US Senate Debate NSA Surveillance 2015, and CPDP 2014/2015. These debates on surveillance and informational privacy weren’t only between politicians and change makers, professors and experts in law have also engaged in some of them to discuss the privacy policies accredited by social networks and online service providers.

The main purpose of the thesis is to understand what level of privacy awareness users on social networks have and how much relevant knowledge about surveillance they recognize. Moreover, the thesis aims to present users opinion about surveillance on Facebook and if they accept to be surveyed in certain scenarios. The choose of Facebook is based on the large number of users on the platform across the world which will be presented broadly in a separate section.

1.2. Motivation

Six years ago, youth in Middle-East and North Africa (MENA) used social media to make a change in their countries, revolutions in six different countries started virtually on Facebook and Twitter, then calling to protests against their government took its place on the ground (Allagui, 2011). Protesters were using social media as rostrum to express their opinions and claim for freedom from the humiliation that are exposed to, therefore some were calling this movement as a “Facebook revolution” (Allagui, 2011, p.2) referring to the huge impact that Facebook has in that period. Apparently, this is the good part of the story; the other side was extremely tragic when some governments in the MENA region decided to monitor the internet network in order to arrest people calling for demonstrations.

When I first found out that I have been selected into the Master programme, I knew that I wanted to write my thesis about something had to do with privacy and surveillance on social media. During my master study I had taken a course called Ethics & Profession in Information Systems, this course was one of the factors that
drive me to choose my thesis topic, mainly because it opened my eyes to the central ethical issues of digital media that I am aware but not much knowledgeable about it.

1.3. Research Aim and Research Questions

The initial purpose of my thesis is to understand a social phenomenon through an in-depth study of information privacy based on individuals’ perception. Therefore, I adapted the following research setting, the thesis is based on qualitative research and interpretive paradigm to achieve the need for in-depth analysis of participants’ opinions and thoughts about presented topics. The selected methods are interviews complemented by a survey. The research is focused on national and international students between 19-29 years old at Linnaeus university. For better focus, I decided to conduct my research on a particular social network, which is Facebook. Moreover, a descriptive study about the terms and data policy on Facebook has been conducted to interpret and analyze the rules and conditions on the platform.

A literature review has undertaken in order to structure my thesis questions, most of the literatures are related to the domain of privacy and surveillance on social media. The literatures gathered from Linnaeus University library, Springer, and Google scholar. Reading some of previous studies and researches in the field of information privacy gave me the ability to discuss the thesis topic from different viewpoints, that reflect the diversity of people perspective and demands. On the whole, the reviews assisting me in formulating the thesis question in a way of displaying the individuals’ perspectives. Eventually, the thesis questions have been designed as follows: Does Facebook do surveillance, or are they a channel for others to do surveillance? What are users’ thoughts about privacy and surveillance on social networks?

1.4. Scope and Limitation

This thesis conducted within the scope of privacy and surveillance over social networks. As a master student, my main goal for the thesis is to produce more knowledge in the field of IS with the focus of informational privacy over social networks. Two methods (interview and survey) used to enrich the quantity and quality of the data collection from the purposeful targeted group (that will be introduced in the methodology section). The corresponding results and findings might be limited since it relies on limited number of participants (9 interviewees and 59 survey participants) which might not completely represent the entire targeted group of students at Linnaeus University.

In addition, the concepts privacy and surveillance over social networks can comprehensively discussed from numerus angels, therefore, Privacy in the thesis will be discussed in terms of information management and information flow, definitely, the literature review will have a discussion about privacy on social media broadly but in the discussion and data analysis sections I will focus on the mentioned areas. On the other hand, surveillance will be discussed in terms of data collection on social networks generally and Facebook specifically, same as privacy, discussion about surveillance on the internet network will take a place in the literature review.
Moreover, information management in the thesis will refer to the way that users of social networks restrict sharing their information with others on the platform, as well as control who have access to certain kind of information. On the other hand, information flow will represent the transmission of information from person to another, and from person to a third-party partner on the platform.

Furthermore, the thesis will have a section studies Facebook terms and data policy to present to the applicable rules on the platform, therefore, this study is valid unless changes has performed on the terms.

1.5. Thesis Organization

The thesis will be divided into seven sections with numbers of subsections. As the first introduction section that has presented above, the concerned topic has introduced with the focus of the thesis, which is about privacy and surveillance over social networks based on users’ perception among students in Sweden. I have explained the purpose and motivation of the study, besides, the scope and limitations. In the second section, relevant literature reviews will be divided into two main subsections one related to privacy, informational privacy and privacy on social networks, while the second subsection will be discussing surveillance as a concept and then surveillance over FB. As the third section, it presents a study I had conducted on Facebook terms and data policy to interpret and analyze the policies applied on such a social platform and to give the reader an insight into the data has being collected by FB. The fourth section will present the research methodology with all details about research methods the thesis will employ. It further explains the data analysis and how I will carry out the data collection into practice. The fifth section considered as the central part of the thesis long as the third one, the empirical findings will be demonstrated with the actual research process and the results will be presented in this section. The sixth section is where I discuss main findings, results and special outcomes upon my own interpretation. The discussion will further reflect the empirical findings in line with the outcomes from the descriptive study and reflections from the literature review. The conclusion will come in the final section, to sum up what the main tasks of the thesis, the critical outcomes and findings, and finally propose some suggestions for future research.
3. Literature Review

3.1. Privacy

3.1.1. Privacy Meaning, Types and Frameworks.

“There is no universal definition of privacy” (Carew & Stapleton, 2005, p.2), and there has been a major problem in its definition, mainly because, there are many disciplines are interested in the topic of privacy and, therefore, there is much difficulty in relating one study to another (Newell, 1988). Presented below is some of the definitions that have been considerably presented in several literatures and academic works, which can build an understanding about privacy as a general concept.

- Interpersonal boundary by which a person or group regulates interactions with others (Derlega & Chaikin, 1977).
- Consensually agreed-upon right to maintain boundaries and deny access to others (Warren & Laslett, 1977).
- Control of movement of information across a boundary to and from individuals and groups (Shils, 1966).
- The claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others (Westin, 1970).

As we see, privacy has several interpretations, each of them related to a context, however, the first distinction evident from the previous conceptualizations is that, privacy is fundamentally formed and realized through information accessibility across contexts and boundaries, no matter if the unit experiencing the privacy is a single individual or group of them. Adding to the previous list, privacy is also described as freedom from interference or intrusion, the right to be let alone (Warren & Brandeis, 1890). This formulation recognizes that each person has a space of existence; where s/he can be free doing activities belong to him alone. This space should be protected especially when individuals want to have some private activities. “Most would recognize the protected sphere to include personal opinions, personal communications, and how one behaves behind closed doors” (McFarland, 2012). Therefore, each individual in the society determine by his own, which sort of activities and behavior could be public and which couldn’t. It’s pretty interesting how McFarland characterize the protected sphere, and by reflecting his view on the thesis topic, users’ profiles on social networks could be considered as a space which they have to have the right to protect it as they see it fit.

Privacy scholars and advocates have developed for years theories, frameworks, white papers to promote and highlight the necessity of privacy in our communities. Michael Burgoon a professor of communication at Michigan State University has developed the privacy framework to elucidate the dimensions of privacy. Burgoon distinguishes three different dimensions of privacy: social, psychological and informational. He defined social privacy as “having control over the actual interaction with others, and the frequency, length, and content of that interaction”. Psychological privacy “protects the individual from intrusions upon one’s thoughts, feelings, and values, and the freedom to decide to whom to disclose certain personal thoughts and feelings”.

Lnu.se
Informational privacy means “the ability to control who gathers and disseminates information about oneself or one’s group and under what circumstances” (2012 cited in Velden & Emam, 2013, p.2). Because information is the source of social networks, Informational privacy is the most one among the three dimensions in relation to the thesis, therefore, a separate section about informational privacy will be presented next.

Generally, perception or the definition of privacy differs from culture to culture and from country to country (Milberg, et al., 2000). Many factors included in shaping the formula of privacy, such kind of factors are: believes, religions, Laws, customs and traditions. In spite of that, all confirm that the main concept of privacy is protecting personal information from being exposed in public. However, it’s not easy to determine which kind of information considered as personal and which is not, especially in a global context.

3.1.2. The Controversy over Informational Privacy

Moor (1989) has defined informational privacy as “the right to control of access to personal information”. From this perspective, we can say protecting informational privacy is actually protecting specific data from being accessed; this sort of protection should be based on controlling. Fried (1984, p.209) states “privacy is not simply an absence of information about us in the minds of others, rather it is the control we have over information about ourselves”. No matter the importance of the information, individuals should have the right to control who is allowed to share it. In this point, the debate between lawmakers, Lawyers, and scholars starts. Moor, professor of Intellectual and Moral Philosophy at Dartmouth College, insists in his article The Ethics of Privacy Protection on the importance of separating the concept of privacy from the concept of liberty and that because “we do not want the right to privacy to become a screen to protect truly harmful actions” (1991, p.74). In similar perspective, politicians indicate the importance of surveillance in protecting individuals and the national security from potential threats. So, in a descriptive sense, what determines a society’s boundaries on the right to privacy?

As a fact, the right to privacy isn’t only a hot topic between philosophers and human rights scholars. It also becomes significantly debatable in business ethics. For instance, considering the debate about targeted marketing that is occurring in many countries, “while organizations claim the right to use information technology to improve efficiency, consumers often exhibit the desire to control the flow and dissemination of their personal information. While businesses claim the right to record information generated from their transactions, consumers increasingly want to know that this information has been gathered and stored and to control its uses” (Goodwin, 1991 cited in Milberg, et al., 2000, p.36). Thus, the trade-off between the benefit that accrue from marketers’ use of personal information and consumer rights to information privacy must be recognized (Milne & Gordon, 1993 cited in Milberg, et al., 2000).
3.1.3. Privacy on Social networks

3.1.3.1. Overview of social networks

The terms Social Media and Social Networks will frequently appear in the thesis, therefore, and before diving deeper, it’s important to distinguish the difference between both terms. Kaplan and Haenlein (2010, pp.61-63) determine the definition and the differentiation of these two phrases. According to them, social media is “a group of Internet-based applications that build on the ideological and technological foundations of Web 2.0, and that allow the creation and exchange of User Generated Content”, while social networks are “applications that enable users to connect by creating personal information profiles, inviting friends and colleagues to have access to those profiles, and sending e-mails and instant messages between each other”. Within these general definitions, we find out that social networks are part of huge cybersphere called social media, which contains many other components like: collaborative projects, content communities, blogs, and virtual game worlds. All these components essentially focus on the communication between people, and try to shape the social media as a firm where individuals can interact and collaborate with each other and with organizations to gain the most of it.

According to statistics published by Twitter (2015), more than 288 million monthly active users on the platform and around 500 million Tweets are sent per day. Facebook (2015) also releases an annual report about the number of users and activities on the platform, the figures shows that 890 million daily active users on average for December 2014 and 1.39 billion monthly active users as of December 2014. However, choosing a platform to conduct my study on, rather than talking about social networks in general, will definitely give enough space to focus on particular details and specific privacy issues facing us while using social networks.

3.1.3.2. Why Facebook?

Facebook has been preferred to conduct my study on for several reasons – here I’ll explain briefly the motivation beyond this chosen -. First of all, the unexpected growing of its usage all over the world, Dogruer, Menevi, and Eyyam (2011) refer to the extensive use of FB by saying it is considered as the most commonly used social networking website, and the number of its users continues to grow markedly from day to day. Second of all, Facebook as a phenomenon becomes an important material to study in universities and research centers, according them there have been mountains of researches which study the use of Facebook in various ways. Furthermore, studying this phenomenon becomes not only important for scholars interested in technology, but also for researchers in politics, economy and psychology. Mainly because of the influence that Facebook has on communities and the important role it plays in directing individuals’ opinions and behavior, to clarify this fact we just need to remember what Facebook did in 2012, when it have had an experiment over 700,000 of its users to see the effect of feeding certain kind of news, Robinson Meyer, an associate editor at The Atlantic, wrote an article about the experiment and mentioned how FB could change what’s shown up in News Feed in order to manipulate users’ emotional states, “which was exactly happening in that experiment” (Meyer, 2014). – It’s important to clarify that what FB did and is maybe doing right now is completely
legal according to its terms of services – . Last but not least, Facebook is considered as one of the most SN that people sharing tremendous amount of information on, most of the information published in Facebook considered as personal especially when it’s related to life events, travel locations, education and work experiences, and relationship status.

3.1.3.3. Previous Studies on Privacy and Disclosure on Facebook

In this section two studies will be presented to bring up some results from previous research work on privacy and disclosure on FB. The first study is Silent Listeners: The Evolution of Privacy and Disclosure on Facebook (Stutzman, et al., 2013), published to present how privacy and disclosure behavior changed among Facebook users between 2005 and 2011. The study used profile data from a longitudinal panel of 5,076 Facebook users of the Carnegie Mellon University (CMU) Facebook network. One limitation of this data according to Stutzman, et al. (2013, p. 8) is that “it cannot reflect a random sample of current Facebook users”.

The second one, Analyzing Facebook Privacy Settings. User Expectations vs. Reality (Liu, et al., 2011), a study focused on measuring the disparity between the desired and the actual privacy settings, quantifying the magnitude of the problem of measuring privacy. The study deployed a survey, implemented as a FB application, to 200 FB users recruited via Amazon Mechanical Turk (Liu, et al., 2011). The survey (FB application) was able to query FB to select content to query the user about, as well as to collect the current privacy settings for the users’ uploaded content. By doing so, the user “asked to provide optional demographic information (age, gender, income, education level, and U.S. state). Then, the user is asked to answer questions about the ideal privacy settings of some of his uploaded content. Finally, the survey collects information from the user’s profile, including the privacy settings for all uploaded content” (Liu, et al., 2011, p. 63).

These two studies have been chosen to be a reference in the thesis for two main reasons. Firstly, with the daily evolution and changes arise on SNs it becomes imperative to study how privacy and disclosure evolved on SNs over an extended period of time, which is the aim of the first mentioned study (Stutzman, et al., 2013). Secondly, the main focus of the thesis is onto privacy issues and concerns on SNs generally and FB specifically, therefore, and before presenting my empirical study is good to show the variance between the desired and actual privacy settings that FB users’ have on their profiles.

According to Stutzman, et al. (2013, p. 7) “over time Facebook users in our dataset exhibited increasingly privacy-seeking behavior, progressively decreasing the amount of personal data shared publicly with unconnected profiles in the same network”, by means, FB users in their study became more protective of spreading personal information with strangers (profiles in the same network but unconnected to the user) by limiting data publicly shared. Below figure will visualize the disclosure patterns in the CMU FB network.
Examining panel sharing over time Stutzman, et al. (2013, p. 7) saw “a consistent reduction in the proportion of the population sharing all profile elements, as the chart moves from reds and purples in 2005 to dark blues in 2009”. As Facebook grew in popularity, and new features were added, the individuals in the panel became less public with the information they shared.

In the study, the authors observed a second result which is, policy and interface changes implemented by Facebook seemingly altered that outcome and countered such privacy-seeking behavior. Specifically, between 2009 and 2010, they observed a significant increase in the public sharing of various types of personal information. They linked the trend reversal to specific changes in Facebook’s site interface and default settings (Stutzman, et al., 2013). As a reflection in this matter they highlighted the power of the platform in affecting individual choices saying that, “the entity that controls the structure (in this case, Facebook), ultimately remains able to affect how actors make choices in that environment” (Stutzman, et al., 2013, p.9).

Third and final observation the authors noticed, over time, the amount of personal information that FB users revealed to their FB ‘friends’ actually increased. In doing so, users ended up increasing their personal disclosures to other entities on the network as well: third-party apps, (indirectly) advertisers, and Facebook itself. Sometimes this occurred without users’ explicit consent or even awareness (Stutzman, et al., 2013).

Moving ahead to the second study, Analyzing Facebook Privacy Settings. User Expectations vs. Reality (Liu, et al., 2011), the data analysis in the research revealed that “while users are uploading significant amounts of content to Facebook, almost half of the content is shared with the default privacy settings, which expose the
content to all Facebook users”, moreover, users in the survey “reported that this was the desired setting only 20% of the time, suggesting that the default settings are poorly chosen”. More worryingly, “even for photos for which the privacy settings have been modified by the user, the modified privacy settings match users’ expectations less than 40% of the time” (Liu, et al., 2011, p. 65), which might suggest that users were having troubles configuring privacy settings in their accounts. The research emphasized on the importance of improving privacy tools that can assist users in managing their privacy. For instance, developing a mechanism that automatically update friend lists based on a community detection algorithm that can leverage the social links between the friends of a user to automatically group them into communities, where each community of friends can be used to create a friend list (Liu, et al., 2011). In this perspective, FB user can select which friend list to share the content with, which in my opinion will save time and bring much privacy for users having big number of friends in their network. Another suggested solution to enhance privacy was, developing a mechanism that measure privacy violations, potentially by using machine learning approaches on metadata (Liu, et al., 2011).

From the first presented study we can see that Facebook users exhibited increasingly privacy-seeking behavior, they became more protective of their personal information by progressively limiting information publicly shared with ‘strangers’, however – and in parallel to their reducing disclosures to unconnected users – they ended up increasing their information disclosures with friends and other entities connected to FB, moreover, and for a period of time the increase in the information disclosure was influenced by the changes implemented on FB policies and user interfaces on the platform. On the other hand, while half of the participants in the second study exposed their information to the public (all FB users), the large majority of them claimed that this was not the desired setting, which might be an indication to troubles in configuring Facebook privacy settings. That being said, the majority of the participants who publicly shared their content, didn’t intentionally do so. Filling in the gap, a part of the thesis will come to investigate what level of privacy awareness users on social network they have, and what ways they use to protect their information privacy on social networks generally, and Facebook particularly.

3.2. Surveillance

This chapter will discuss the history of surveillance by giving some examples for such an act in the past, some types of surveillance for instance surveillance over social networks and mass surveillance, how governments and big enterprises could perform surveillance over the public or internet-users specifically. Finally a separate subsection will discuss surveillance on a selected SN platform which is Facebook.

It’s important to point out that this chapter doesn’t give an intensive information about the subject (surveillance) in its all kind of implementation rather than it’s discuss the phenomena with respect to the thesis topic. Moreover, there is lack of the academic authentic resources that could be used to support the presented arguments, especially for the ones depend on the global surveillance disclosures by Edward Snowden, That being said, the following arguments don’t represent an absolute truth but opinions based on experience and top secret documents leaked by ex-NSA contractor Edward Snowden.
3.2.1. Definition, History and Examples

According to Merriam-Webster (2015) dictionary, surveillance is defined as “the act of carefully watching someone or something especially in order to prevent or detect a crime”. Oxford Dictionaries (2015) also define surveillance as “close observation, especially of a suspected spy or criminal”. Both definitions explain surveillance as a monitoring process to prevent felonious actions in order to protect individuals, groups or even objects.

Throughout history, people always had interest in collecting information since more information means more power. However, the possibility of watching people's private lives on a large scale only became possible since the invention of the press, telephone, and cameras as Robert Ellis Smith (2013, time: 1:00) explains. Large companies like Western Union had access to people's personal information such as relations and history of transactions. This situation continued until two lawyers: Samuel D. Warren and Louis D. Brandies initiated the first law review named “The Right to Privacy” which discussed public privacy in the commercial life. The government did not take a role until the twentieth century when the ability to listen to and capture people's phone calls, also known as wiretapping, became feasible. However, large and organized collection of public data only became possible after the invention of the computers. This data was collected and used by governmental institutions responsible about public assistance and like the FBI and NSA (Smith 2013, time: 1:10).

Surveillance has many types depending on the means that are used to conduct the act. A widely spread type of surveillance is on-line surveillance. As the name suggests, on-line surveillance uses the World Wide Web to spy on people. An example of on-line surveillance is the ability of NSA to read the email of any person who uses common email services inside and outside the US (Snowden 2015, time: 1:09:00). Even though some email services providers have an encryption technique to secure their users’ data, those providers have been forced by governments to allow access to their customers’ encrypted emails. Another example is the recording and analysis of internet traffic by the NSA as well. According to Snowden, even if the government doesn't have the right to read your data without a reason, there are programs and algorithms that analyze your data constantly. Thus, any normal person can be flagged for inspection in a day just because he visited a certain sequence of websites for example! When flagged, your personal data becomes prone for investigation (Snowden 2015, time: 28:00). The On-line surveillance by NSA doesn't only read unencrypted data, it continues further to intercept them and redirect or load them with malicious softwares (Snowden 2015, time: 40:00). On the other hand, some surveillance methods don’t require the user to be on-line. Using the GPS data collected from a mobile device, the government can track the person who is holding the device, so do other governments, hackers, and some enterprises. The information obtained from GPS can also be used to analyze the users’ relations. For example, if two mobile devices “sleep” at the same place every night, then their users are probably in a relation (Snowden 2015, time: 1:11:00).

The main problems with surveillance today can be summarized in three points. First, people are targeted regardless of their criminal activities and private data and records are used and shared without people’s consent (Snowden 2015, time: 18:00). Second, even though people now know that they are being surveyed, governments are reacting
with more surveillance (Snowden, 2015, time: 24:45). Finally, one cannot opt out of surveillance anymore. Internet and on-line social networks are necessities in life nowadays and not using them can cause many problems like not getting a job or being branded as socially awkward (Nissenbaum, 2013, time 3:20).

3.2.2. Surveillance on Facebook

An interesting company to be examined about surveillance is Facebook. One reason is that as of the second quarter of 2015, Facebook had 1.49 billion monthly active users (Statista, 2015). Another reason is the type of data people upload to Facebook. Today, people share their everyday status, pictures, friends, ideas, emotions, and much more on Facebook. Studying this information might tell more than the person knows about him/her self. In his paper “An Alternative View of Privacy on Facebook”, Fuchs (2011, p.148) argues that “social networking sites are especially suited for targeted advertising because they store and communicate a vast amount of personal likes and dislikes of users that allow surveillance of these data for economic purposes, finding out which products the users are likely to buy”. When realizing that targeted advertisement is the main source of income to companies like Facebook, it becomes expected that mass surveillance is applied on Facebook users (Stallman 2011, time: 0:25). An important characteristic of this surveillance is that it requires “permanent input and activity of the users are needed, which are guaranteed by the specific characteristics of web 2.0, especially the upload of user-generated content and permanent communicative flows.” Moreover, this surveillance is imposed on the public for two reasons: First, because “Targeted advertising is automatically activated and cannot be deactivated in the account- and privacy-settings” (Fuchs, 2011, p.152). Second, because it is becoming harder to not use a Facebook account today as argued before.

The process that Facebook uses for targeted advertisement is complicated. However, Fuchs (2011, p.156) summarizes the process of data gathering and analysis in the following paragraph:

“Facebook watches and records usage behavior and personal data uploaded and entered by users (surveillance), it aggregates information about users that is obtained from its own site and other sites (aggregation), based on aggregation it identifies the consumer interests of users (identification)”

The second stage is actually very critical. It means that users’ data is not only collected and analyzed on Facebook, but also connected and compared with websites and companies that have similar surveillance techniques. This guarantees two properties for the collected information: authenticity and generality. Since the data is collected from multiple websites, comparison of data can show any odd properties and neglect them. It then becomes harder for normal users to fake personal information and the resulting data is consistent and authentic. On the other hand, gathering personal information from multiple companies which provide different services means that the resulting data is versatile and contains information of wide range like musical and fashion preferences. Thus, personal data can be sold or used by a wide range of enterprises which are willing to pay the price! — In fact, what’s written above and what will come after will drive us to an important subject which is Big Data & Analytics, the term that has become a ubiquitous in many parts of industry and
academia. Unfortunately, my thesis scope doesn’t cover the topic (big data & analytics) explicitly, therefore I won’t dive deeper in this subject but the upcoming sections will have some points that are tightly related to the concept —.

Facebook, however, doesn't stop at collecting its users’ information, it goes further to grant government agencies like NSA the right to access these data as well. Facebook has been part of an NSA project called PRISM since 06/03/2009 (Snowden 2014). As Edward Snowden revealed the US PRISM programme it’s about the content, it had been surveying the transmitted data of US and non-US citizens (Whitley, et al., 2013, p.84). Some companies like Yahoo tried to refuse being part of this project but to no avail. So far, a clear description of PRISM has not been leaked. However, Richard Lempert (2013) gives a rather simple explanation of what PRISM is capable of:

“PRISM appears to be a far narrower intelligence gathering program but far more intrusive. It can capture not just meta-data but the content of communications transmitted via the web, including messages sent and retrieved, uploaded videos and the like. It is specifically targeted, and without a warrant neither American citizens nor permanent resident are legal targets. However, the protections citizens and permanent residents enjoy appear loose. News stories suggest that data capture is allowed to proceed whenever a responsible agent thinks it more likely than not that a possible target is foreign”.

This passage explicitly says that NSA actually can access the data stored on the servers of companies that are part of PRISM including Facebook. It doesn't only give NSA the ability to analyze personal data, but also the ability to access the content of this data. The critical yet vague conditions under which PRISM can be used is what makes PRISM dangerous to people not only in the U.S. but also around the world. Actually, as can be seen from the passage, foreigners have less protection to their personal data than U.S. citizens, which is why many countries around the world today are calling for a change in the surveillance policies conducted by the US government and agencies. Most people around the world are still in a state of consent to these policies. In fact, these people are giving up serious rights that might become important in a future where on-line life dominates.
4. Study on Facebook Terms and Data Policy

4.1. Introduction

This section of the thesis will be divided mainly into two sub-sections, the first one will be a study on FB terms, where I can give an insight into the terms and rules derived from FB principles to govern the relationship with FB users, as well as others who interact with Facebook products, brands and services. While the second sub-section aims to draw a picture of how FB deals with users’ data, to what extent FB can collect information and how much data was being kept in its servers.

Basically, the purpose of this study is to build an understanding about FB terms and data policy, how much control FB has over users’ information, and relate afterwards observations from this study with the empirical findings from the interviews and survey, which will lead to a meaningful discussion at the end of the thesis.

4.2. Statement of Rights and Responsibilities

As any social network, anyone wants to have a Facebook account needs to accept the terms and data policy as a first step to create a profile, in FB main page it’s clearly stated “by clicking Sign Up, you agree to our Terms and that you have read our Data Policy, including our Cookie Use” (Facebook, 2015). Some users before clicking on Sign Up they go through the links to know what they give their consent on, while others don’t check at all.

This part of the thesis will discuss some of the terms and policies that all FB users consent on since they created their profiles, whether they pay attention to them or not. Furthermore, the upcoming discussion will show the privileges that FB has over users’ information and activities on the internet network. At the end of this section, the reader will have a picture about the amount of information that FB can collect and an overview about privacy vulnerabilities in such a network.

Starting with the Terms page, you will find yourself in a long web page titled as ‘Statements of Rights and Responsibilities’, with around 3363 words this page divided into 18 sections each one related to a certain type of regulations, such as privacy, safety, payments, termination, disputes, … etc., under each section of them there are several rules and conditions that govern the relationship between different parties. At the end of the page there is a link to the Data Policy page and 10 other links to documents “which provide additional information about your use of Facebook” (Facebook, 2015).

The first policy under Sharing Your Content and Information section states:

For content that is covered by intellectual property rights, like photos and videos (IP content), you specifically give us the following permission, subject to your privacy and application settings: you grant us a non-exclusive, transferable, sublicensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook (IP License). This IP License ends when you
delete your IP content or your account unless your content has been shared with others, and they have not deleted it. (Facebook, 2015)

This policy is basically saying, if someone uploads a picture or any kind of IP content such as, video or audio, he has the copy right of that material, and by uploading such a file he gives FB permission to use it however they want, which is clearly described later in the terms, when FB defines the word ‘use’:

By "use" we mean use, run, copy, publicly perform or display, distribute, modify, translate, and create derivative works of. (Facebook, 2015)

“In essence, Facebook owns most of your data” (Semitsu, 2011, p.313). But, it’s all ‘subject to your privacy and application settings’ which demonstrates that FB doesn’t have the right to disseminate a user’s intellectual property beyond the user’s approved distribution list (Semitsu, 2011, p.313). Actually, this interpretation is based on limitations and Semitsu says: “it’s not clearly written in the contract” (Semitsu, 2011, p.314). However, the above interpretation is applied if an IP content is owned by only one user but what if it is shared with others, in this case one textual and reasonable interpretation says: “once a user has shared a photo with another person who does not delete the content, Facebook has an irrevocable license to distribute the photo to whomever it wants” (Semitsu, 2011, p.314). It seems that FB designed this policy as it is to protect itself from copy right violations and to grant itself the right to disseminate and distribute users’ intellectual properties without infringing intellectual property statutes. Despite the fact that FB has been granted the right to use its users’ IP content, it has the right to sublicense it to whomever it wants. In addition, once the user accepts the terms by having a FB account, the company (Facebook) has the right to distribute his IP contents to any third-party or advertiser it’s dealing with. So, anyone has a public profile shouldn’t be shocked if one day he uploads a video on his Facebook account and later on he finds it published on a third party website without him knowing. It’s important to note out that none of the above affects the user ownership or copyright privileges for the IP content he has. Thus, in the event of copyright infringement by a third-party, Cerroni (2012) advices “the person whose rights are breached to send a takedown notice to the host of the images”. To be fair, one thing should be pointed out here before moving to another clause, which is, Facebook does a decent job when it ends up its license to use an IP content as soon as the user delete that content and that’s clearly stated: “This IP License ends when you delete your IP content or your account unless your content has been shared with others”(Facebook, 2015), to clarify this matter more another clause designed immediately after, which says:

When you delete IP content, it is deleted in a manner similar to emptying the recycle bin on a computer. However, you understand that removed content may persist in backup copies for a reasonable period of time (but will not be available to others). (Facebook, 2015)

Even though FB terminates its license to use a content as long as it’s removed by the user who own it, but there is still a debate about the period it takes for a complete deletion from its servers. Moreover, FB promised that the backup copies won’t be available for others but that doesn’t deny the truth that it’s still somewhere in those servers.
The next paragraph should be highlighted up here from the *Statements of Rights and Responsibilities* is the one related to Advertisements and Commercial Content, which is numbered as 9 in the *Term* page,

Our goal is to deliver advertising and other commercial or sponsored content that is valuable to our users and advertisers. In order to help us do that, you agree to the following:

1. You give us permission to use your name, profile picture, content, and information in connection with commercial, sponsored, or related content (such as a brand you like) served or enhanced by us. This means, for example, that you permit a business or other entity to pay us to display your name and/or profile picture with your content or information, without any compensation to you. If you have selected a specific audience for your content or information, we will respect your choice when we use it.

2. We do not give your content or information to advertisers without your consent. (Facebook, 2015)

In this part of the terms, FB has determined clearly that it could use some of users’ information for advertisements and commercial purposes — and there is no clarity above what has written in the first paragraph — However, for some it could be somehow acceptable to let FB use some of their information as long as they have a good privacy settings and FB is the only one handling the whole process, but is it the case? The second term in above paragraph comes to give FB more privileges in distributing users’ information. It shows that FB could give some information or content of its users to advertisers if it gets the user’s consent on that. Actually, the term ‘without your consent’ is maybe the most abused term in the *Statement of Right and Responsibly* because it is not explicitly saying what that means. Clarifying that, consent usually requires some sort of affirmative step, like saying ‘Okay, I’ll give this information over’, whether or not, clicking on I agree on the *Terms and Data Policy* or simply putting the information on FB is consent enough, but that’s still a little bit up in the air.

### 4.3. Data Policy

Facebook has applied many changes to its data policy, most of the updates were modifications on existed terms, and a new set of rules/terms that the company wants to implement have been set in place. Facebook announced that working out on the new data policy will take effect on January 30, 2015 and by using FB services after that date, users agree to updated terms, data policy as well as cookies policy (Facebook, 2015). Facebook (2015) justified the new policies as a responding to people who have asked for better explanation in how the company gets and uses information of its users, as well as it comes to introduce new controls and features which help users to get more out of FB.

Diving deeper in Facebook data policy, a well formatted webpage contains approximately 2600 words divided into 8 parts, each of them comes to answer a specific question that users could have in mind regarding data policy on FB, e.g. What
kind of information does FB collect? How does FB use this information? How is this information shared? And so on.

In 2014, Anne Helmond a lecturer at University of Amsterdam wrote an article about the new FB data policy which went into effect at the beginning of 2015, Helmond gave a good analysis of FB new terms in the article, therefore, arguments from her article will be used to explain some of the new terms.

The first part to be discussed in the data policy is the one titled as “What kinds of information do we collect?” In point of fact, Facebook collects different kind of information from and about its users depending on the services used. 8 main subsections included under the question to describe how data are being collected and used. Under Things you do and information you provide, Facebook says:

We collect the content and other information you provide when you use our Services, including when you sign up for an account, create or share, and message or communicate with others. This can include information in or about the content you provide, such as the location of a photo or the date a file was created. We also collect information about how you use our Services, such as the types of content you view or engage with or the frequency and duration of your activities. (Facebook, 2015)

The general translation for that is, Facebook knows what you are doing on FB and they can use what you are doing to tweak FB and make the services better for you. According to Helmond (2014), “Facebook explicitly acknowledges that it is tracking its users to collect data” and the above paragraph comes to announce that publicly. Actually, Facebook doesn’t only collect content such as (posts, photos, messages ...) but also, collects meta-data from files you upload. For example: each picture you publish on FB has a set of meta-data inside of it, like: camera type, phone model, location (if GPS is enabled), and many other information. Certainly, FB could use this sort of information for whatever purpose it wants. On the other hand, FB records users’ activities on its platforms as long as they use any type of its services, but does the events scheduler on FB start recording only when users visit the platform? And is there a possibility that FB can watch the internet browsing activities even though the user is logged out? Finally, what about non-Facebook users, does the company have the ability to track them or watch what they are doing on their browsers? All of these questions and more will be answered in the section which talks about the data infrastructure that Facebook is building.

Another headline under the same inquiry (What kinds of information do we collect?) is, Things others do and information they provide. In this part, FB determines how it deals with users’ information provided by their friends or others on the network, e.g. users’ photos that are uploaded by their friends on the network, received messages, posts that the user has been mentioned on by his friends ... etc., under the subtitle previously mentioned, Facebook says:

We also collect content and information that other people provide when they use our Services, including information about you, such as when they share a photo of you, send a message to you, or upload, sync or import your contact information. (Facebook, 2015)
What Facebook tries to show through the above paragraph is, when it comes to privacy you are not the only one who control your privacy in that sort of information, other people who upload pictures of you, or who upload the contacts box, or who message you, they also provide FB with quite a bit of information about you whether you like it or not. In a nutshell, Facebook doesn’t collect information about you only through your profile and activities you’ve done in its platforms but also gets a lot of information about you through your friends on the network. Helmond (2014) elaborates in this matter, according to her, “your Facebook friends determine which part of your data will be shared with their apps through their app settings”. In that sense, your FB friends are able to share some information about you with the apps they use, and as a result, those apps can use your information in whatever way they want - the term *use* has been defined previously according to FB terms -. However, can we know what kind of information that your friends on FB are able to share about you with the apps they use? Simply, going to App Setting, under Apps Others Use there is a description about the categories of information that people can bring with them when they use FB apps, and the picture below shows that clearly:

<table>
<thead>
<tr>
<th>Apps Others Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>People on Facebook who can see your info can bring it with them when they use apps. This makes their experience better and more social. Use the settings below to control the categories of information that people can bring with them when they use apps, games and websites.</td>
</tr>
<tr>
<td>✓ Bio</td>
</tr>
<tr>
<td>✓ Birthday</td>
</tr>
<tr>
<td>✓ Family and relationships</td>
</tr>
<tr>
<td>✓ Interested in</td>
</tr>
<tr>
<td>✓ Religious and political views</td>
</tr>
<tr>
<td>✓ My website</td>
</tr>
<tr>
<td>✓ If I'm online</td>
</tr>
<tr>
<td>✓ My status updates</td>
</tr>
<tr>
<td>✓ My photos</td>
</tr>
<tr>
<td>✓ My videos</td>
</tr>
<tr>
<td>✓ My links</td>
</tr>
<tr>
<td>✓ My notes</td>
</tr>
<tr>
<td>✓ Hometown</td>
</tr>
<tr>
<td>✓ Current city</td>
</tr>
<tr>
<td>✓ Education and work</td>
</tr>
<tr>
<td>✓ Activities, interests, things I like</td>
</tr>
<tr>
<td>✓ My app activity</td>
</tr>
</tbody>
</table>

*Figure 2- Application Settings on Facebook (Others Use)*

The control panel in the Apps Setting page gives the user the ability to manage which kind of information that his friends are able to share about him when they use FB apps, as well as it gives him a privilege to turn off all Platform apps. But remember, you will not be able to use any games or apps yourself.
website” (Helmond, 2014). So, FB users who want to prevent application providers from getting their information, can either banned all apps from getting any kind of information about them through their friends and in return they lose some of FB services, or they allow their friends’ apps to get at least their basic information (profile info and list of friends) and in this case they would still have access to FB apps.

Talking about the data-intensive infrastructure which Facebook has been building, I have to go further in the data policy, and give more details about the data are being collected by FB. According to Helmond (2014) “it becomes clear that Facebook is increasingly expanding its data collection mechanism using more devices, services and partners”. Nowadays FB collects more and more data, a few things are being collected for example, device information, credit card and payment information and last but not least, data about you from third-party partners. In fact, it’s not hidden that FB gets users’ device information and when we say device information we mean all kind of electronic devices where users can have access to FB through them, e.g. computers, phones, tablets, smart watches and smart TVs. According to FB data policy and under Device Information subtitle, Facebook says:

We collect information from or about the computers, phones, or other devices where you install or access our Services, depending on the permissions you’ve granted. We may associate the information we collect from your different devices, which helps us provide consistent Services across your devices. Here are some examples of the device information we collect:

- Attributes such as the operating system, hardware version, device settings, file and software names and types, battery and signal strength, and device identifiers.
- Device locations, including specific geographic locations, such as through GPS, Bluetooth, or WiFi signals.
- Connection information such as the name of your mobile operator or ISP, browser type, language and time zone, mobile phone number and IP address.

(Facebook, 2015)

Based on the above, Facebook assumes that its users are on notice that the company can get some kind of information from users’ devices, it’s right that all is depending on the permissions that the user grants but it’s still unclear how much data FB can collect from users’ devices.

Some of the new features that Facebook recently added to its platform are buy button and donate button, according to Facebook the new tools come to make purchases more convenient and to help people discover and purchase products without leaving the platform (Facebook, 2015). Moreover, Facebook is developing peer-to-peer payments feature through FB messenger, this service is launched across the entire U.S. and the company plans to make it internationally available in near future. What makes this service really beneficial, according to Facebook (2015), it’s free, easy and secure. In terms of security concerns, Facebook added that users’ debit card information will be “kept in a secured environment that is separate from other parts of Facebook,” and that a “team of anti-fraud specialists” will monitor the platform for suspicious activity (Facebook, 2015). Thus, in order to make transactions and payment services more efficient, Facebook decided to get more financial information
from its users, such as credit or debit card number, authentication information, billing and shipping details. According to the data policy and under Information about payments, Facebook says:

If you use our Services for purchases or financial transactions (like when you buy something on Facebook, make a purchase in a game, or make a donation), we collect information about the purchase or transaction. This includes your payment information, such as your credit or debit card number and other card information, and other account and authentication information, as well as billing, shipping and contact details. (Facebook, 2015)

Last think I’ll talk about it in this section is the information that Facebook gathers from third-party partners. Regardless what users decide to disclose on FB products, Facebook will collect information about you from third-party websites and apps that use its services even before you connect to any FB products (Facebook, 2015). Some of the services that FB provides to third-parties are like, share, comment and FB login buttons. It’s not completely clear how much information FB collects from third-party partners but we already knew that it could get records about what you are doing at these websites. I won’t dive deeper in this subject but I’ll conclude by mentioning what is written in FB data policy regarding this matter.

**Information from websites and apps that use our Services.**
We collect information when you visit or use third-party websites and apps that use our Services (like when they offer our Like button or Facebook Log In or use our measurement and advertising services). This includes information about the websites and apps you visit, your use of our Services on those websites and apps, as well as information the developer or publisher of the app or website provides to you or us.

**Information from third-party partners.**
We receive information about you and your activities on and off Facebook from third-party partners, such as information from a partner when we jointly offer services or from an advertiser about your experiences or interactions with them. (Facebook, 2015)
5. Methodology

5.1. Methodological Tradition (Paradigm and Research Type)

A paradigm is a pattern of thinking, “a set of philosophical assumptions” (Myers, 1999 cited in Finken, 2014). Interpretive paradigm has chosen for the thesis; choice of the paradigm has been made based on my goal to investigate the participants’ perspective of privacy and surveillance over social networks which is connected with the aim of the paradigm to “understand phenomena through the meanings people assign to them” (Myers, 2013, p.39). Walsham (2006, p.1) argued that “interpretive methods of research start from the position that our knowledge of reality, including the domain of human action, is a social construction by human actors.” He continued, “our theories concerning reality are ways of making sense of the world”. Therefore, and in order to illustrate people’s opinion about privacy and surveillance over social network, we need to understand what level of privacy awareness users on social networks have and how much relevant knowledge about surveillance on social networks they recognize. Thus, I have chosen the qualitative research as the type of the research. Here, it’s important to point out that both the methods (will be presented in another sub-section) and the chosen paradigm fit very well with the research type. On this point Mayers (1997, p.2) wrote: “qualitative research involves the use of qualitative data, such as interviews, documents, and participant observation data, to understand and explain social phenomena”

5.2. Methods/Techniques for Data Collection and Analysis

5.2.2. Sampling Method

Having a good picture about the sample of the empirical study is one of the key elements to obtain useful outcomes answering the research questions. Many factors can drive a study to a certain conclusion and may have a major effect on the result, like targeting a particular group having a similar education level or people having the same interest, nationality, age, gender, or even cultural behavior. On the other hand, “the cost of studying an entire population to answer a specific question is usually prohibitive in terms of time, money and resources. Therefore, a subset of subjects representative of a given population must be selected” (Lunsford, et al, 1995, p.105). Based on the above, putting a strategy to identify the best sampling method that fit well with the thesis goals is significantly imperative. Thus, a literature review about qualitative evaluation, sampling in qualitative research and qualitative methods has been made in order to address my concerns. A book written in 2002 by Michael Quinn Patton which is qualitative research & evaluation methods comes to answer my questions and gives me guidelines for selecting the appropriate sampling method. Patton determines 14 strategies for all purposeful sampling (see Appendix A), and creates a QUALITATIVE EVALUATION CHECKLIST. The aim of this checklist is “to guide evaluators in determining when qualitative methods are appropriate for an evaluative inquiry and factors to consider, to select qualitative approaches that are particularly appropriate for a given evaluation’s expected uses and answer the evaluation’s questions” (Patton, 2003, p.1). This checklist helps me in the empirical setting by giving advices, options and recommendations in selecting the qualitative
approach (sampling method), and collecting high quality and credible qualitative data. All in all, this checklist benefits the thesis by making the empirical study structured in a based-formative way.

Diving deeper, maximum variation has been chosen to be the sampling strategy of my study (see Appendix A). Mainly because, among the 14 various strategies that Patton defines, maximum variation sampling comes to be the closest one meets my expectations about the selective sample. According to Patton (1990, p.170), maximum variation sampling aims to “capture and describe the central themes or principal outcomes that cut across a great deal of participant or program variation”, he also added, this strategy “would not be attempting to generalize findings to all people or all groups but would be looking for information that elucidates programmatic variation and significant common patterns within that variation”. From above perspective and to apply maximum variation strategy in a purposeful sampling, 3 key things need to be identified. First, the purposeful sample, which is Linnaeus university students who have a Facebook account, this selection has been made eventually based upon the key identifications of the sampling method. Besides, being a student at the university gaining me access to both individuals and facilities where I can carry out the data collection in my empirical study. Second, selecting the characteristic of variation, diversity is the essential criteria for constructing the sample of my study, because the way individuals perceive privacy on Facebook is tightly related to how they understand the concept in general which could be totally different from culture to another as we’ve discussed previously. So, multi-nationalities or multi-cultural behaviors will be the dimension of variation of the sampling units. Lastly, the common pattern within that variation, which is all interviews and survey participants have a FB account and a good educational level.

From theory to practice, the interview participants have been chosen based on the three following conditions:

- The participant must be a student at Linnaeus university who has a FB account
- The participants should not be selected from a single country, in order to represent the characteristic and dimension of variation described above.
- No personal relationship with the interviewees, to avoid any negative impact on the interview process.

Based on the above, I have communicated with friends and colleagues at Linnaeus University to recommend some candidates who fulfil the selected criteria.

5.2.2. Interviews

The purpose of interviews was most importantly enabling and encouraging a meaningful conversation with the participants in order to reflect individuals’ perspective about privacy and surveillance on social networks generally and Facebook particularly. The interviews were based on a structured interview that aims to present exactly the same questions designed in the interview guide to make sure all given answers can be reliably aggregated. However, some of the questions had an open-ended form to allow a less restricted conversation with the interviewee while the rest were close-ended ones (see appendix B).
The interviews were individual face-to-face ones, and the location was chosen by the interviewee ‘most of the time’, to ensure that s/he is comfortable during the interview session – out of 9 interviews, 4 were held in the participants’ rooms, 3 at the university library and the rest in open areas inside Linnaeus campus –. The estimated time of the interview was 45 to 60 minutes, and the table below shows the diversity in gender, age and nationality among the interview participants which meet the characteristic of variation of the selected purposeful sample.

<table>
<thead>
<tr>
<th>Region</th>
<th>Gender</th>
<th>Age</th>
<th>Nationality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Europe</td>
<td>Female</td>
<td>22</td>
<td>Swedish</td>
</tr>
<tr>
<td></td>
<td>Male</td>
<td>23</td>
<td>Swedish</td>
</tr>
<tr>
<td></td>
<td>Male</td>
<td>21</td>
<td>German</td>
</tr>
<tr>
<td>Middle East</td>
<td>2 Male</td>
<td>21, 29</td>
<td>Syrian</td>
</tr>
<tr>
<td></td>
<td>Male</td>
<td>26</td>
<td>Palestinian</td>
</tr>
<tr>
<td>Africa</td>
<td>Male</td>
<td>27</td>
<td>Zambian</td>
</tr>
<tr>
<td></td>
<td>Female</td>
<td>25</td>
<td>Rwandan</td>
</tr>
<tr>
<td>Asia</td>
<td>Male</td>
<td>19</td>
<td>Chinese</td>
</tr>
<tr>
<td></td>
<td>Female</td>
<td>22</td>
<td>Bengali</td>
</tr>
</tbody>
</table>

*Figure 3- Interview Participants*

Following the interview guide (see appendix B) which designed to ensure that all questions set in one place and avoid any kind of missing information, I divided the conversation with the interviewee into 3 main parts. The first, is an introduction about the thesis and thesis questions, followed by a clarification about what kind of information I’m gathering, and how I would use the collected data. Then, couple of minutes more would be spent explaining the ethical considerations that has been defined widely in the up-next section based on Patton (2003) checklist and his recommendations about the basic ethical issues should be considered in an interview. Last in the first part, asking the interviewee if s/he has any inquiry about what have being said and take a permission to start asking the questions. The second part is an interactive session where all questions have been prepared in the interview guide are being asked, however, the participant can refuse to answer any question could make him uncomfortable and without giving any excuse or a reason. The final part of the interview is formed to get the participant’s observations and comments on the interview, determine if there is any given information should be out of the record and thank him/her for participating in my study.

5.2.3. Survey

I felt, having interviews with only 9 participants wasn’t enough to draw up a clear picture answering the thesis questions. I also felt more opinions can be taken into consideration to accurately represent the larger group which is Linnaeus university students. Therefore, I decided to spread out a survey in order to reach and engage more people in my study.

I have chosen an online web questionnaire instead of paper-based survey as it comes with several advantages in terms of speed, cost, flexibility, appearance and usability (Lumsden, 2005). For instance, “delivery is faster, responses are received more
quickly, and data collection can be automated or accelerated” (Lumsden, 2005). In fact, gaining the most benefit of the online questionnaire requires having a well-structured form of it, therefore, I decided to include only close-ended questions to the questionnaire, because, “close-ended questions in general yield higher percentages than open-ended question for answers that are identical in both question forms” (Reja, et al, 2003, p.159). In addition, the open-ended questions produce a much more diverse set of answers and the probability of having missing answers is higher, besides, the process of coding and classifying the answers much harder. In fact, having the interviews done in an early stage helped me a lot to reform the questions and figure out the options and types of answers I need to consider in the survey multiple-choice questions. At the end, I designed a survey that fits well with the thesis goal and takes around 5 minutes from participant to fill it out.

Going further to determine the sample size, I’ve done an investigation about the average number of students participated in similar surveys tested by Linnaeus students. This investigation helped me anticipating the amount of responses may I get through the online questionnaire, plus, gave me lessons from previous experiences. Some PhD students at Linnaeus affirm that the maximum number of responses they’ve gotten through such a survey doesn’t exceed 60-90, however, that’s mostly related to the way they’re targeting people and how they distribute the survey, as well as, how long it is. 50 records was a roughly estimation about the number of students could fill out my survey, that’s if I follow the usual ways in spreading it out – posts on FB groups belong to Linnaeus students, and a personal communication with friends asking them for recommendations –.

I have used two ways to distribute the questionnaire and collect data, the first one was through the FB groups belong to Linnaeus students while the second one by approaching students at Linnaeus university library and asking them to fill out the online form which was accessible through an IPad device, in both ways, filling out the survey was completely voluntary. Eventually, 59 participants from 22 countries have filled out the survey – It’s important to point out that as I couldn’t completely control the flow of the survey on the FB groups, I didn’t have control of who has answered, nor how many declined to answer, over and above, I couldn’t 100% confirm that all participants in my questionnaire were Linnaeus students –.

5.2.4. Why Two Methods

Two methods have been used for collecting data, interviews and survey. Mainly because, having interviews with not small number of students is time consuming, beside the efforts needed to find an appropriate time and place for each participant. Therefore, the survey has helped to collect data from more students, especially those who are hard to reach in person. On the other hand, Interviews allowed me to gather a wide range of open-ended qualitative data, and obtain detailed information about personal opinions, feelings, and perceptions. While the survey gave an extra feature to the data analysis which is, using the build-in tools to make categorization and comparison.
5.2.5. Data & Analysis

After applying the methods (interview & survey) that have been chosen in my empirical study and in order to be able to present the data have been gathered effectively, I divide the data analysis into two separate parts, one for analyzing the interviews and the second one for analyzing the survey. The main reason behind this separation is actually to bring order and understanding to the qualitative data have been collected through the interviews and design a statistical view through the information gathered by the survey. Diving deeper, having open-ended questions in the interviews (see Appendix B) gave me the chance to have a dialogue with the interviewees which turns out to have more textual data, while the answers I got from the survey were short and controlled as most of them were based on multiple choice questions (see Appendix C).

Finding a good approach for data analysis was a struggle for me due to the luck of experience in the qualitative research. In the beginning, I chose to go with the three Cs approach (the three Cs refers to Coding, Categories, and Concepts) developed by Lichtman (2013). According to Lichtman’s recommendations, 6 steps have to be performed as follows:

- Step 1. Initial Coding. Going from responses to summary ideas of the responses
- Step 2. Revisiting initial coding
- Step 3. Developing an initial list of categories
- Step 4. Modifying initial list based on additional rereading
- Step 5. Revisiting your categories and subcategories
- Step 6. Moving from categories to concepts. (2013, p.252)

In practice, I didn't follow the steps and found myself making adjustments in the process to adapt it with my way of thinking of implementing data analysis, therefore, I decided to change the previous approach seeking resilience and flexibility.

Thematic analysis was a good technique to simplify the process and get a meaning from data have been gathered. According to Boyatzis (1998), thematic analysis is a process for encoding qualitative information, it’s not a separate method, such as ethnography or grounded theory, but something to be used to assist the research in the search for insight. He continued, the objective of the method is to develop thematic codes with which to observe and perceive people, groups, organizations, cultures or events. Since theme is the fundamental concept of thematic analysis it’s important at this point to give more clarification around it. Braun and Clarke (2006, p.10) defines what count as a theme saying, “a theme captures something important about the data in relation to the research question, and represents some level of patterned response or meaning within the data set”. Furthermore, they clarified the two primary ways that scholars followed identifying themes or patterns within data, inductive or ‘bottom up’ way, and deductive or ‘top down’ way. According to them (2006, p.12) “inductive analysis is a process of coding the data without trying to fit it into a pre-existing coding frame, or the researcher’s analytic preconceptions”, in contrast, a deductive thematic analysis “would tend to be driven by the researcher’s theoretical or analytic interest in the area, and is thus more explicitly analyst-driven”. It’s important to point out that in thematic analysis there is no much restrictions on ways of data analysis, otherwise, recommendations and guidelines. However, Braun and Clarke (2006)
developed a step-by-step guide for doing thematic analysis and the table below summarizes their recommendations.

<table>
<thead>
<tr>
<th>Phase</th>
<th>Description of the process</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Familiarising yourself with your data:</td>
<td>Transcribing data (if necessary), reading and re-reading the data, noting down initial ideas.</td>
</tr>
<tr>
<td>2. Generating initial codes:</td>
<td>Coding interesting features of the data in a systematic fashion across the entire data set, collating data relevant to each code.</td>
</tr>
<tr>
<td>3. Searching for themes:</td>
<td>Collating codes into potential themes, gathering all data relevant to each potential theme.</td>
</tr>
<tr>
<td>4. Reviewing themes:</td>
<td>Checking in the themes work in relation to the coded extracts (Level 1) and the entire data set (Level 2), generating a thematic ‘map’ of the analysis.</td>
</tr>
<tr>
<td>5. Defining and naming themes:</td>
<td>Ongoing analysis to refine the specifics of each theme, and the overall story the analysis tells; generating clear definitions and names for each theme.</td>
</tr>
<tr>
<td>6. Producing the report:</td>
<td>The final opportunity for analysis. Selection of vivid, compelling extract examples, final analysis of selected extracts, relating back of the analysis to the research question and literature, producing a scholarly report of the analysis.</td>
</tr>
</tbody>
</table>

Following Braun and Clarke recommendations, I’ve started with the first two phases to generate codes from the recorded interviews, at the end of listening to all records, each interview had a transcript that includes all questions and answers have been collected. Then, revisiting the initial codes (transcripts) is performed looking for patterns and themes that connect or relate participants’ answers to each other and to the thesis questions. In this stage, notes have been taken to map codes from different transcripts as a step to generate themes. After that, I distributed codes based on notes and mapping have been done earlier, here, initial themes started to appear, and codes have been minimized to have only those are related. At the end of this process, several themes emerged into three areas of interest that are headlines in the thesis, which are: Data collection over SNs, privacy and privacy protection over SNs, and surveillance on SNs. Each one of those headlines has discussed participants’ answers to certain questions in the interview guide, and some interpretations made of connecting
answers from different questions. At the end, the final report has been produced and fully described in Analyzing Interviews section.

5.3. Validity and Reliability

Patton (1990) states that validity and reliability are two factors which any qualitative researcher should be concerned about while designing a study, analyzing results and judging the quality of the study. In rough aspect, validity refers to the extent of which a test measures what we actually wish to measure (Blumberg et al., 2005), in simple terms, Validity of research work can be explained as an extent at which requirements of scientific research method have been followed generating research findings. In this thesis, it will be difficult to know for certain if the research conducted is valid for the research questions, mainly because, there is lack of qualitative academic resources discussing surveillance on social networks, moreover, some assumptions and conclusions in the thesis have been made based on the current terms and data policy performed on Facebook, thus, changes on FB terms especially the statements have been discussed could affect the validity of the thesis. Talking about reliability, Blumberg et al. (2005) explained the term as a measurement that supplies consistent results. By means, the ability to obtain same or closely similar results using the same instruments more than one time. In this matter, the majority of the data collection in the literature review is gathered from established international journal, previous academic researches, and recorded interviews with experts in the field, and it’s therefore a reason to believe that the data gathered is reliable. However, the potential issues of reliability in the thesis are mentioned and discussed in the areas need to be considered.

5.4. Ethical Consideration

Ethical considerations in data collection can be identified as one of the most critical parts in a research or a dissertations work. According to Bryman and Bell (2007), principles of ethical considerations must have been always considered when planning any type of data collection, therefore, in order to address the ethical challenges in the qualitative study, I followed some suggestions from Patton (2003) checklist in the part concerned about ethical issues in a qualitative research. Below is a list of the ethical considerations that have been determined before proceeding the interviews and testing the survey.

- **Explaining purpose**: Before starting the interview or filling out the survey, the participants will have a short description about the thesis study to understand what they are involving in, moreover, the participants will also get information about the methods I’m using and my intention to use their answers and responses to get outcomes from the study.

- **Promises & reciprocity**: High promises won’t be given out as I am not sure how much my thesis study will benefit the community. However, the main objectives of the thesis will be introduced to the interview and survey participants. *No high promises will be given out to the interviewees or survey participants unless I am sure to keep them.*

- **Confidentiality**: Both the interviewees and the survey participants will be informed that, no contact details about them will be given out. The
participants won’t be named in the thesis or in future publications of the results, if any. The information collected from the interview will be used under nationality, age and gender. Furthermore, if the interviewee accepts to voice record the interview, information about who can have access to the record and when the record will be destroyed will be presented in the interview guide (see appendix B). On the other hand, the survey will be designed to be anonymous one (see appendix C), besides, the IP track feature will be disabled in the survey to ensure the anonymity of the participants.

- **Informed Consent:** The interview participants will be asked to give a verbal informed consent after being given information about the study, and the following statement will be proposed to each participant, “proceeding with the interview, means, you (the participant) give me (the interviewer) an informed verbal consent to use the information you provide to serve my academic works with respect to what have been described about the ethical considerations in my study” (Interview Guide, appendix B). While the following statement will be included in the survey “By clicking Submit/Done you agree to participate in this anonymous survey and you give the researcher an informed consent to use the information you provided to serve his academic works” (appendix C).

- **Data collection boundaries:** All the survey questions will be optional to answer and I won’t force the participant to answer any question included in the survey. Regarding the interview, in the ethical considerations’ section in the interview guide the participants will be aware that, “the interviewee has the right not to answer a particular question or to terminate the interview altogether without giving any explanation”, also “if the interviewee becomes distressed, the interview will be abandoned” (Interview Guide, appendix B). However, I won’t push hard to get data from the interviewees, I will be open to have a discussion on any question but without going out of the scope of the thesis.

- **Interviewees have to be comfortable with the location of the interview, therefore, (public/private) alternatives will be suggested to bring their comfort.**

- **Advice:** Professor Sisse Finken, who’s an expert in Ethnographic studies, Design and Displacements, Interaction Design and Design Research, she was the counselor on matters of ethics in data collection during my study.
6. Empirical Findings

In this section, I will present all findings based on my research methodologies and strategies as introduced previously. The results are based on two main research methods that are survey and structured interviews. Moreover, the data analysis is relied on the material of all interview transcripts and survey responses that were provided by the participants. As described, the research objectives are students at Linnaeus University in Sweden, and all participants have been selected with the balance between cultural and educational background. As agreed with the participants, they are anonymous in my research and will be named by gender, age and nationality, for example: 21 years old Swedish female, to protect participants’ privacy and respect the principle of research ethics.

6.1. Analyzing Interviews

The interviews didn’t only provide me with information about what the participants think about privacy and surveillance over social networks but also gave me more information on how they behave to protect their online privacy, therefore, the data presented in this section will be divided into three subsections each presented by a title. Before moving ahead to the data analysis, I just want to highlight that all the participants were having a Facebook account, therefore all the questions included in the interview guide have been asked.

Data collection over social networks

During the interviews, the participants were asked about their knowledge about data collection on social networks, how they will react if social networks announce that they will sell some of their users’ information for special agencies, and if they have ever read the terms and data policy on social networks they use. The reason behind these questions was to understand how much individuals aware about data collection and terms over social platforms which will be mapped latter on with their behavior to protect their privacy online. The majority of participants (6/9) had a little knowledge about data collection on social networks, some of them were familiar with the term (data collection), the others had a little information about the process. One of the participants (male 19, Chinese) said: “well, it seems they gather information to develop the platforms”. The 22 years old Bengali female expressed that she had read once about data collection over social networks, she understood that social websites collect users’ information to improve the services and to give a better performance for users, she followed “that’s all I know”. The second part of the participants (3/9) they were highly informed about the concept, not only that but they were also knowledgeable about data policies on some social platforms. The three participants shared a common factor make them aware about data collection over SNs, which is, they all have experienced certain event which encouraged them to read more about the subject. The 26 years old Palestinian male expressed what motivated him to search more about Facebook data collection as follows:

couple of years ago I had no idea about online data collection but after a specific occasion I did a research … what made me curious about my online information, I was using a search engine looking for online retailers to buy a shoes, I found a
one and I made my order, couple of days later I found a targeting ads on my FB news feed showing me the same shoes I bought.

The 21 years old German male had a totally different story, what actually drove him to read twitter’s data policy was an incident happened with his girlfriend, when someone stole her online identity and starts to publish some nasty tweets on the fake account. He summarized the story by saying:

We have experienced online identity theft but that didn’t last long, we reported the incident and the fake account closed down… the good side of the story, right now we’re aware about privacy and data policies on Facebook and Twitter.

The three participants had a good knowledge about the massive data collection on Facebook, they elaborated by giving some examples, e.g. targeting advertisements, building huge data warehouses to analyze the data has being gathered, and collecting data to improve the platform services.

I wanted to know how the participants will answer and react for a certain given scenario related to data collection on Facebook, I therefore followed up with the next question, “if Facebook said publicly: we will sell some of our users’ information to some corporations or agencies, will you accept that?” (Interview Guide, appendix B). The majority of the participants (7/9) answered immediately, NO I won’t. Another response was, “OK, I don’t put much information on Facebook” (female 22, Swedish) while the 21 years old Syrian male said: “probably yes, if they give information about the type of data and to whom exactly”. The previous question had a second part in case the interviewee answered by No, “So will you deactivate your account?” Surprisingly, even though the vast majority in the first part of the question answered No, they were irresolute and they haven’t had a quick answer to the second part. It seems when it comes to communication with their network, decision is not easy to make. The 29 years old Syrian male expressed that he has huge personal information in his Facebook profile, he also highlighted that Facebook is the main stream he uses to communicate with his network and family members. On the opposite side, the 21 years old German male said: “I will use another website”. At the end, four out of nine decided to deactivate their account if that scenario happened, three participants didn’t decide and two would keep using Facebook in such a case.

In line with the statistics mentioned before regarding the most social network platforms used among teens and adults, it becomes clear that Facebook is an important platform that individuals use to communicate with their network. I have to admit I wasn’t expecting that the participants will compromise their personal information in order to keep in contact with their FB friends. Eventually, I couldn’t generalize that for all the interviewees but a not inconsiderable proportion have thought twice before giving out an answer on the given scenario.

Going back to the scope of the section, the participants have been asked if they have read the terms and policies on Facebook or any other social network they have an account on. The three participants who were knowledgeable about data collection on social networks confirmed that they have read both the terms and the data policy. The 22 years old Swedish female said: “that was exhausting, I couldn’t believe how long it is”. The other participants were barely knowledgeable about the terms and conditions
on the social platforms they use, “I didn’t read the terms on Facebook or Instagram but I know little from articles I read talking about this topic” (Female 25, Rwandan). Six out of nine participants have confirmed that they didn’t read the terms or the data policy neither on Facebook nor any other social network they use, but some of them were aware about certain regulations applied on social networks through newspaper, articles, YouTube videos or other resources.

**Privacy and privacy protection over social network, especially Facebook.**

During the interviews it became clear that the participants couldn’t find easily a definition for privacy on social networks. That being said, “How can you define privacy on social networks?” (Interview Guide, appendix B) The participants gave different answers for this question, some went to describe privacy as a concept then trying to find a delineation for privacy over social networks, while others were circulating around informational privacy. In line with what I have discussed in chapter 1, it seems like the participants made their definition of privacy in ways dictated by upbringing, experience and culture. Some will argue why I have mentioned the nationality of the participants in my study, it was important for me to select a list of participants sharing different cultures and traditions, where I can get ‘potentially’ different answers and map afterward how they present the concept putting into consideration their cultural perspectives. Eventually, all the participants have agreed that “privacy is freedom from interference or intrusion, the right to be let alone” (Warren and Brandeis, 1890, p.193), but when it came to informational privacy, the participants showed different responses. One of the participants said: “social networks is built to let people know more about each other, it’s not only to communicate” (21 male, Chinese), few of the participants had the same impression but in different phrases, the 29 years old Syrian male added “I often post personal status on my Facebook account but never thought that type of information shouldn’t be posted”.

The concept itself ‘privacy on social networks’ was not easy to cover in few words, therefore, the majority of the participants found a problem to get a clear explanation, I could interpret that, the *privacy norms* are changeable with time by means you couldn’t determine a typical form of the concept and say it will stay be usable for several generations. The daily changes occurring in social networks with the increased automated services there, encourage users of social networks to become more open to provide more information to get a better service. However, one of the participants concluded that privacy means, having control over certain type of information and putting boundaries between share or not to share (26 male, Palestinian), while the 21 years old German male gave his view as “don’t take what I don’t want to give you, this is privacy for me”. Moving ahead to the second part of the question, “Do you think you’re sharing the same definition with your culture?” Some of the participants said: yes, I guess we share the same view, while the rest didn’t say that explicitly. Alongside with what the participants expressed and based on my observation from the question that has been asked about the type of personal information that the participants share on Facebook, it looks as if the fundamental ideas about privacy differ among regions. For instance, the interviewees from Eastern cultures tended to share and post more personal information on their Facebook profiles than the interviewees from Western cultures, even though both sides didn’t know all their Facebook friends. Answering the previous question only the 23 years old Swedish male had different opinion, “well, I guess I am not a typical Swedish when it comes to
privacy online”, this participant had acknowledged that he is posting personal photos and videos regularly on his Facebook.

When asked about the ways that the participants protect their privacy on social networks, most of the participants (7/9) gave examples could be categorized as having a good privacy setting, controlling who have access to certain posts or managing friends list. Here, I’ll discuss the participants’ opinion on this point then I’ll continue with the other two participants who have different answers. The 27 years old Zambian male expressed that he has a good privacy setting, he’s limiting who can see his information, and he also limits the audience from sharing his posts. In a similar action, the 21 years old Swedish female was more focusing into classifying her friends into close friends, family members, and so on, according to the post she wants to publish she identifies who can see it. However, the rest of the answers were slightly different but still having the main focus on managing the targeted audience, restricted privacy settings and controlling who can have access to photos and videos. On the other hand, only two participants have completely different answers. “it’s not about directing the flow of the information, it’s more about limiting the amount of data need to be published” he continued “any system has a vulnerability and I don’t guaranty that hackers or bad guys can’t have access to my data on the internet in general” (21 male, German), this participant was pretty much aware of security threats on the internet and his girlfriend’s experience with online identity theft let him more concerns about publishing information online. In a similar perspective, the 26 years old Palestinian male has expressed his concerns about privacy on social networks by saying “I was oversharing my information on Facebook but not anymore … now I am concerned about my information on social networks, so I am not publishing or sharing that much of personal information anymore”. Those two participants had concerns not only about who’s seeing their information on social networks but also who can access their data, moreover, both participants have showed that the best to protect privacy on social network is by publishing/uploading less information. It seems they have this perspective the less you share the more secure you are.

Last point I want to highlight here before moving ahead to the last subsection in the interview data analysis, No one of the participants directly showed concerns about data collection applied on social networks in terms of privacy protection, taking into consideration that they have been asked previously a question related to data collection on social networks.

**Surveillance over social networks**

During the interview the participants have been asked to give their opinion on, whether or not they think that governments do surveillance on social networks, also they have been questioned if they accept such an action and support governments in their potential endeavors. The participants expressed their mixed feelings towards governments surveillance on social networks, they were skeptical and few of them were able to give a direct answer, generally, no clear answers have been presented as there are lack of information in the given subject and usually the public don’t get that kind of information from their governments. So, when some of the participants answered by ‘yes’ they were counting on the leaks they have read about surveillance on social networks, or they were relying on national/international debates they have watched.
The 19 years old Chinese male gave a thought that some governments could have a surveillance program on social media, it’s a possibility but “no one knows”, two other participants from Middle East were inclined to say that some governments apply surveillance on SNs, the 21 years old Syrian male said “I don’t trust some governments, they are always some secret programs running on … I would say governments are monitoring social networks”. Some other participants were more into the following statement I don’t think governments do monitor social networks while the rest had no idea and no clue. The following list shows what view the participants tended to have in mind.

(3/9) some governments do surveillance on social networks.
(2/9) governments don’t monitor users’ activities on social networks.
(4/9) have no idea.

When it came to the next question, “do you agree that governments do surveillance on social networks to protect national security or control Cyber-bullying cases?” (Interview Guide, appendix B). The participants were divided into two groups, one group (2/9) supported that idea, while (6/9) did not. One of the participants justified his answer by saying “we have bad guys, trying to spread out hate, violence and terrorism … we need to fight those people and stop their psychopath” (25 male, Zambian), on the opposite side the 23 years old Swedish male has expressed his view as “I 100% disagree with such an action for several reasons, … having a surveillance program on social networks means all users will be survived and no one could be out of the program” he also added “we can protect ourselves by having surveillance on specific target of people who could be welling to do criminal activities”, this participant and some others who disagreed with the given case, they were worry about their privacy if governments do surveillance over social networks because for some this action could lead to privacy violations.

6.2. Analyzing Survey

The data collected from the survey will be presented in statistical figures and charts to illustrate the participants’ responses to questions have been asked. In fact, using SurveyMonkey as a platform to test the questionnaire helped a lot in the analysis phase as the platform provides a set of tools to filter, analyze and represent the data collected. The data analysis has been handled by the built-in tools in the platform, and there has been no need to use other techniques to perform the analysis.

The survey data analysis will be divided into parts, and each one will address an angle from the thesis questions. Some of the survey questions will be discussed together and some results or reflections will be drawn by mapping answers from multiple questions.

Data collection over social networks

The participants have been asked if they have ever read Facebook terms and data policy. All the participants have answered this question and the result was (39/59) participants haven’t read the terms, while almost 34% have read it, keeping into consideration that all the participants have a Facebook account and the question wasn’t asking if they have read the terms when they signed up on Facebook. Below
Figure shows the statistical result of the participants’ responses answering above question.

![Bar chart showing Yes and No responses](image)

Figure 5- Participants have read FB terms

I wanted to know more from the participants who answered by yes, specifically, the amount has been read from the terms and policy. Thus, the followed question comes to give me that kind of information.
From the above figure we can notice that even though (20/59) of the participants have acknowledged that they have read the terms and data policy but there is still a proportion of them (8/20) they just randomly surfed the content while the rest of the participants showed that they either read all of the content, most of it or a certain part. In the next chapter (discussion) I’ll give my reflection on this result comparing what the participants in the interview said with what the participants in the survey answered.

In order to understand how much the participants aware of the terms and data policy in Facebook, they have also been asked about a specific clause included in the Facebook terms page. The question formed according to Likert scale as follows: On a scale from 1 to 5 (1 is strongly disagree and 5 strongly agree) determine your opinion on the following statement:
Running a filter on “have you ever read Facebook terms & data policy?” and responses from above statement, I found out that from 28 participants who have been aware about the permission they gave to Facebook when they signed up, only 13 of them have read the terms and data policy. On the other hand, 15 participants have been aware about above permission, but they have not read the terms and data policy on the platform. Apparently, even though 66% of the participants haven’t ever read Facebook terms and data policy, but that doesn’t mean they have no knowledge about certain rules and clauses included in the terms.

In line with the title of this subsection, another question has been included in the survey to get the participants’ opinion on a given viewpoint, the question also designed according to Likert scale as follows.

On a scale from 1 to 5 (1 is strongly disagree and 5 strongly agree) determine your opinion on the following statement:

As one can see from the figure, there are 76% of the participants (45/59) they do believe that social networks sell users information for their own benefits, 11.86% of the participants (7/59) they disagree with the given thought, while the rest of the participants (7) preferred to stay in the gray area. A filter on the result from this question and have you ever read FB terms and data policy, shows that more than half of the participants who read the terms and data policy believe that social networks sell users information (see figure 13).
Please note that Q4 refers to have you ever read Facebook term & data policy?

Going back to the descriptive study which talks about FB terms and data policy, there is no clear statement says that FB sell users’ information and in the same time there is also no statement in the terms and data policy can invalidate that. However, some more clarifications will be presented in the discussion chapter to settle the debate in this matter.

Privacy over social networks especially on Facebook.

In order to understand participants’ behavior on FB in terms of protecting their informational privacy, two questions have been asked to the participants. The first one asked if they share any kind of personal information on their FB profiles, and the second one asked if they know all their FB friends. In first question I didn’t mention the type of information as I’ve found through the interviews, what can be defined as personal for someone might be not for another. The following figure counts the answers of both questions.

As can see, (40/57) of the participants share personal information on their FB profiles – whatever the term personal means to them – while only (9/57) agreed with the given sentence and admitted that they don’t share any kind of personal information on their FB account. Moving to the second sentence in the table, 48% of 58 participants they don’t know all their friends on FB, which means they have some ‘strange’ people on their friends list and those can properly see the information shared with actual friends. On the other hand, around 33% of the participants know all friends they have on FB. Apparently, 22 participants were skeptical and didn’t decide, which means in my opinion, there is a high possibility among those 22 participants to have some strange friends in the list.

In connection to privacy protection on FB, the participants have been answered if they have a good privacy setting on their profile or not. As a result, more than half of the participants who answered the question (31/58) confirmed that they have good
privacy setting on their profiles, around 26% were skeptical and the rest they believe they don’t have. At first glance, we might say that the users who have good privacy setting on FB there are concerned about their information disclosure and they already took a step in managing their information flow, but could we say having a restricted privacy setting means a good privacy on FB. Here, I wanted to know more about the participants, therefore, I did a comparison with other question they answered and I got the following unexpected result. From 31 participants who have good privacy setting, almost 1/3 of them they don’t know all their friends on FB. Getting this result affirms that many factors should be taken into consideration when discussing privacy on social networks and information management is just a factor but it’s not the whole.

Before moving to the last subsection in analyzing the survey responses, one last statistic should be mentioned here. In the survey, the participants have been questioned if they have concerns about their privacy on social networks, and the result shows that more than 71% they do have concerns, while only 13.5% they don’t.

<table>
<thead>
<tr>
<th>I have concerns about my privacy on Social Networks</th>
<th>Strongly disagree</th>
<th>Disagree</th>
<th>Undecided</th>
<th>Agree</th>
<th>Strongly agree</th>
<th>Total</th>
<th>Weighted Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.06%</td>
<td>8.47%</td>
<td>15.25%</td>
<td>30.51%</td>
<td>40.60%</td>
<td>59</td>
<td>3.93</td>
<td></td>
</tr>
</tbody>
</table>

Figure 11- Concerns about privacy in SN

**Surveillance over social networks**

This subsection will present the participants responses on two given scenarios. The first one formed to see if the participants accept that governments and special agencies watch their activities on SNs, and the second one, came to ask if they support surveillance programs in order to control cyber-crimes and protect national security.

<table>
<thead>
<tr>
<th>I have nothing to hide; government and special agencies can have a look to my activities on social network.</th>
<th>Strongly disagree</th>
<th>Disagree</th>
<th>Undecided</th>
<th>Agree</th>
<th>Strongly agree</th>
<th>Total</th>
<th>Weighted Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>23.73%</td>
<td>16.95%</td>
<td>22.03%</td>
<td>23.73%</td>
<td>13.66%</td>
<td>59</td>
<td>2.66</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Governments should do surveillance on social Networks to control/avoid cyber-crimes and terrorist attacks</th>
<th>Strongly disagree</th>
<th>Disagree</th>
<th>Undecided</th>
<th>Agree</th>
<th>Strongly agree</th>
<th>Total</th>
<th>Weighted Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>23.73%</td>
<td>20.34%</td>
<td>20.34%</td>
<td>23.73%</td>
<td>11.66%</td>
<td>59</td>
<td>2.80</td>
<td></td>
</tr>
</tbody>
</table>

Figure 12- Participants’ opinion about surveillance on SN
As can see, almost similar percentages have been recorded from both sentences. Around 42% of the participants in average don’t accept that governments/special agencies watch their activities on SNs and don’t support such actions, while 36% of the participants have no problem if governments/special agencies watch their activities on SNs, and they support government surveillance on SNs.

6.3. Summary of the Critical Findings

- Most of the interview participants showed lack of knowledge about data collection on SNs, some were familiar with the term but only few of them were strongly aware about the process of data collection on SNs.
- Most of the survey participants have not read FB terms and data policy. Only 34% of them have read the terms and data policy, and the majority of this percentage read only certain part or randomly surfed.
- 76% of the survey participants believe that social networks sell users’ information to other organizations and special agencies for own benefits.
- Most of the interview participants protect their informational privacy on SNs by having good privacy settings, controlling who have access to certain posts or managing friends list.
- Small percentage of the survey participants (13.5%) don’t have concerns about their privacy of SNs, while the majority they have.
- 70% of the survey participants share personal information on their FB profile, around 48% of the participants don’t know all their friends on FB, and 19% aren’t sure.
- Around 42% of the survey participants don’t accept that governments/agencies watch their activities on SNs and don’t support such actions.
7. Discussion

The discussion section will be divided into three subsections. First, a discussion will be carried out based on the findings and results that are presented above. I will present the discussion through my own reflection and understanding of what the findings have shown and what it means for the study. Also some of the results of the empirical findings will be presented in connection to the literature review and previous researches have been presented. Second, based on the empirical findings, the discussion in the literature review and the study on FB terms and data policy, I will further present suggestion of possible approaches to enhance individuals’ privacy. Thirdly and last, I will point out some suggestions that SNs and governments could perform to raise privacy protection and build trust with users of social networks.

6.1. Reflection and interpretation on presented results

Privacy on social networks

As we’ve seen in the interview analysis the participants couldn’t easily define privacy on social networks, it seems when the two terms (privacy, social networks) combined together the concept becomes more descriptive, probably because there are no ideal principles have been set and implemented in social networking, over and above the uncertainty and ambiguity about data collection and information flow on SM. In fact, the actual practice of social networking shows that there are high concerns about privacy on SNs, at least in mind of the participants of my study. As the statistical figure presented previously more than 71% of the survey participants have concerns about their privacy on SNs, but where these concerns come from.

Many factors play a role when we are talking about privacy concerns on social networks. First and foremost, **ambiguity in some of the terms and data policy.** As being showed in above study the one conducted on FB terms and data policy it becomes clear that there are many vague areas in the terms of FB. For instance, the permission that FB grants itself to use the users IP content and the way it uses them. This sort of uncertainty could explain users’ thoughts about selling their personal information to agencies and third-party partners, 76% of the survey participants have acknowledged that they do believe that social networks sell users’ information for their own benefits, while only 11.8% doesn’t. Doing further investigation to settle the debate in this matter, Facebook answered that in its help center.

Does Facebook sell my information?
No, we don't sell any of your information to anyone and we never will.(Facebook)

In privacy law, terms and data policy on social networks is a legal document signed between the two parties (the platform and the user) which provides principles & policies to be guidance of the ways a party gathers, uses, controls, discloses, and manages a client's data, thus, what’s included in the "contract" should be clear for both sides. In fact, the terms and data policy usually include variety of statements that legalize the relationship between different parties, therefore, we significantly need
demystified information about how SNs deal with users’ data in order to build *transparency and trust* between all parties.

Second of all, **awareness about information management and information flow.** As discussed in the literature review “privacy is the control we have over information about ourselves” (Fried, 1984, p.209), also it is the control of accessing personal information (Moor, 1989). Based on my empirical study I find out that the participants attitude towards information management and information flow is more focusing onto managing the account privacy settings while many other factors have an impact but not much taken into consideration. For instance, 1/3 of the participants who have good privacy settings they don’t know all their friends on FB, which obviously makes information posted by these participants available to some unknown friends. Keeping in mind that most of the users on SNs tend to share a variety of personal information – as seen in the literature review – Clearly, privacy setting is just an approach to restrict shared content but it’s not everything to control information flow.

Thirdly, **awareness about SNs data collection.** Through the interviews I realized that most of the participants aren’t much knowledgeable about data collection on SNs, the term itself is familiar for all of them but there is no clear view about the amount of information that SNs can gather about/from users, one of the reasons behind that, 66.1% of the survey participants haven’t read FB terms & data policy. “Does it make a difference if I read it or not” the 19 years old Chinese participant showing his carelessness to read the terms & data policy of FB or other SN has an account on. More, the majority of the interview participants (6/9) showed lack of knowledge in the given subject. On the other side, only 24% of the survey participants were aware about the privilege that FB mobile app has on phones to access text messages, where the rest were skeptical or unaware about it – I’m not saying FB collects information from users’ textbox but it’s important to know the privilege that FB has over phones –. Facebook realized that some of the permissions sound scary (Facebook help center) therefore they elaborate the reasons behind the permissions and give examples of the way they use the permissions for. In conclusion, reading FB data policy will definitely increase users’ awareness about data collection and the amount of information that the company is capable to gather, but in the same time that doesn’t mean the process and the type of information are being collected are recognized in the data policy, which explains the participants’ opinion about selling their information on social mediums to third parties and special agencies.

**Surveillance over social networks**

As shown in the literature review, information becomes the main source of income to social networks, there, we discussed experts and authors opinions about targeted advertisements and mass surveillance, afterwards we investigated about whether FB is selling users’ information or not, and from the data analysis we’ve seen the participants’ opinion – 76% of the survey participants they believe that social networks sell their information for own benefit –. Furthermore, 77% of the interview participants refused the following scenario ‘If Facebook said publicly: we will sell some of our users’ information to some corporations or agencies, will you accept that?’ and they were irresolute about deactivating their FB in such a case. From above two conclusions we can come up with. First, users of social networks become more dependent on the platforms they use (especially Facebook). Second, the majority of
them don’t trust social networks in terms of privacy protection for some reasons mentioned previously.

No clear image has been developed whether governments do surveillance over social networks or not, especially with the lack of authentic resources in this topic. In general, and based on the recourses used in the literature review, evidences on the existence of surveillance programs have been introduced, keeping into considerations that the mechanism and the way of using these programs are not much known. However, the participants expressed their opinion which has been categorized into, governments do surveillance over SNs, they don’t and no clue at all. Apparently, this difference of opinion appears due to lack of information in the given subject.

6.2. Suggestion of possible approaches to enhance privacy

When I’ve done the literature review and data analysis of interviews and survey. I wrote down some suggestions that users on SNs can take into consideration to improve their informational privacy. Also, I’ve noted down some actions and approaches that governments and social networks could perform to boost transparency and trust with users. In the beginning, it wasn’t my intention to share these views in the thesis as I didn’t follow an academic way to reach them but personal observations and own thoughts on presented arguments. Afterwards, I realized that these suggestions could be a notion or a step for further research work in the field of information privacy.

6.2.1. Suggestions for users on SNs

In this section I will present some possible approaches that users on SNs can take into consideration to enhance their privacy, these approaches are based on the arguments presented in the literature review, participants engagement in the interviews, and my personal observation.

- Reading the terms and data policy.
- Controlling privacy settings & Apps settings.
- Managing and categorizing the friends list.
- Less share of personal information.
- Considering what is private and not to share.
- Using privacy Check-up (integrated in some SNs).
- Awareness of information flow.
- Awareness of targeted ads mechanisms.

6.2.2 Suggestions for SNs and governments

In this section I will present some suggestions that could help in building transparency between individuals and SNs from a side, individuals and governments from the another. The suggestions have been developed based on the literature review and the observations I had from the empirical study. Two different parts will illustrate the presentation of the suggestions; one will be directed to SNs and the second one to governments.
As we have noticed from the data analysis, the participants had privacy concerns about their information on SNs and they tended to adopt negative conclusions due to the lack of clarifications that addressing their concerns. However, the terms and data policy is a way to legalize the relationship between parties and a way to increases individuals understanding about privacy protection and data collection applied on SNs but still not enough to reassure users. What I also realized from the study I conducted on FB terms and data policy that some of the terms have meanings loose and could be interpreted in wide contexts. For instance, the definition of the word use determined in the terms, or the privilege over users’ information, keeping aside the ambiguity of some of the terms. Therefore, simplification and better illustration of the terms and data policy are significantly needed in order to avoid misinterpretation and misunderstanding. That could happen not only by using simple words or by rephrasing some clauses but also by introducing the can do and can’t do allowed and not allowed style into the terms. For instance, FB gives an example about what it can do by the permission that FB app has over the textbox messages but it didn’t determine what is not allowed in such a permission. Alongside, elucidation of the data collection mechanism can decrease users’ concerns against privacy violations could happen by SNs. Apparently, social networks gather information from third-party partners as long as they transfer information to vendors, service providers, and other partners who support their businesses. Details about the data exchange and the companies/partners shared data with mostly not disclosed and shared with the public. In my opinion, The information secrecy in this context will expand the trust gap between SNs and users on the platforms, also, skepticism will be promoted in people’s minds.

Governments can play a critical role in protecting informational privacy on SNs. What we can all agree upon that SNs broke the borders between countries and build a community for all regardless their nationality. Therefore, legalizing an international law to protect online information is a need to protect individuals’ rights, and especially who engaged in the online social networking process. Moreover, we also need an international committee to govern and monitor SNs in order to avoid any violation could happen to information privacy. Lastly, governments should be transparent with people about surveillance programs that are running by them on social platforms, because transparency is a way to build trust.
8. Conclusion

8.1. Conclusion of main arguments and findings

Overall, the main purpose of the thesis is to understand what level of privacy awareness users on social networks have and how much relevant knowledge about surveillance on SNs they recognize. Moreover, the thesis aims to present users opinion about surveillance on Facebook and if they accept to be surveyed in certain scenarios. The thesis questions are: Does Facebook do surveillance, or are they a channel for others to do surveillance? What are users’ thoughts about privacy and surveillance on social networks? The motivation of choosing Facebook is based on the large number of users on the platform across the world which being considered as one of the most popular platforms among youths and adults.

A study on Facebook terms and data policy has conducted to build an understanding about some of the rules and see how much privilege FB has over users’ information. Evidently, there has been ambiguity in some of the terms and data policy, while there has been clarity that Facebook applies massive surveillance in terms of data collection on all users on the network.

The thesis has investigated privacy awareness and knowledge about data collection among students at Linnaeus University in Sweden. The study has explored how users of SNs protect their informational privacy and how much relevant knowledge about surveillance on SNs they recognize. However, I’ve argued that the awareness of young adults about terms and data collection on SNs is generally weak, even though, most of the study participants claimed that they are privacy concerned. Moreover, I’ve reported that the majority of the participants don’t trust social networks in terms of privacy protection for some reasons mentioned previously.

As a summary to the main findings, 71% of the participants had concerns about their privacy on social networks, 66% didn’t read Facebook terms and 76% did believe that social networks sell users information for own benefits. Two-thirds of the interview participants showed lack of knowledge about data collection on SNs, and didn’t know if governments do surveillance on social platforms or not. However, more than one-third of the survey participants claimed that they have nothing to hide, and almost similar percentage support government surveillance. Further, most of the interview participants protect their information privacy on SNs by having good privacy settings, controlling who have access to certain posts or managing friends list. However, 1/3 of the participants who had good privacy settings didn’t know all their friends on FB.

The thesis findings presented based on the research methodologies (survey and interviews), then I’ve introduced my arguments on the main factors drive privacy concerns on SNs, which are, ambiguity in some of the terms and data policy, awareness about information management and information flow, and lastly awareness about SNs data collection. No clear image has been developed whether governments do surveillance over social networks or not, especially with the lack of authentic resources in this topic. However, recommendations for possible approaches to enhance privacy have been introduced, and the list comes as follow:
- Reading the terms and data policy.
- Controlling privacy settings and Apps settings.
- Managing and categorizing the friends list.
- Less share of personal information.
- Considering what is private and not to share.
- Using privacy Check-up (integrated in some SNs).
- Awareness of information flow.
- Awareness of targeted ads mechanisms.

Moreover, some suggestions for SNs and governments have also been introduced to help in building transparency between individuals and SNs from a side, individuals and governments from the another. The suggestions are:

- Simplification and better illustration of the terms and data policy
- Elucidation of the data collection mechanism
- Legalizing an international law for information privacy
- Establishing an international committee to govern and monitor SNs
- Transparency about surveillance programs running by governments.

8.2. Future research suggestions

As the thesis investigated many interesting topics related to privacy and surveillance on social networks. During the analysis process, I realized that several concepts are strongly interconnected to each other but still can be investigated separately in whole new researches. For instance, data collection mechanism, information flow, surveillance and monitoring programs on social networks. Therefore, and from theoretical perspective, I propose a further research to investigate one of these concepts and how it influence user perspective of privacy on social networks. Furthermore, my study has identified the culture differences as one of the factors that affect personal privacy awareness and the use of social media. So, further researches can be focused on how users recognize privacy issues based on their diverse cultural backgrounds. However, raising privacy awareness throughout the society is fundamentally important, and researchers from relevant fields should be endeavour to minimize the risk of privacy violations by providing suggestions and practical solutions.
Bibliography


Facebook help center. Why is the Facebook app requesting permission to access features on my Android? [Online] Available at: https://www.facebook.com/help/210676372433246 [Accessed 1 July 2016].


Smith, R. E., 2013. Online Privacy: How Did We Get Here? | Off Book | PBS Digital Studios. [Video online] Available at: <https://www.youtube.com/watch?v=SCmKJyVx9AY > [Accessed 01 May 2016].

Snowden, E., 2015. Snowden and the debate on surveillance versus privacy. [Video Online] Available at: <https://www.youtube.com/watch?v=mD44gguSZzc > (International Journalism Festival).

Snowden, E., 2014. How We Take Back the Internet | TED Talks.[Video Online] Available at:<https://www.ted.com/talks/edward_snowden_here_s_how_we_take_back_the_internet > (TED, Canada).


Appendix A

- **Purposeful sampling strategies**: Select information-rich cases for in-depth study. Strategically and purposefully select specific types and numbers of cases appropriate to the evaluation’s purposes and resources. Options include:
  - Extreme or deviant case (outlier) sampling: Learn from unusual or outlier program participants of interest, e.g., outstanding successes/notable failures; top of the class/dropouts; exotic events; crises.
  - Intensity sampling: Information-rich cases manifest the phenomenon intensely, but not extremely, e.g., good students/poor students; above average/below average.
  - Maximum variation sampling: Purposefully pick a wide range of cases to get variation on dimensions of interest. Document uniquenesses or variations that have emerged in adapting to different conditions; identify important common patterns that cut across variations (cut through the noise of variation).
  - Homogeneous sampling: Focus; reduce variation; simplify analysis; facilitate group interviewing.
  - Typical case sampling: Illustrate or highlight what is typical, normal, average.
  - Critical case sampling: Permits logical generalization and maximum application of information to other cases because if it’s true of this one case, it’s likely to be true of all other cases.
  - Snowball or chain: Identify cases of interest from sampling people who know people who know people who know what cases are information-rich, i.e., good examples for study, good interview subjects.
  - Criterion sampling: Pick all cases that meet some criterion, e.g., all children abused in a treatment facility; quality assurance.
  - Theory-based or operational construct sampling: Find manifestations of a theoretical construct of interest so as to elaborate and examine the construct and its variations, used in relation to program theory or logic model.
  - Stratified purposeful sampling: Illustrate characteristics of particular subgroups of interest; facilitate comparisons.
  - Opportunistic or emergent sampling: Follow new leads during fieldwork; taking advantage of the unexpected; flexibility.
  - Random purposeful sampling (still small sample size): Add credibility when potential purposeful sample is larger than one can handle; reduces bias within a purposeful category (not for generalizations or representativeness).
  - Sampling politically important cases: Attract attention to the evaluation (or avoid attracting undesired attention by purposefully eliminating politically sensitive cases from the sample).
  - Combination or mixed purposeful sampling: Triangulation; flexibility; meet multiple interests and needs.
Appendix B

Interview Guide

- Ice breaking for 5 mins. (Inform the interviewee this is out of record)
- Go to step 1 in the interview guide, which talking about the thesis and the thesis question, don’t be strict to what’s written and don’t elaborate more than expected.
- Describe what kind of data I’m gathering and how I’ll use the collected data. (Around 5 mins)
- Jump to step 2. Ethical Considerations.
- Ask if we can start the interview and inform the interviewee that notes will start be taking, also ask if it’s possible to record the interview.
- Then jump to step 3, try to get answers for all questions in 30 mins.
- Ask the participant if s/he has any question or concern regarding the interview. And be aware if s/he wants to keep any information had given out of the record.

1. Description about my thesis and thesis question: (Max 10 mins)

My thesis comes to elucidate the definitions of privacy, informational privacy and surveillance over social networks generally and Facebook particularly. The thesis questions:

Does Facebook do surveillance, or are they a channel for others to do surveillance? What are users’ thoughts about privacy and surveillance on social networks?

Interpretations about terms and data policy used by social networks like Facebook, will take its place in my thesis to give the reader a deeper insight into the data is being collected by such social networks. On the other hand, statistical studies about daily use of social media, most popular social networks among teens and adults, personal information posted in Facebook, and some other studies, will be pointed out to draw up a clear picture about the activities and the data being published over social platforms. Finally, an empirical study will be included to show up people’s opinion about privacy and surveillance on social networks, and what they are doing to protect their information on social networks.

2. Ethical Considerations (Max 10 mins)

- Confidentiality: no contact details will be given. Interviewees won’t be named in my thesis, and the information had given by them will be used under nationality, age and gender. Like (26 male, Swedish). Also, I will not identify the interviewee by name in any reports using information obtained from this interview.
• The interviewee has the right not to answer a particular question or to terminate the interview altogether without giving any explanation.

• If the interviewee becomes distressed, the interview will be abandoned.

• If we record the interview (voice recording), I’ll be the only one who have access to that record and I’ll delete the record when I am done taking notes out of it. (the voice record will be destroyed by maximum 31 August 2015)

• **Informed consent:** proceeding with the interview, means, you (the participant) give me (the interviewer) an informed verbal consent to use the information you provide to serve my academic works with respect to what have been described about the ethical considerations in my study.

3. **Interview questions: (max 30 mins)**

   i. What is your nationality? And what’s your age?

   ii. Do you have a FB account? (if No, don’t ask iii and vi)

   iii. What kind of personal information with your friends on Facebook? Do you know all your friends on Facebook?

   iv. Have you read the Terms and Policies on Facebook or any other platform that you have an account on?

   v. What do you know about data collection on social platforms? Did you get the knowledge about that from social media?

   vi. If Facebook said publicly: we will sell some of our users’ information to some corporations or agencies will you accept that? If No, So will you deactivate your account?

   vii. How can you define privacy on social networks? Do you think you’re sharing the same definition with your culture?

   viii. How do you protect your privacy on social networks?

   ix. Do you think that governments are monitoring users’ activities on social networks? What’s your opinion about that?

   x. Do you agree that governments do surveillance on social networks to protect its national security or control Cyber-bullying cases? Would you like to add something related to surveillance over social networks?
Appendix C

Privacy & Surveillance over Social Networks

1. Nationality:

2. Do you have a Facebook account:
   - Yes
   - No

3. What activities are you doing on Facebook?
   - Likes
   - Comments
   - Post personal photos
   - Post personal videos
   - Messaging friends
   - Playing games
   - Using Apps

4. Have you ever read Facebook term & data policy:
   - Yes
   - No

5. If Yes for previous question, how much you read from the terms & data policy?

6. Are you aware about Facebook data collection?
7. Have you checked the Application Setting on Facebook and did you control your preferences there?

8. On a scale from 1 to 5 (1 is strongly disagree and 5 strongly agree) determine your opinion for each of the following statements:

<table>
<thead>
<tr>
<th>Statement</th>
<th>Strongly disagree</th>
<th>Disagree</th>
<th>Undecided</th>
<th>Agree</th>
<th>Strongly agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>Social Networks sell some of its users' data for their organizational benefits.</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>I don't share any kind of personal information on my Facebook account.</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>It's Ok if my friends on Facebook share my information with Facebook Apps.</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>I know all my friends on Facebook.</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>I am aware that when I signed up on Facebook, I give them a permission to use, run, copy, publicly perform or display, distribute and modify my contents with respect to my privacy setting.</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>I have nothing to hide, government and special agencies can have a look to my activities on social network.</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Governments should do surveillance on Social Networks to control/avoid cyber-crimes and terrorist attacks.</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Facebook App on my phone can read all messages I have in my phone inbox.</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>I have good privacy setting on my Facebook account.</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>I have concerns about my privacy on Social Networks.</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
</tbody>
</table>

All information collected will be used in a thesis study. There will be no connection to you, specifically in the results or in future publication of the results. By clicking Submit/Done you agree to participate in this anonymous survey and you give the researcher an informed consent to use the information you provided to serve his academic works.
User perspective of privacy and surveillance on social networks

Does Facebook do surveillance, or are they a channel for others to do surveillance?
What are people’s thoughts about privacy on social networks?

Linnaeus University, Växjö Campus.