User Perspective of Privacy Exposure on Facebook: An Examination of Risks Perception Among University Students in Sweden

Author: Silvia Anderchen & Martin Charvát
Supervisor: Jan Aidemark
Examiner: Anita Mirijamdotter
Date: 2016-05-24
Course Code: I6VT-4IK50E, 15 credits
Subject: Informatics
Level: Master
Department: Informatics
Abstract

Social media become a powerful communication medium for effective online social interaction globally. The use of various social networking sites has integrated into people’s daily lives especially among young adults. Problem arises when personal information is used without individuals’ involvement and relevant privacy risks increased. The main focus for the thesis is to investigate privacy perception and risks knowledge of Facebook usage among university students in Sweden. Based on this focus, the research identifies the key reasons that students decide to use and still use Facebook despite of privacy risks. The study also explores how user perspective of privacy affects the utilization of Facebook. The adopted methodology is qualitative research through the methods of interview and Facebook data analysis among ten young adult students at Linnaeus University in Sweden. As result, the research has identified seven concepts and three special outcomes to answer the research questions. Through the analysis, we have recognized weak perception of privacy risks among university students. Although users claim they are privacy concerned yet large amount of private information is shared on Facebook. The findings have shown that users are somewhat willing to accept certain part of potential privacy risks and personal information usage by different parties, in exchange for benefits and needs of online interaction in today’s modern society. Users believe the shared personal information on Facebook is under control and they can prepare for possible consequences. However, we believe that people’s needs for popular online social interaction outweigh privacy concerns. We suggest that it is significantly important for social networking sites’ users to balance benefits and risks, in order to maintain balanced usage and positive effects of online personal privacy. In the end of the thesis, we have suggested two future research directions based on our research topic.

Keywords

Social media, social networking sites, Facebook, third parties, information privacy, risks perception, big data, university students.
Acknowledgement

We would first like to thank our thesis supervisor Mr. Jan Aidemark from the Faculty Information system at Linnaeus University. We are grateful that Jan always gave us quick responses even outside of his working hours and efficient communication. We are very appreciating his professional and valuable guiding opinions for the thesis that has led us through the entire research process.

We would further like to thank the examiner Prof. Anita Mirijamdotter who has provided many effective seminars during the thesis course and useful feedbacks for our thesis. Our appreciation also goes to Prof. Christina Mörberg and Mr. Jeff Winter, who we had a lot of interesting discussions about social media privacy in the courses of Ethics and Professions in Information Technology and Informatics. The knowledge we have learned from them was strongly inspired and motivated for researching the topic of social media privacy.

Further, we are especially thankful for all the participants who are willing to take part of our research. They have offered many valuable facts and perspectives that have contributed the research the positive results and findings. These important findings enrich our understanding of social media privacy issue to a great level. Thanks to all participants, their involvement was the fundamental component to accomplish this thesis.

As important, we want to express our appreciation for the two researchers in this thesis. As young researchers we realized there are much knowledge need to be learned in scientific field. During the research, we have constantly fought and debated, closely discussed and collaborated together. Most importantly, we have studied a lot from each other, motivated and supported each other. It was tough but a happy and proud journey.

Finally, our deepest gratitude goes to our friends and family for their unfailing support and continuous encouragement throughout the entire thesis research. This thesis would not be possible without them. Silvia Anderchen would like to express her heartfelt gratefulness to her beloved husband Patrik and son Liam, family in China, “you are the most important life power and motivation for me to chase all my dreams and achieve all my life projects”.

Contents

1 Introduction ................................................................................................................. 1
  1.1 Introduction and Topic Justification ................................................................. 1
  1.2 Purpose Statement and Research Questions ............................................... 3
  1.3 Background Research .................................................................................. 3
  1.4 Scope and Limitations ............................................................................... 6
  1.5 Thesis Organisation ................................................................................... 6

2 Literature Review ...................................................................................................... 7
  2.1 Privacy Definitions .................................................................................... 7
  2.2 Information Privacy on Social Networking Sites ......................................... 7
  2.3 Facebook and Privacy Risks ................................................................ ...... 9
  2.4 Individuals Privacy Risks Perception .......................................................... 10
  2.5 University Students Privacy Management on Facebook ......................... 11
  2.6 Privacy Model and Communication Privacy Management Theory ........... 12
  2.7 Big Data ................................................................................................... 15

3 Methodology .............................................................................................................. 17
  3.1 Methodological Tradition ......................................................................... 17
  3.2 Methodological Approach ......................................................................... 17
  3.3 Methods/Techniques for Data Collection and Analysis ............................. 18
  3.4 Validity and Reliability ............................................................................. 20
  3.5 Ethical Considerations ............................................................................. 21

4 Empirical Findings ..................................................................................................... 22
  4.1 Data Collection Process ........................................................................... 22
  4.2 Research Question 1 ................................................................................ 23
  4.3 Research question 2 ................................................................................ 30

5 Discussions ................................................................................................................ 40
  5.1 Findings Discussions .............................................................................. 40
  5.2 Special Outcomes .................................................................................... 43
  5.3 Overall Reflections .................................................................................... 45

6 Conclusion .................................................................................................................. 47
  6.1 Main Purposes and Findings .................................................................... 47
  6.2 Special Outcomes and Argumentation ...................................................... 48
  6.3 Contributions ........................................................................................... 49
  6.4 Future Research Suggestion .................................................................... 50

7. References ................................................................................................................... 51
Figures:
Figure 1: Heatmap visualization of disclosure patterns in the Carnegie Mellon University (Stutzman et al., 2012, p. 17) 11
Figure 2: Expanded privacy model (Benson et al., 2015, p. 429) 13
Figure 3: Facebook Data Policy (Facebook, 2016) 13
Figure 4: Illustration of data collection sources 15
Figure 5: "Download your information" page 20
Figure 6: Example of changed privacy settings 34

Tables:
Table 1: Participants gender and nationality 18
Table 2: Concepts and categories connected to RQ1 23
Table 3: Concepts and categories connected to RQ2 23
Table 4: Frequency of Facebook access in certain time period 24
Table 5: Participants’ education background and level 26
Table 6: Assigned ads topics by Facebook and clicked ads by participants 28
Table 7: Information shared publicly 31
Table 8: information shared with friends (*has albums with multiple participants) 31
Table 9: Number of removed friends 33
Table 10: Timeline actions 36

List of Abbreviations:
CPM Communication Privacy Management
ISRA Information Security Risks Assessment
PIP Personal Information Privacy
SNSs Social Networking Sites
TPB Theory of Planned Behaviour
TPE Theory of Reasoned Action
1 Introduction

1.1 Introduction and Topic Justification

The rapid growth of the Internet and its extensive worldwide usage succeed today’s information era in the 21st century. As the Internet connects more than one-third of the world’s population, it offers great opportunity for “cross-cultural encounters” (Ess, 2013). With the Internet power of fast disseminating digitalized information, the rise of digital media has changed ways of communication and information disclosure among people to a completely new and revolutionary level (Ess, 2013). According to recent report, in 2015 there are 2 billion online social networks users worldwide and the estimate number will reach 2.5 billion by year 2018 (Petkos et al., 2015, p. 592). For Sweden, approximately 5.3 million Facebook users by 2018 is estimated (Statista, 2016). Through the enormous number, one can see the popular adoption of social media globally. Different social networking sites (SNSs) such as Facebook, enables possibilities for its users to share their private lives with extensive amount of personal information e.g., photos, relationship status, current location and daily activities. This personal information could reach hundreds or even thousands of Internet users just by one single click. Individual user shows willingness to disclose personal information in various social networking forms (Benson et al., 2015, p. 426). Despite of all positive impacts for social and economic areas, the booming adoption of SNSs has also brought privacy issues and challenges to the society. Personal information exposure on social networks is a major privacy concern (Benson et al., 2015, p. 428).

With the increasing influence SNSs has today, it is important for users to be aware of the high potential privacy risks when sharing personal information (Qi and Edgar-Nevill, 2011, p. 74). Information disclosure brings benefits but it is also accompanied with relevant risks such as increased digital footprint (Litt, 2013, p. 1649). Large amount of private information is frequently exposed and disseminated through various social networking sites every day. This information can be collected and used by SNSs providers and third parities (Petkos et al., 2015, p. 592). The personal information exposure creates opportunities for privacy invasion by different parties such as Facebook, third parties or even government authorities, for their beneficial or unknown purposes. “Problems arise when personal information is stolen, co-opted without permission, or otherwise compromised” (Conger et al., 2012, pp. 401-402). This issue is essentially important, because privacy is defined as “a basic political right that cannot be sold out in the marketplace” (Reidenberg, 2000, cited in Ess, 2013). Besides, privacy exposure could also build up potential risks for different kinds of financial and social consequences such as scams, identity theft, impersonation and cyber bullying (Otto et al., 2015, p. 6). Especially for users without information security knowledge the ‘not hermetically sealed’ online environment it is a certain threat that could cause stealing of their privacy data and identities (Altshuler, 2013, p. 2). As Lori Andrews humorously states, “Unlike Vegas, what happens in Facebook doesn’t stay in Facebook” (Andrews, 2011, p. 5). Thus, issues of information privacy produced by social networking sites become a threat landscape throughout the society.

In today’s network society information privacy cannot be controlled by individuals, but by those online organisations that keep the information (Benson, et al., 2015, p. 427). To some extend, information privacy become a societal issue, it might not be only the
responsibility of other parties, but it should also be carried by individual users for their immersed usage of social networks and over-sharing private information. For instance, the location information shared through enabled GPS could expose large amount of that collected by social media technologies (Benson, Saridakis and Tennakoon, 2015, p. 427). Besides, it is particularly important to know that information cannot be permanently deleted once they are posted on the Internet. With technologies such as big data enabled data mining, personal information can be easily collected or invaded by third parties without the individual's involvement. Technology can even record and analyse user's preference by his/her online activities such as Google searches or “Facebook Like” button, which could expose personal information to the public (Zhang et al., 2014b, p. 58). As Saridakis et al. underlines, “Social networks enable data accumulation on a previously unimaginable scale, yielding both benefits and undesirable consequences for their users” (2016, p. 320).

Although the use of SNSs and personal information exposure will bring corresponding privacy risks and consequence, that does not seem to affect people’s enthusiastic usage on variety of social networking sites. Facebook is the most popular social network site in Sweden (Statista, 2013) and its users are continually increasing. Relevant questions arise, despite of privacy risks, what are the main reasons for individual user to use and continuously use the Facebook? How these reasons impact people’s perception of personal information exposure? What degrees of the privacy awareness and risks knowledge users have? How privacy perspective affects the use of Facebook and what are the approaches users adopt to enhance privacy protection? Along with these questions, we will initiate a thesis research to generate scientific knowledge and to explore the topic of SNSs privacy. Although the evidence have shown that the majority of users is willing to share certain amount of personal information on SNSs, privacy issues still should be addressed (Qi and Edgar-Nevill, 2011, p. 76). However, personal privacy invasion might be difficult to measure or control by individual users, but with high-level of privacy concern and relevant risks knowledge, it is possible to effectively prevent risks and consequences at the first place. It is therefore critical for privacy advocate to examine privacy risks perception of individual users, to design effective approaches and improve the situation.

1.1.1 Brief Introduction of Research Setting

The initial purpose of the thesis is to understand a critical social phenomenon through an in-depth study of information privacy based on individual SNSs users’ perception. Therefore we adapted following research setting, the thesis is based on qualitative research and interpretive paradigm to fulfill the need for in-depth analysis of participants perception and ideas about privacy issues of SNSs usage. The selected methodology is interview consisting of ten participants who are students at Linnaeus University in Sweden with variety of national backgrounds. The research methods are interviews complemented by data analysis of Facebook data. The research is focused on international university students between 18-25 years, as the young adults demographic. For better focus, we decided to conduct the research based on a specific SNSs platform, Facebook. The choice of Facebook is based on its large amount of users across the world and it is the one of most commonly used social networking sites in Sweden. More importantly, it is a very popular online communication platform to engage in various activities and exchange information among students. Therefore university students are the selected target group since they can represent young adult users’ privacy perception
in a good way. We believe our research topic of social media privacy among university students can be addressed in a rich way and provide interesting results. More details about research setting will be comprehensively described in the Methodology section.

1.2 Purpose Statement and Research Questions

The fundamental purpose of the thesis is to address privacy issues on SNSs with the focus on individual users perception of privacy risks. Within the topic, we would like to explore the research through the focus on Facebook and university students. There are two main purposes for the thesis. First, the research is aimed at understanding what level of privacy awareness SNSs young adult users have and how many relevant risks they recognize. The purpose is achieved through identifying what are the main reasons for university students to use and continue using Facebook although privacy risks exist. The second purpose is to explore how university students as Facebook users, perceive personal information exposure on Facebook and how these perspectives affect their usage of Facebook. Within this purpose, we also investigate what are the methods students adopted to enhance personal privacy protection. Based on the purposes, we have formulated two research questions as the fundamental guideline through the whole thesis:

1) What are the main reasons for university students to use Facebook despite of privacy risks?
2) How university students’ perspectives of privacy exposure affect the use of Facebook?

1.1.2 Motivations

The primary motivation of the thesis is the global concern of increasing social media privacy challenges. We recognize that the issue of privacy invasion on SNSs has to be addressed since a large amount of stakeholders is involved. We realize that it is essentially important to enhance online personal information privacy protection in order to build up a healthy Information and Communication Technology (ICT) society. Privacy awareness in the digital age should be raised not only among individual online users but also all involved parties across the network society. Therefore the motivation of the research is aimed to provide valuable findings that could raise social awareness of social media privacy. Also, the topic of personal information privacy on social networks is closely connected to the area of information systems because it is in connecting the technology, people and society. A society with good presence of information privacy in today’s digital environment will be a sustainable and thriving way of living. This needs to be effort by all researches and different actors in the society. We as researchers in Information Systems field shall particularly pay attention to this topic with our endeavor and contribution through relevant researches.

1.3 Background Research

1.3.1 Social Media and Facebook

Social media is the computer-mediated medium that could enable individuals or organisations to share, deliver and/or exchange for example instant messages, thoughts
and career interests information (Buettner, 2016), it also allows dynamic content e.g. pictures and video to be posted in different types of social networking communities. There are various kinds of social media but they do have some common characters. For instance, social media are web-based social interaction applications that give its user possibility to generate contents and disseminate them immediately within his/her established networks community (Obar and Wildman, 2015, Kaplan and Heanlein, 2010). It also has the function to connect user’s profile with other individual users and groups internationally, based on the designed-function of specific networking site or organisation (Obar and Wildman, 2015, Kaplan and Heanlein, 2010). Today’s social media not only depends on internet-based technology but also on the possibility of mobile-based usage. This easy access provides increased opportunity for user’s self-expression and high interaction between different individuals, groups and organisations within the community (Obar and Wildman, 2015, Boyd and Ellison, 2007). The main difference between traditional media and online social media is the medium format change from one-way communication to interactive dialogues.

However, the crucial feature of social media is internet-based social interaction. One of the most representative social media platforms is Facebook, Mark Zuckerberg and his Harvard colleagues launched this website in 2004 and it became a trendy social networking site ever since. By the beginning of 2016 Facebook has already 1.65 billion monthly active users, which it rewards as the most popular social networking application worldwide according to statistics (Statista.com, 2016a). Worth mentioning, right after Facebook, WhatsApp and Facebook Messenger ranked as the second and third popular applications (Statista, 2016b). It is important to know that WhatsApp was bought in 2014 and Facebook Messenger was launched in 2011 both by Facebook, Inc. One can see that Facebook, Inc. has huge amount of users among social media market worldwide. Nevertheless, as the most adopted social media platform, Facebook has its own special features such as user profile/personal timeline, news feed, like button, the function of following other users, etc. In spite of those particular characteristics, Facebook also has a privacy setting function that allows its users to choose and manage the setting according to one’s preferable privacy needs. Which means that Facebook user has the possibility to decide who or which group of selected people will be able to access for example his/her profile information, friends list and shared content. If user does not have any customized privacy setting, it will automatically follows the default setting as “share with everyone”, which means that every internet user is be able to view all information this user shared on Facebook.

1.3.2 University Students and Facebook

When speaking of Facebook, its history has told that Facebook was founded by a couple of university students at Harvard University in United States. At the very beginning, Facebook was created as a social network among university students within Harvard University but it rapidly expanded to other universities and colleges in Unite States followed by the expansion to the other parts of the world. As in 2006, the usage of Facebook already covered 2000 colleges in United States (Ellison, Steinfield and Lampe, 2007, p. 1144). Obviously, university students were the central users of Facebook. “Since its inception in 2004, this popular social network service has quickly become both a basic tool for and a mirror of social interaction, personal identity, and network building among students” (Debatin et al., 2009, p. 83). Nowadays, like the above information has shown the Facebook has a large amount of users globally.
Although Facebook has covered all different types of users e.g., individuals with diverse occupations, even public figures and various organisations, university students are still one of the dominant user groups for Facebook, since a student life without Facebook is unimaginable (Debatin et al., 2009, p. 83). This is the major reason we select university students as the target group for the study, because this young adults group is one of the most active user groups on Facebook. According to report, Facebook is one of the most popular social networks in United States where 90% of college students are engaged on it (Fogel and Nehmad, 2008).

1.3.3 Privacy and SNSs Privacy

Privacy as the major topic in this thesis is referred to personal information privacy. In a digital age, today’s reality of privacy issues is more connected to online private information invasion. Online privacy embodied most through personal utilization of various social networking sites. Given that “the individual trades private information about himself as a kind of currency in exchange for anticipated goods and service”, privacy issues occur when personal information is being used without user consent (Conger et al. 2013, p. 401-402). The situation of stolen private information seems to become a common trend in today’s social media world. Therefore it is important to increase individual user’s privacy awareness of information security for a better online society (Farahmand, et al., 2009, p. 462). In order to enhance individual’s privacy awareness, relevant risks knowledge has to be present among all users on SNSs. The potential risks and consequences are essentially vital for controlling personal information and privacy protection. Despite the responsibility of individuals, it is as important to emphasize the role of other parties, for instance third parties and government authorities in shaping a good environment for SNSs privacy. Because third parties and government authorities have accountability to prevent privacy invasion based on ethics and policy implementation.

1.3.4 Media Technology and Big Data

Media technology as defined in Kingston Smith’s article (2014) is “technology which disseminates, stores or produces media content”. In connection to our study the most important is the media content in forms of pictures, videos and audio available on the Internet. Good examples of media content providers on today’s Internet are YouTube or Spotify both founded in 2005 (YouTube, 2016; Crook and Tepper, 2015). These are both major players in media streaming industry. The Facebook is a very convenient platform to share media content as well. It is also connected to many other mediums such as YouTube and Spotify. With more than one billion daily users (Newsroom, 2016) Facebook has clearly shown its significant role in people’s life that presents large percentage of world’s population. In other words, Facebook have the ability to generate extensive amount of personal information with various media contents. These personal information and media content can be easily collected by Facebook or third parties through media technology such as Data warehouses. Hence, relevant privacy issues occurred, "…pervasive technology often leads to unintended consequences, such as threats to privacy" (Debatin et al., 2009, p. 83). These privacy threats are even multiplied by emerging phenomena of Big Data (Porter, 2014). Enormous data storage capacities, the Internet of things and steadily emerging new algorithms to process collected data. This combination creates an environment where protecting people's online privacy is harder than ever before. Therefore it is important to explore people’s
perception of the data collection technology on whether SNSs users are even aware of the possible technology for personal data collection.

1.4 Scope and Limitations

This thesis is conducted within the scope of one-year master degree project of Information System programme. As young researchers, our primary goal for the thesis is to generate more knowledge in the field of information systems with the focus on SNSs information privacy. Due to the scope and time schedule limitation, there are challenges to adopt a large methodology and multiple methods at the same time to enrich the quality and quantity of the data collection. For better results of the study, the key research methods are interview and Facebook data analysis, they are employed with the principle of a comprehensive analysis from two angles, but also based on a manageable level. It thus affects the count range of selected participants and the corresponding results and findings might be limited since it relies on small amount of users which might not completely represent the entire target group of university students in Sweden. Besides, the limited amount of data provided in Facebook data file influence our ability to illustrate certain phenomena identified in the interviews. More, we realize the complication during interview process and our fresh interview experiences might lack of mature techniques to carry out ideal interviews. However, within the scope, the study is not only endeavor for seeking more scientific knowledge in the area but also maximize the contribution based on our ambitions, which could decrease the limitation to a minimum level, as we believe.

1.5 Thesis Organisation

The thesis will be divided into six main sections with numbers of subsections. The first section is already presented above as an overview introduction for the thesis. We have introduced the concerned topic with focus area of the thesis, which is about SNSs privacy based on individual user’s risks perception among university students in Sweden. We have explained the main purposes and motivations for the study, as well as the scope and limitation. In the second section, relevant literature review of the scientific studies focused on personal information privacy on social networks will be presented. Individuals’ risks perception of SNSs privacy and the critical theories that are used for the research will be presented. The third section presents the research methodology with all details about research approaches/methods the thesis employs. It further shows the designed empirical settings with clear explanation of how exactly we will carry out all data collection into practice. The fourth section, which is considered as the central part of the thesis, because empirical findings and results will be demonstrated, begins with the actual data collection process. As results, the seven identified concepts will be deeply analysed to answer the two research questions based on our research strategies of data collection. The fifth section is where we discuss main findings/results and special outcomes based on our own interpretation. The discussion will further reflect on the important findings and its meanings for the field of IS. The final section is the conclusion of the thesis. It summarizes main tasks and findings of the thesis, together with the key argumentations based on the results. It will further present what we have contributed from the research of addressed privacy issues. The section will end up with the suggestions of further research direction.
2 Literature Review

2.1 Privacy Definitions

This section should start with an important question in relates to the topic: what is privacy? According to Alan F. Westin’s (1970) definition, “privacy as the right to define for oneself when, how and to what extent information is released, gives a perspective that more closely fits today’s reality” (cited in Conger et al., 2013, p 401). Another scholar Sabine Trepte, defines that “Privacy is perceived as a basic human need and, its loss, as an extremely threatening experience” (Trepte, 2011, cited in Amyrich-Franch, 2014, p. 1). Although people often believe privacy is some kind of right, yet Roger Clark (2006) argues that privacy is a thing people would like to have much of instead of a right with absolute standard. He therefore defines privacy “is the interest that individuals have in sustaining a ‘personal space’, free from interference by other people and organisations”. However, different scholars have own definition of what privacy is based on their motivations. Yet one can still sense the fundamental component of privacy, which is the human desire of private life and information that needs to be respected and no disturbing from others.

Then why privacy is important? For scholar Clarke (2006), privacy is critically important because it could affect people’s lives from perspectives of psychologically, sociologically, economically and politically. He further claims the importance of privacy is reflected of many international and national Constitutions and Bills of Rights. Yet how should privacy be protected? Even before the digital age, privacy respect is already recognized by Council of Europe, “Everyone has the right to respect for his private and family life, his home and his correspondence” (1950, cited in Ess, 2013). For UN laws of privacy in 1966, it clearly stats, “No one shall be subjected arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks” (Vlemmix, 2013). The law tells that privacy is seen as a human right that plays crucial role to people’s life. However, privacy in today’s information age is facing new challenges when compared with traditional privacy right.

2.2 Information Privacy on Social Networking Sites

As Westin’s (1970) definition, privacy perspective should meet today’s reality. And personal privacy in today’s practices is often connected to information privacy, because in digital age, personal information can be rapidly disseminated worldwide and collected or stored by computer technology. The concept of information privacy is sometime referred to data privacy, it “is the interest an individual has in controlling, or at least significantly influencing, the handling of data about themselves” (Clarke, 2006). Why should people care about information privacy? The fast development of Internet in the 21st century allow user to take central stage in the web through the thriving usage of various social media and social networking sites because it changed the communication pattern from published content to the people who created it (Bichsel et al., 2014, p. 27). Privacy issues and its potential risks confront big challenges when huge amount of people are joined social network sites. According to studies in 2014, 74% Internet users are also users to some social networking sites (Hossain and Zhang, 2015, p. 246). Further, individuals are attracted by the special features of social networks and post
their private information with own willing. The phenomenon raises public concern of privacy and freedom for individuals, and the relevant privacy issues increased when smart devices are widely utilized (Benson et al., 2015, p. 426). Problems occur when personal information exposure gives opportunity for privacy violation and risks such as cyberbullying or online harassment, it happened particularly among teenager users on social networks (Saridakis, 2016, p. 321). Besides, many social networking sites allow user to upload variety of personal information that includes photos and videos such multimedia contents, “where the contents may be highly relevant to users’ privacy, such as identities, locations, preferences, and social relationships” (Zhang et al., 2014a, p. 60). Also, this personal information usually disclosed on the social networks platforms to other users but it can also collected by service providers (Zhang et al., 2014a, p. 56). Relevant issues arise when information is taken with compromised or without consent (Conger et al. 2013, pp. 401-402). Users who are without awareness of controlling personal information, their privacy could be easily invaded by these third parties (Zhang et al., 2014a, p. 57). To some extent, privacy invasion is rooted in the use of social media where the network sites’ providers offer free services in order to extensively collect personal data (Post and Walchli, 2014, p. 115). It is important to note that even government authorities or law agencies can require social media organisations to collect users personal information for their needs (Hossain and Zhang, 2015, p. 246). Therefore, “privacy might be a problem for anyone who leads a life mediated in part by digital technologies” (Tabitha, 2015, p. 893).

Social networks’ intimate interaction is often carried by people with wrong perception of privacy that could cause harm to their security and sensitive personal information, since it is difficult to control other online users and different parties (Altshuler, 2013, p. 2). Hence, information security turned out to be essentially important because it is closely connected to information privacy (Benson el at. 2015, p. 427). Despite of the sensitive personal information, there is information that users displayed on social networks might looks impersonal. Yet media technology such as Big Data can gather any type of data and to easily identify a person with comprehensive image, it can even analyse a person’s walking pattern that is recorded by surveillance camera (Turker, 2013, p. 64). For data technology today, it is become more obvious that personal information privacy can no longer managed by individuals (Conger et al. 2013, p 401). Given that individual’s awareness of personal information sharing is still matters because it could affect privacy protection to certain level. It is important to note that 75% of information data is generated by individuals in year 2012 (Tucker, 2013, p. 64). How users think about great amount of personal data that is exposed in terms of their information privacy? Study has showed that users do admit that they have insufficiently controlled over “what, who, where, when and how their information is disclosed, shared, reached or used”, this is certainly a critical issue of such behaviour (Ngeno el at. 2010, p. 1041). The real problem is that sometime users do not even realize the disclosure of their personal information and do not intent to keep them safe (Zhang el at. 2014a, pp. 60-61). The risky engagement of social networks activities by giving away their private content can rise possibilities for victimization, specially for young adults (White el at. 2015, p. 1408). As scholar Marwick (2014) claims, it is rather easy to image potential risks if people have weak awareness and privacy management of shared personal information, when reflected on the power of information dissemination on social media could research large audiences rapidly. Therefore he tends to argue “the only way to maintain privacy is not to share in the first place” (p.1052).
However, Conger et al. claim that public awareness of privacy issues and provided action-oriented approaches would be the encouragement for solving privacy problems. Therefore the authors emphasize privacy issues should be composed by individual personal information control and societal protection (2013, pp. 413-414). The proposed solution may be Internet safety education not only for young people but also for teachers and parents, and it needs to be effectively implemented in order to against potential risks (White et al. 2015, p. 1421). Because with enhanced knowledge in privacy risks perception through privacy concern education, relevant issues can be changed to a better level (Saridakis, 2016, p. 326). Nevertheless, before the investigation of individual’s risks perception, it is important to identify some general online risks in order to know what kinds of potential risks can be carried out.

2.3 Facebook and Privacy Risks

The Internet provides many benefits and opportunities to all of its users, but it is not any exception for the rule that these big opportunities as research suggest comes with many risks (Chou et al., 2005; Leung and Lee, 2011). The main focus of this thesis is on privacy issues, the fast development of the Internet bring us to the age of big data analytics where it is harder than ever for individuals to keep desired level of privacy (Tucker, 2013, pp. 64-66). However the technology of big data is not the only risk that users have to keep in mind while they browse the web. Almost every day we are informed about new vulnerabilities explored in operating systems we use. For example the Heartbleed Bug which became public in April 2014 and allowed stealing of information protected by OpenSSL cryptographic software library (heartbleed.com, 2014). Moreover, these vulnerabilities can be used by hackers to run malicious code on our devices. Latest example of this is glibc buffer overflow vulnerability (Overflow, 2016). Due to these vulnerabilities malicious parties could collect all information including everything we do on Facebook.

Another very common type of risk all of us daily encounter is commercial. In connection to previously mentioned technical issues of commonly used software it would be foolish to believe that all of our transactions online are 100% secure. In addition to that the social engineering technique has to be mentioned because it is considered as very effective method to gain information access (Mann, 2008, p. 1). Facebook is very effective tool to share fraudulent information and and by that “increasing its impact” (Gupta and Garg, 2015, p.19). Through social engineering it is possible for malicious parties not only get access to people’s online bank accounts but also other private information. Furthermore, the Internet has impacted the new generation to a large extent, this generation never lived in environment without it. There are risks for children users, three main categories of risks for children are recognized by De Moor et al. (2008): content risk, contact risk and commercial risk (cited in Schilder, 2015, pp. 286-287). These refer to the fact that children exposed to multimedia content originally aimed on adult audience. Anonymity of the Internet allows malicious users to cyberbully or steals personal information. Further findings about risks of the Internet for kids can be found in Risks and safety on the Internet: The perspective of European children (Livingstone et al., 2011).

One of the main categories of online risks is several times mentioned privacy. This topic is studied from many perspectives (Madden et al., 2013; Moreno et al. 2013; Tucker, 2013; Andrews, 2011). The advent of new media technologies causes many concerns
among public as well as academics. Patsakis et al. (2014, pp. 521-525) provides one of possible categorisations for privacy issues with multimedia content sharing. It is examined that even when users do not perceive direct exposure of their private information during sharing content on SNSs, the possibilities to generate these information indirectly from multimedia content exist. Because of the fact that metadata can identify location that could lead to unintended information disclosure (Furini and Tamanini, 2014, p. 9796). Since SNSs are designed to promote content sharing it is very easy to do so even without permission of content owner. User can be tagged without previous notice (Grimmelmann 2009, p. 1146) and external application can very easily gather data from SNSs accounts. Search engine capabilities can expose the activity on SNSs to the whole Internet and it further complicates the ability to delete such content. Last but not least is the concern focused on the fact that user’s personal data disclosure to government agencies has been reported (Greenwald and MacAskill, 2013).

2.4 Individuals Privacy Risks Perception

The research of individual’s privacy awareness and risks perception on social media is essential. In order to understand the sharing behaviour of SNSs users, we need to learn how much they know about privacy risks. Also, the perception of privacy risks can explain why users tend to use the SNSs despite the evident presence of relevant risks (Ngeno et al. 2010, p. 1042). The study confirmed, “privacy invasion is part of the Facebook reality and not just a hypothetical possibility” (Debatin et al., 2009, p. 99). This issue is also recognized by Kanter et al. from parent-child perspective (2012). Regarding to individuals’ privacy perception, Benson et al. argue that SNSs users lack of privacy awareness of their shared personal information and content is used by SNSs providers and third parties (2015, p. 433). Yet there is a study conducted by Sørensen and Skouby (2009) that find out that SNSs users are concerned about privacy situation. The participants of this study were 33-55 years old and involved or interested in ICT industry. The result is definition of “requirements focused on self control and privacy” (Sørensen and Skouby, 2009, p.5). Ngeno et al. (2010) decided to test the methodology from Sørensen’s and Skouby’s study on broader demographics. Part of the results confirmed that users “want assurance of data privacy” (Ngeno et al., 2010, p. 1042). The data gathered from different demographic groups provided also additional results. People have limited understanding of what is done with their information and who has access to it. Further, it is not perceived as a “big enough problem” for them, to require any extraordinary efforts in regards to security (Ngeno et al., 2010, p. 1042). The comparison of these two studies provides a good example of how knowledge background influences user’s privacy perception. It has been illustrated that the perception of people can be changed if the situation is explained. In study focused on location privacy in SNSs, Furini and Tamanini show that “people who were initially concerned, are less worried” after the appropriate introduction to the issue of location privacy (2015, p. 9823). Besides, the study by Ur et al. (2012, p. 1) finds that users perceive the online behavioural advertising (OBA) “simultaneously useful and privacy invasive”. As O’Brien and Torres (2012, p. 63) presents in their study, only approximately half of Facebook user base is privacy aware. However, even privacy aware users decide to still utilize Facebook. The reasons for this decision are based on belief that benefits prevail the perceived risks (O’Brien and Torres, 2012, p. 93).

Debatis and Lovejoy (2009) identified in their study two interesting concepts, the “Routinization” and “Ritualization”. The first concept describes the fact that Facebook
become a daily routine for many users. Participants describe it as convenient way to keep in touch with friends. Second concept refers to the “ritualistic function” of Facebook (Debatin and Lovejoy, 2009, p. 96). Not only the process of joining Facebook is defined as some sort of ritual but also the actual Facebook usage is ritualized (Debatin and Lovejoy, 2009, pp. 95-96). Next, O’Brien and Torres identified that information disclosure is driven by “desire for social acceptance” on SNSs instead of “privacy concerns” (2012, p.93). This result supports the opinion that even when users know about risks they tend to ignore them. Lastly, the findings from Benson et al. (2015) show that users which perceive the SNS security policy transparent, more likely decides to “benevolently share their information with the site” (p. 434). These are the reasons we identified in current literature, why user tend to use Facebook despite of perceived risks. Combined with acceptance of certain data usage scenarios such as OBA, these reasons create an environment where users favor benefits over perceived risks.

2.5 University Students Privacy Management on Facebook

The investigation of actual Facebook usage by university students is important for privacy research. By identification of most common usage patterns we can find out what puts students into risks. More, during this research it is also possible to explore the approaches students use to protect their privacy. As Stutzman et al., (2012) find out in their article, students from Carnegie Mellon University changed their sharing behaviour significantly between 2005 and 2011. Figure 1 illustrates what type of information was commonly shared (red colour) and what students tend to keep private (blue colour). The trend to limit the amount of information that is available on Facebook about them is evident.

![Figure 1: Heatmap visualization of disclosure patterns in the Carnegie Mellon University (Stutzman et al., 2012, p. 17)](image)

Personal information control on Facebook is influenced by many factors. Christofides et al. (2009) presented in their article that users with “higher self-esteem” and/or “lower levels of trust” tend to utilize the information control methods more often (p. 343). The intended audience also plays a role in information control. As Peluchette and Karl find out, students expressed “strong agreement” that sharing information with friends or family is valuable, but sharing information with strangers or employers is not welcome.
Further the “need for popularity” is relevant, since some people are not ready to “sacrifice their popularity” just because of their concerns about privacy (Christofides et al., 2009, p. 344). Lastly the cultural differences as identified in Vasalou’s et al. article influence how important are certain elements of Facebook for its users (2010, p. 727).

The methods of information control, such as content removal, limited sharing or removing friends are used by many students. This way they try to deal with “the tension between perceived privacy risks and expected benefits” (Debain and Lovejoy, 2009, p. 87). Debain and Lovejoy (2009) further argue that students frequently provide more information through SNSs than they would provide in other contexts (p.88). Question of students sharing behaviour, which could lead to disclosure of “confidential workplace information” after they switch to corporate environment, is raised in discussion by Peluchette and Karl (2008, p.96). The suggestion is to provide an “orientation or training programs” for new employees to help them adjust to company policy (Peluchette and Karl, 2008, p.96).

Overall it has been proven that the certain level of information control is necessary. “SNSs help maintain relations” and are very convenient tools to communicate with acquaintances (Ellison et al., 2007 p. 1164). Yet, without control over personal information, it could reach unintended audience such as future employer (Peluchette and Karl, 2008, p. 96). However, even the best personal information control practices do not limit the information that is available to Facebook and its third parties (Stutzman et al., 2012, p. 31).

2.6 Privacy Model and Communication Privacy Management Theory

Personal information privacy (PIP) issue is no longer only the concern of every individual but also includes several other parties. These parties have to be taken into consideration while reflecting on personal privacy. This situation is illustrated in PIP model which is presented in Conger et al. (2012) article. The figure 2 shows the connection between each party. The first party represents the actual users of a service such as Facebook and is connected to Second and Fourth party. The second party is connected to every other party and is represented by actual service providers, their vendors and suppliers. Data sharing partners represent the third party which receives data from second party. The fourth party composed by variety of malicious entities is also connected to every other party since it is possible to attack each of previously mentioned parties. Conger et al., argue, “data-sharing environment is a key source of vulnerability” (2012, p. 407). It is the constant information sharing that provides the opportunities for illegal hackers to access personal information transferred in these transactions.
The role of individual in privacy protection is gradually changing, yet it is still her/his decision to use the service or not. If user perceives the benefit provided by service “outweighs the potential risk of a privacy invasion” she/he is more likely to utilize it (Awad and Krishnan, 2006, p. 26). It is common that users are “unable to control the practices of those who collect their information” (Tsai et al. 2011, p. 267). Still, they have a choice to not share or limit the type of the content they want to share.

For our study the second party is represented by the Facebook. To define the role Facebook has in information transaction process, three sections of its data policy are showed in figure 3. First section illustrates what kind of information does Facebook collect. Second section of data policy illustrates how does Facebook use this information. Lastly is presented the list of how information is shared. The effort to make all of this easy to understand is clear. However even the best intentions fall when majority of users does not even try to read the data policy (Agnellutti, 2014, p. 141). More, once the information leaves the control of first and second party “data have a life of their own” (Conger et al., 2012, p. 406).

**Figure 2: Expanded privacy model (Benson et al., 2015, p. 429)**

**Figure 3: Facebook Data Policy (Facebook, 2016)**
Facebook states that all its partners “must adhere to strict confidentiality obligations” that are coherent with its Data policy and other arrangements they agree on (Facebook, 2016). Individuals control over the shared information is already lost during this step. Therefore, it is important for government, media and public to motivate “the business community to self-regulate” and promote fair use of personal information (Culnan & Bies, 2003, p. 338). Further, the government as third party actor has to be considered. In this sector “individuals are obligated to relinquish personal data” to support collective good (Conger et al., 2012, p. 406). There is a problem with unlimited data collection from available technologies. Facebook represents one of the channels for government to collect personal information. More, there is plenty of other examples such as RFID, Smart motes or Bio organisms (Conger, Pratt and Loch 2012, pp. 408-409). Because of that, we currently face the challenge to define the boundaries of appropriate data collection practices (Albrecht & McIntyre, 2005).

Lastly the fourth party represents the malicious data usage by thieves, hackers and malicious third party employees (Conger et al., 2012, pp. 406). The fourth party also includes the hacktivists which use hacking skills to enhance their activism efforts. The threads of such actions are rapidly evolving and could cause irreversible damage such as, “having your data breached, website vandalized and reputation destroyed” (Caldwell, 2015, p.12). The increasing activity of hackers is a fact supported by “Data Breach QuickView report” which states that 2015 sets the record in number of data breaches (DatalossDB.org 2016).

The situation of privacy protection is fairly complex. The PIP model describes the connections between four parties included in privacy exposure of every individual. It is also clear that the individuals do not have the absolute control over exposed information (Conger et al., 2012, pp. 406). However, that does not completely remove the responsibility to do so. In field of IS exist many theories describing possible behaviour of individuals to enhance their privacy. One of them is Communication privacy management theory which was developed by Sandra Petronio in 1991 (Petronio, 1991). CPM theory utilizes the metaphor of boundaries in a way that every information one posses have its own boundary assigned and defined by individual. For cases when individuals desire to share the information with others the negotiation of rules for information sharing takes place to keep the boundaries under the control (Petronio, 2002, pp. 5-6). In Xu’s et al. (2011) article the model utilizing CPM is presented. During the validation process of model by survey, the strong link of “perceived control in alleviating privacy concerns” among social network users has been measured. Furthermore, the links between “Perceived Effectiveness of Privacy Policy” and privacy risk of individuals as well as “Perceived Effectiveness of Industry Self regulation” and privacy risk of individuals is described in the model. Both of them have been proven to reduce the perceived privacy risks (Xu’s et al., 2011). As author Eden Litt (2013) believes, CPM theory is a valuable framework to identify the factors that influence people to enhance technology boundaries on SNSs by first understanding people’s general privacy boundary (p. 1650). To clarify the role of CPM in this study, it is used as inspiration during the process of concept creation and not as a framework that would be applied throughout the whole study.
2.7 Big Data

Big data is expression used not only to highlight the volume but also the variety and velocity of data generated in today’s information society. The considerable amount of this data is generated by users on social media and the risk of the unintended privacy disclosure as consequence of this situation are two main reasons, which explain why is the topic of big data important for our study. Obole et al. describe in theirs article how could the aggregation of information from diverse sources bring risks for average user (2012, pp.5-6). The figure 4 illustrates the brief selection of most common sources of information that is gathered daily about every user of these services. Since it is very convenient to use the login information from e.g. Facebook or Google account to other services, it became easier for these companies to collect information about people’s daily lives. With analytical possibilities that are available to such technology driven companies it is no surprise that this situation raise many concerns and questions (Obole et al., 2012). When data is gathered about people’s usage of Facebook, Twitter, YouTube, Spotify, Netflix, Instagram as well as our browsing history the privacy one would imagine is present in online space “instantly disappears” (Che et al., 2013).

![Figure 4: Illustration of data collection sources](image)

One of the ways to diminish the concerns of social media users about their privacy in regards to data collection on these sites is honest and clear explanation how the data can be used and how it could affect them. In the world of social media analysis (SMA) we can find three main methods that are commonly used: “text analysis/mining, social network analysis and trend analysis” (Stieglitz et al., 2014). With the text analysis it is possible to identify the sentiment, opinions or topics of studied text. It is possible to identify previously not obvious communities or other types of connection between social media users thanks to social network analysis and the trend analysis can produce forecasts about future behaviour, topics of interest or behaviour of users.

These and many more emerging methods can be used for very beneficial purposes. In health care industry it is for example possible to monitor adverse drug reactions and by that save many lives (Yang et al., 2015). Governments are already using mixture of these methods to improve theirs crisis and security management (Wybo et al., 2015, p.117). These examples are just a tip of the iceberg and new ways how data can be beneficially used are discover every year. Therefore it is important to support the data analysis efforts. Clearly SMA is not without risks, it is important to ensure awareness of every entity included in this process about controversial and potentially harmful misuse.
scenarios. Moreover, the creation of environment where “only legitimate processing of personal data” will be tolerated is essential (Rubinstein, 2013).

One of the values that threatened by inappropriate usage of SMA is already mentioned personal privacy. The Seven types of privacy were analysed in Strauss’s and Nantwich’s (2013) article, privacy of “behaviour and action”, “data and image”, “thoughts and feelings”, “communication”, and “association” are evaluated as at least partly affected by current common usage of social media. The usage of social media is however constantly developing and in the future it is expected that all privacy types will be affected in some way. Moreover according to Fuster's and Scherrer’s (2015, p.29) study “ ‘pseudonymised’ data must be qualified as personal data” since with capabilities of big data analysis it is possible to connect ‘pseudonymised’ data back to original person.
3 Methodology

3.1 Methodological Tradition

3.1.1 Paradigm

The chosen paradigm for research is interpretive. Choice of the paradigm has been made based on our goal to investigate the student’s perspective of privacy risks on SNSs, which is connected to general effort of this paradigm to “understand phenomena through the meanings that people assign to them” (Myers, 1997, p. 5). The representation of reality and knowledge is perceived as a “social construction by human actors” (Walsham, 1993, p. 10). In contrast with the positivist paradigm which assumes that “reality is objectively given and can be described by measurable properties” (Myers, 1997, p. 5). It has been proven that this paradigm fits very well for qualitative type of research which is in line with our choice to use an interview study. It will be conducted among several students with similar relation to social media and privacy risks they can cause. The insight about how students perceive these risks and effects it has on Facebook usage, will be gathered through series of interviews and data analysis. These methods will help us to create complete image of their perception and behaviour since they complement each other.

3.2 Methodological Approach

3.2.1 Interview Study Complemented by Data Analysis

The study focus is perception of multiple participants about risks that exist on Facebook, explore the experiences, opinions and various other factors that influence the behaviour on Facebook. Therefore, we have chosen the qualitative approach elaborated as the interview study inspired by McCracken’s book “The Long Interview” (1988). Our interviews are complemented by analysis of additional data available about participants on Facebook. This type of research methodology is described in Robson’s (2011) Real world research book in category of “flexible designs”. Which suggest that methods, questions and contribution can alter during the process. However, it is crucial to identify the starting point otherwise there would not be anything to alter from. Our study serves the purpose of “analytic generalization” (Robson, 2011, p. 140). The goal is not to generate any statistical generalization of population. Robson (2011) suggest that during this type of research multiple methods to gather data should be used. The details about methods chosen for this study are described in next section.

3.2.2 Empirical Settings

The purposive sampling is used to select the participants for our study. Every participant is university student from Linnaeus university. The age range of participants is between 18-25 years with the demographic consideration of young adult group, and the selected location of residence is Växjö Sweden. We selected the study participants based on demographic range with decided location, age and occupation as main categories. Moreover, mainly the international students for the ease of access are chosen as participants to streamline the process of data gathering. The invitation to participate in a study was communicated either personally or trough Facebook messenger. For the
purpose of our study, students which access Facebook at least several times per week were selected, this intentionally exclude students without Facebook account or non active users which are not in the focus of our study. This selection is made to ensure that results will be comparable. Therefore we will be able to “replicate findings” from our interviews (Baxter, 2008, p. 548). In the table 1 bellow the information about gender and nationality can be found. The green color indicates that participants from corresponding nationality and gender were part of our study and red indicates the opposite.

<table>
<thead>
<tr>
<th>Nationality/Gender</th>
<th>Bangladesh</th>
<th>Canada</th>
<th>Czechia</th>
<th>Germany</th>
<th>Mexico</th>
<th>Poland</th>
<th>Sweden</th>
<th>Turkey</th>
</tr>
</thead>
<tbody>
<tr>
<td>Woman</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Man</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Table 1: Participants gender and nationality*

It is clear from table 1 that in our study we gathered information from 10 participants with variety of nationalities. The gender attendance is not absolutely equal however any significant influence of the participant’s gender was not observed. The main part of our data generation process including interviews and data gathering from selected student’s profiles was conducted during March 2016. The process of data gathering was followed by data analysis process both of these are described below.

3.3 Methods/Techniques for Data Collection and Analysis

3.3.1 Interview

During the interview we will ask about general attitude towards Facebook and potentially also other social media sites which could affect their relation to privacy and security in online space. Our main focus during the interviews will be students’ perception of possible risks social media could cause, their awareness of privacy issues and knowledge about how to avoid risky behaviour. Crang (2007, p. 60) mentions that interviews can range from “highly structured” to unstructured. Interviews conducted in this case will be in the middle of this range with several prepared questions which will generate further discussion about the topic and therefore fits into category of semi-structured interviews. The topics for discussion are as follows:

- general sharing behaviour
- attitude towards online privacy when sharing personal information
- currently practiced methods of protection
- perceived benefits
- awareness of potential privacy risks
- knowledge about potential privacy risks
- Perceived improvements of privacy situation

During the process of question creation several aspects were considered. It was important that every question except several warm-up question is connected to our
research questions. Following the suggestions from Robson (2011, p. 282) we aimed for short, unbiased questions created without any words potentially unknown to participants. Furthermore we tested our initial set of questions on three volunteers. Thanks to these testing interviews which are not included in our results we further adjusted the questions. We analysed if questions included in first set lead to answers for our research question and also the feedback from participants were taken into account.

All of the interviews were conducted face to face on Linnaeus university campus. The exact time and location was negotiated with interviewed participant with focus to find most suitable settings for him/her, so they feel comfortable and have enough time. At the start of every interview was every participant asked if he/she agrees with the recording. In addition to the voice recording the notes were made during the interview. The transcription is not required immediately but the process of notes summarization should follow closely after the interview to gather main ideas discussed in the interview. At the same time as summary session, the exclusion of unimportant data will take place. This process however must very carefully consider that even on first sing unimportant data could gain some meaning later in the study.

### 3.3.2 Data Analysis

Since SNSs serves as very convenient way to share big amount of multimedia content as well as friendship lists and many very personal information about the individuals, all of these aspects will be analysed and the amount of content shared on Facebook profile will be taken into consideration. Moreover, the privacy settings of participant’s will be examined to observe if the default settings have been changed. For example through tagging, one can have photographs linked to his profile even without actually sharing anything by himself/herself. (Patsakis et. al., 2014, p. 523) This way we will be able to examine the difference between what students share to public and what is shared only among their friends and that will help us to gather information about which type of information is important for them to stay out of the public sphere. This approach is raising many ethical questions on the both sides, not only for the researched individuals but also for the researchers. This issue is further developed in ethical considerations section. It is very important to use this method to complement our understanding of user’s attitudes and perceptions from interviews. Furthermore, it will help validate the concepts proposed by interview analysis. The type of data that will be analysed:

- Personal information (e.g. home address, phone number)
- Amount of multimedia content
- Type of multimedia content
- Number of likes and shares
- Number of friends and friend list visibility
- Privacy settings

We will gather the needed information about participants with help of “Download your information” function that is provided by Facebook for every user. As shown on figure 5, the file provided by Facebook includes many useful information about our participants, for example the information about deleted friends, not accepted friend requests, frequency and time of logins, multimedia content hidden even from friends and many more. The file includes also all the messages participants send during their Facebook usage. Due to the fact that these messages are perceived as very sensitive and
are not in our interest during this research, participants are free to delete this part of
document provided by Facebook.

Figure 5: "Download your information" page

3.3.3 Analysis

In the process of data analysis which's main part will follow directly after the data
generation phase will be done according to Lichtman’s (2013) six steps description:

1. Initial coding. Going from responses to summary ideas of the responses
2. Revisiting initial coding
3. Developing an initial list of categories
4. Modifying initial list based on additional rereading
5. Revisiting your categories and subcategories
6. Moving from categories to concepts

The audio recordings from interviews were divided into 2 groups randomly and each
member of research team transcribed one of these groups. The transcription was
conducted as close to actual interview as possible. The same interviews that were
transcribed by one of the researcher were also coded by him/her. The codes were then
revisited and relevant categories developed, during this process some of the irrelevant
codes were excluded from the data set. The created categories were discussed, modified
and the hierarchy of main categories with subcategories was made. This process was
followed by session during which the main concepts were identified by combination of
several categories. The importance of individual categories and the possible connections
between them were discussed. The most important concepts related to the research
question were selected.

These concepts were complemented by data obtained from students Facebook profiles
to validate our findings and further develop the understanding of student’s perception of
studied issues with privacy and risks encountered during usage of Facebook.

3.4 Validity and Reliability

During a research process we face many challenges that potentially endanger the quality
of results. To consider results good they must be valid and reliable, as stated in
Silverman (2013, p. 301) the “validity is another word for truth” and “reliability refers
to degree of consistency” present in coding an analysis. In other words validity indicates how solid are our assumptions and if they are trustworthy. The reliability indicates how coherent are decisions made during the research process and especially the analytical parts of it. For every research it is important to ensure the validity and reliability as without them there is no reason to publish it at all. The issue of validity in qualitative research can be approached in many ways. The efforts have been made to use “the refutability principle” and “The constant comparative method” described in Silverman (2013, p. 301). The basic interpretation of the refutability principle is the need to refute the initial assumptions generated from gathered data. Assumptions were subject of debate between both researchers throughout the all discussion process. During these discussions the findings from different cases were compared with effort to identify the concepts relevant for our focus, also the “the principle of multiple interpretations” naturally occurred, as several points of view were considered many times (Klein and Myers, 1999). Moreover, during the analysis process also the other 6 principles defined in Klein and Myers (1999) article were kept in mind to ensure the validity of our research.

The proper description of our empirical settings, methodology and analysis process is provided as part of our study to improve the reliability of our results. The process of coding, categories and concepts creation was based on Lichtman’s (2012) description. This method of analysis was studied by both researchers at the same time to ensure the consistency of coding and category creation throughout our work.

3.5 Ethical Considerations

Before the start of research process, it is very important to consider ethics for every research carried among people, it is even more important when the focus is on privacy and risks perception of college students. According to Codex.vr.se (2016) these are the main points every participant has to be informed about in the informed consent:

- the overall research plan
- the aim of the research
- the methods to be used
- the consequences and risks that the research can entail
- who the principal investigator is
- the fact that participation is voluntary
- the fact that the subject has the right to cease participation at any time

Therefore the informed consent will be created containing sufficient and precise information about our research plan. In this consent the information about aim, methods, possible consequences, risks, identity of investigators, voluntariness and possibility to withdraw at any time will be described. As suggested by Wiles et al. (nd, cited in Robson 2011, p. 203) this consent should not extend one page since that could overwhelm participants.

It is also essential to consider ethics of researchers themselves. During the research process we will work with private personal information of participants and it is therefore crucial that we apply effective anonymization techniques and use data in consistency with the Swedish Personal Data Act (PUL).
4 Empirical Findings

In this section, we will present all critical findings based on our research methodology and strategies as introduced in the previous section. The results are based on two main research methods that are semi-structure interviews and data analysis in order to give reliable answers to our research questions. Therefore the analysis is relied on the material of all interview transcripts by approved voice recordings and Facebook data file that was provided by our participants. As described, the research objectives are ten university students who are between 18 to 25 years old and study at Linnaeus University In Sweden. All participants are selected with the balance between genders, cultural and educational background. As agreed with participants, they are anonymous in our research and will be named by numbers only, such as Participant 1 to 10. For protecting participants’ privacy and based on the principle of research ethics, in some parts of the analysis, their number will not be appeared with specific marks or opinions from them.

4.1 Data Collection Process

During the research process, the most time consuming step was the data collection. For interviews, we scheduled date and time with each participant and booked a room to initiate the interviews. Before we meet participant, we had a general introduction for our research topic and sent the consent document to participant to find out if they are interested to take part in the research. In the beginning of the interview, one of us was responsible for the introduction of the research that includes the focus topic, noticed that there are approximately eighteen questions and it might take thirty minutes long. We even informed participants about our roles during the interview, that one researcher is guiding the conversation and the other one will take important notes. This was a very important step for our participant to have a concrete idea what is going on. All the ten interviews were successfully carried out and the length is between twenty-five to fifty minutes. It is important to mention that after two interviews we have conducted, we decided to add a question which was “what is privacy mean to you?” in the end of the interview, because we realized this will be a very good question to understand each participant’s privacy boundary in order to have a fundamental understand of their privacy knowledge and risks perception, etc. However, we decided to stay with ten participants for interviews instead of involving more participants because it is believed that there was nothing new can be added on for the material after ten interviews.

According to our techniques to analyse interview in qualitative research, there are six steps within three C strategy—coding, category and concept, we have found approximately 100 codes and twenty-nine categories, which in the end we deleted some irrelevant and less interesting categories in relation to our major research focus. As results, we have identified seven crucial concepts that conclude twenty-one categories in total, three categories for each concept as shown in table 2 and 3. These seven concepts are: **Necessity of communication and connection**, **Knowledge of privacy risks**, **Acceptance of personal data usage**, **Individual privacy boundary**, **Personal information control**, **Maintain balance usage** and **Choice and prepare for consequence**. Gladly, through these concepts we found answers for both the research questions. The first research question can be answers by the first four concepts and the second research question can be answer by the last four concepts. Therefore the section is divided into two main parts in order to clearly demonstrate how these concepts answer each research question.
Table 2: Concepts and categories connected to RQ1

What are the main reasons for university students to use Facebook despite of privacy risks?

<table>
<thead>
<tr>
<th>Concept</th>
<th>Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>Necessity of Communication and Connection</td>
<td>• Contact Convenience</td>
</tr>
<tr>
<td></td>
<td>• Various Information Access</td>
</tr>
<tr>
<td></td>
<td>• Strong Facebook Culture</td>
</tr>
<tr>
<td>Knowledge of Privacy Risks</td>
<td>• Privacy Awareness</td>
</tr>
<tr>
<td></td>
<td>• Risks Perception</td>
</tr>
<tr>
<td></td>
<td>• Hopping for the Best Scenario</td>
</tr>
<tr>
<td>Acceptance of Personal Data Usage</td>
<td>• Advertising Open-minded</td>
</tr>
<tr>
<td></td>
<td>• Government Access Tolerance</td>
</tr>
<tr>
<td></td>
<td>• Limited Ability to Change</td>
</tr>
</tbody>
</table>

Table 3: Concepts and categories connected to RQ2

How university students’ perspectives of privacy exposure affect the use of Facebook?

<table>
<thead>
<tr>
<th>Concept</th>
<th>Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individual Privacy Boundary</td>
<td>• Individual Definition of Privacy</td>
</tr>
<tr>
<td></td>
<td>• Change According to Environment</td>
</tr>
<tr>
<td></td>
<td>• Trust Friends</td>
</tr>
<tr>
<td>Personal Information Control</td>
<td>• Restrict Shared Content</td>
</tr>
<tr>
<td></td>
<td>• Privacy Settings Management</td>
</tr>
<tr>
<td></td>
<td>• Future Career Concern</td>
</tr>
<tr>
<td>Maintain Balance Usage</td>
<td>• Comparison between Benefits and Risks</td>
</tr>
<tr>
<td></td>
<td>• Evident Positives</td>
</tr>
<tr>
<td></td>
<td>• Hidden Negatives</td>
</tr>
<tr>
<td>Choice and Prepare for Consequence</td>
<td>• Decision-making</td>
</tr>
<tr>
<td></td>
<td>• Change Difficulty</td>
</tr>
<tr>
<td></td>
<td>• Prepare for Consequences</td>
</tr>
</tbody>
</table>

4.2 Research Question 1

RQ1: What are the main reasons for university students to use Facebook despite of privacy risks?

This question will be answered by following concepts:

1. Necessity of communication and connection
2. Knowledge of privacy risks
3. Acceptance of personal data usage

4.2.1 Necessity of Communication and Connection

The first concept that will be introduced is necessity of communication and connection, and its’ key word is necessity. This concept is established by three categories: contact and communication convenience, various information access and strong Facebook
The significant pattern of Facebook as mainly communication, information gathering and social participation, a great communication tool in every day life as most of the participants have described. Even though potential risks exist and possible consequences are connected with the usage of Facebook, participants still perceived the usage of this platform is essentially important, because of it is very necessary to be part of online interaction in today’s modern society. To be part of modern society one has be a part of social media and since Facebook is one of the leading social media platforms with large amount of users, it is very common that people choose to become a Facebook user. To complement the interview results we used the Facebook data file to analyse how often participants accessed the Facebook. The table 4 contains the sum of session update’s and logins in a period of time that was available for analysis in data sample. The presented data indicates that the participants accessed Facebook at least once a day which corresponds with the results we gathered during the interview data analysis. It also indicates that usage of Facebook become a part of their daily routine. Table 4 alone does not provide enough information since it is for example not clear how long participants stayed on the site during average login session, however our analysis of interviews confirmed that it is very common that all the participants have daily access on Facebook.

Table 4: Frequency of Facebook access in certain time period

<table>
<thead>
<tr>
<th>Participant</th>
<th>Facebook access count</th>
<th>Time period</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>160</td>
<td>29/1/2016 - 19/4/2016</td>
</tr>
<tr>
<td>4</td>
<td>259</td>
<td>9/1/2016 - 1/4/2016</td>
</tr>
<tr>
<td>5</td>
<td>257</td>
<td>16/1/2016-23/4/2016</td>
</tr>
<tr>
<td>8</td>
<td>86</td>
<td>1/5/2015 - 19/4/2016</td>
</tr>
<tr>
<td>10</td>
<td>105</td>
<td>30/11/2016 - 15/3/2016</td>
</tr>
</tbody>
</table>

Our interview analysis showed that students, and especially international students perceive the usage of Facebook to communicate with friends as the most beneficial and convenient factor. The opportunity to communicate is not only reflected on the communication with close friends and family, but also with people from different countries in the world. Convenient communication and connection is seen as one of the main benefits provided by Facebook. Moreno et al, (2014) mentions in his article that “social media has changed the landscape for communications”, and Facebook provide its user possibilities which were not available before social media was launched. “It is also good to know what’s going on in their lives, it is important when you are not there”, participant 7 says. Despite the perceived benefits not all of the responses were only positive. Some of the participants expressed that the situation of Facebook as the main platform gives little alternatives since there are lack of comparable platforms. Like participant 4 states, “It is a monopole so I have to use Facebook to keep in touch with my friends”.

24
The second important category contributes this concept is various information access. The usage of Facebook is considered as necessity, it is also because of the possibility to manage and organise diverse groups and through this process gather desired information. Like Participant 8 says, “There is a group, if you are looking for job, internship, you can basically find everything on Facebook. It makes life easier for me”. Also, participants perceived communication as beneficial mainly because Facebook is a central platform that everyone can easily access worldwide. Besides, for being a university student in Sweden, people often found information on Facebook benefits their study and campus life. There are large amount of activities that are initiated through Facebook by school departments and students, and many school faculties have an official account on Facebook to distribute information which is relevant for their education and researches. As Participant 10 explains, “All the exams, hints about the exams, hints about the teachers, that was the main reason... for example to know that some classes were cancel and stuff like that”. As Park’s et al. (2009) states, the reasons why students join the groups on Facebook are the possibility to access the “information about on- and off-campus activities, to socialize with friends, to seek self-status, and to find entertainment”. Just like Participant 4 introduces, “I am looking for a flat in Warsaw and its so easy because I got a lot of feedback from people living in Warsaw or around so I get the inside information the easiest way”.

What we have analysed above with various information access, it seems impossible to talk about it without stress the fact of strong Facebook culture. Because of the social impact Facebook causes, it creates the power of gathering not only different people and various organisations, but also large amount of information. From Participant 2’s perspective, “Facebook has become such a medium for workplaces, campaigns, companies, universities... all the information are usually shared on Facebook”. It is not difficult to see that Facebook itself become a culture, a strong Internet culture.

In conclusion, the benefits of communication and connection, various information access and the strong Facebook culture have built up the necessity usage of Facebook among university students. But it has also been mentioned in interviews that limitations and challenges of Facebook usage are certainly present. Yet the restriction of Facebook usage would cause complications and partial exclusion from modern society. The possibility to communicate with all friends, in case of our participants usually situated all over the world. Very convenient way of managing and gathering every day life information and possibility to easily participate in social life is simply considered as necessary part of student’s daily life and Facebook is perceived as the most convenient way to perform all of these task at one place. This necessity of usage created the environment where the participation is almost compulsory and therefore it is important to develop certain habits to protect private information. For answering the first research question, necessity of communication and connection is considered as the first important reason for users to engage on Facebook although there are privacy risks.

4.2.2 Knowledge of Privacy Risks

Right after the concept of necessity of communication above, we have found another concept that created by three categories: privacy awareness, risks perception, hopping for the best scenario. The crucial word for this concept is knowledge. This concept is one of the critical reasons to answer the first research question. To begin with privacy awareness in general, the pattern shows that most of the participants claim they are privacy concerned, also they realize that private information and shared content on
Facebook is not 100% secured. But not everyone that cares about personal information is being exposed on Facebook because there are different definitions of privacy according to individuals. Privacy boundary differs when people have various understanding of what is considered as private information, and this topic will be expanded in another concept of privacy boundary. Like Participant 5 mentions, “(information) like my location, what I do what I work, things like this, nothing private, nothing sensitive”. As Participant 7 who has different privacy boundary, “I don’t like the concept of privacy on FB, that’s why I don’t share too much. I don’t want to put everything I do there. I don’t want to share everything about me, how I feel on the web”. The awareness of privacy is also affected by users’ increasing age and life experiences. Some participants admitted that they shared more information on Facebook when they were younger, “when I start using FB I was only 17, so basic on that, I just wanted to tell the world everything I was doing”, says by Participant 9. As Participant 7 also states, “When you were younger, you don’t think much about it (privacy). When you grew up and you see something, then you realize it is important to keep some information, not to share to everyone”.

Apart from that, privacy awareness is also highly influenced by user’s education background and perception of risks, to be more specific, perception of privacy risks and/or media technology. Knowledge of privacy risks is crucial because it could impact personal usage of Facebook in terms of information privacy concern. “What you know decide what you do” can be an appropriate phrase to describe the importance of relevant knowledge of information privacy, because it affects user’s actually sharing behaviour and the capability to manage privacy on Facebook. Following table 5 is the education background and level of all the participants.

<table>
<thead>
<tr>
<th>Education background</th>
<th>Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>European social science</td>
<td>Bachelor</td>
</tr>
<tr>
<td>Design</td>
<td>Bachelor</td>
</tr>
<tr>
<td>Mechanical engineering</td>
<td>Bachelor</td>
</tr>
<tr>
<td>Political and cultural science</td>
<td>Bachelor</td>
</tr>
<tr>
<td>Literature</td>
<td>Bachelor</td>
</tr>
<tr>
<td>Political science</td>
<td>Bachelor</td>
</tr>
<tr>
<td>Informatics</td>
<td>Master</td>
</tr>
<tr>
<td>Mechanical engineering</td>
<td>Master</td>
</tr>
<tr>
<td>Economics</td>
<td>Master</td>
</tr>
<tr>
<td>Media technology</td>
<td>Master</td>
</tr>
</tbody>
</table>

As one can see from the table, there are two participants with education background of informatics and media technology and the rest is without or little education of information privacy matters. During the interviews, the two participants with relevant education background of information privacy and technology, exhibited stronger privacy awareness when compared with others. When it comes to potential risks they can also recognize more according to their rich knowledge of privacy issues. So as one of them points out,
“In the privacy policy, Facebook has right to collect information about you, even outside of Facebook, they can collect your credit card information about you, things being published in a magazine online and offline, they have right to collect any public information about you.”

Another participant emphasises, “It (personal data) won’t be permanently deleted. It is store somewhere, and there is a data server on Facebook. You can deactivate it...max, but the data will be there, they can find it in many archives. That’s how it works”. Other participants without concrete education of privacy or media technology do not have significant differences in terms of privacy awareness, but in general they have little knowledge of possible risks and consequences. “I don't feel like I am at risks...from the information that is so far shared about me on Facebook but...No, no, I don't feel like I am at risk”, participant believes.

Speaking of hopping for the best scenario, even though the majority of the participants are considered as privacy concerned, the frequency of their usage and the large amount of information they share on Facebook somehow does not 100% match what they expressed during the interviews. Large amount of personal information is still shared on Facebook. One of the main reasons is the attitude of hopping for the best scenario, because it is based on the needs of communication and connection as described in the Necessity of communication and connection concept. Besides, the desire of being part of trended social lives in the today’s social media culture, as well as the addiction of being self-expressed and online journalist, these factors also play critical role of their active engagement on Facebook. Therefore even users with privacy awareness and certain risks perception, all the influence aspects give a comprehensive understanding of user’s not matching behaviour based on their privacy attitude. At this point, hopping for the best scenario naturally takes the place in user’s continuing and active usage on Facebook, because of that they tend to ignore relevant risks. Participant 4 says, “Sometimes I just try to not worry about privacy stuff because I think in the end everyone is on Facebook, and some people share more so you always think like you are on the safe side”.

However, based on the analysis for the concept of risks knowledge, we can see the other reason why user decides to user Facebook even privacy risks are existed. From the analysis, one can see there is certain degree of privacy awareness among the participants and they realize the importance to have risks perception. But in the meantime, users carry limited amount of knowledge for media technology, as well relevant risks and consequences. Sometime, users intend to ignore privacy risks. Hopping for the best scenario automatically became the main psychological support for their involvement on Facebook. These factors constitute user’s common perception of privacy risks, which gives answers to the first research question in a good way.

4.2.3 Acceptance of Personal Data Usage

As the other main concept we have found from the pattern that can answer the first research question is, acceptance of personal data usage. The key word of this concept is acceptance, and it is created by three identified categories: advertising open-minded, government access tolerance and limited ability to change. The concept demonstrates what level participants can accept in terms of their privacy information is being used. In
other words, it illustrates how much privacy invasion can reach user’s tolerance. On Facebook, there are different kinds of advertising is shown on user’s News Feed depends on whether that user fits to a description set by an advertiser (Facebook, 2016). To be more specific, Facebook delivery ads to its users according to their online interests-based on one’s activities on websites or applications outside of Facebook. What Facebook does is called Online Behavioural Advertising (OBA), a term which is commonly used in today’s Internet marketing field. This kind of the targeting behaviour has raised privacy concerns, because “…behavioural targeting makes use of predictive data derived from user’s’ online behaviour” (Beales, 2010, p. 2). The method of OBA is about “advertising networks profile a user based on his or her online activities, such as the websites he or she visits over time” (Ur et al, 2012, p. 1). Some of the participants express their generous understanding because they believe that Facebook has to gain profits in order to run the company, and selling users data is one of them. More, several participants would rather perceive their privacy data that used by Facebook is one way users paid for the free service. “…there is never free service, you have to pay in someway”, Participant 7 believes. “Facebook has to make money somehow, and your information is how you pay”, said by Participant 9. And Participant 4 also believes, “In today’s information age, personal information is money”.

In addition, some of the participants even appreciate the ads on Facebook, because it provides alternatives, information and convenience for their needs of targeted shopping. Sometimes, advertising could also deliver information for their potential desire of purchasing. A participant who is entrepreneur says that, “I don’t mind advertising, sometimes they sent me interesting ads… it is benefits for me”, this participant further explains, “I can just delete some additional emails if they are not interesting or disturbing, it is not much work to do anyway”. The following table 6 indicates how many ads topics Facebook assigned to each user and how many times they have clicked on the ads within a certain time period. According to the data, it is interesting to see there is only one participant within the group who has never clicked on any ads that pushed by Facebook. And we have learned that this participant is the one who has particular privacy education.

<table>
<thead>
<tr>
<th>Participant</th>
<th>Topics</th>
<th>Clicked Ad count</th>
<th>Time period</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>191</td>
<td>21</td>
<td>31/1/2016-25/3/2016</td>
</tr>
<tr>
<td>4</td>
<td>132</td>
<td>4</td>
<td>15/3/2016-20/3/2016</td>
</tr>
<tr>
<td>5</td>
<td>209</td>
<td>0</td>
<td>N/A</td>
</tr>
<tr>
<td>6</td>
<td>185</td>
<td>11</td>
<td>14/2/2016-4/4/2016</td>
</tr>
<tr>
<td>7</td>
<td>182</td>
<td>58</td>
<td>15/2/2016-4/4/2016</td>
</tr>
<tr>
<td>9</td>
<td>27</td>
<td>10</td>
<td>22/2/2016-7/4/2016</td>
</tr>
</tbody>
</table>

Acceptance of data usage also refers to the tolerance of government access citizens’ data on Facebook. This finding is mainly based on the responses from interviews. Perspectives from participants at this matter are generally acceptable, or they feel it is difficult to have a clear line for whether they should reject it or happily accept when
government would like to use their data for certain reasons. Even government authorities often claim that personal information access or data collection of citizens on social media is for ensuring state security or criminal investigation. Although, in one way, it is sort of citizen’s responsibility to assist authorities for state safety, but in another way, this reason cannot become an excuse to invade citizens’ privacy without ethics and limitation. As Participant 1 says it is acceptable for government to access personal data for security since it is more important than personal privacy, and Participant 5 points out that there should be a balance of accessing personal data no matter from third parties or government sides. Also, Participant 9 has similar opinion, “I don’t think it is morally correct but that is what happening now”.

Furthermore, another important factor that affects their acceptance perspective of privacy data usage is users’ limited ability to change against the situation of how personal data is being collected or used without user’s agreement. Most of them think, “There is nothing I can do about it” to show their defenceless place. Besides, individual users’ vulnerable position also refers to other parts of privacy data collection by Facebook or third parties. Like Participant 7 says, “I don’t accept it (personal data collected or used by Facebook, third parties or government authorities), but not much I can do about it”. “I accept it as it is. I don’t say I am super happy about it but I just have to take it if you want to have some social live”, said by Participant 6. Participant 11 also states, “I don’t like it, but I accept it”. One can see how users feel about restricted capability to do anything to defend themselves from this kind of the privacy invasion.

However, with all the analysis above regarding to the concept of acceptance of private data usage on Facebook, it is kind of forced acceptance to some certain extent. Based on their generous understanding of Facebook’s necessary profits through business and advertising, and when considering it is the way to exchange all benefits Facebook has provided. As the table above has shown, one can see the open-minded level for their acceptance of advertising. Beside the acceptance of advertising, the result also indicates user’s tolerance of government data access for security reason but also reflected on his/her vulnerable position to change the situation. This concept of acceptance of personal data usage have shown the other important reason why user continuously engaged on Facebook even though relevant risks could occur for their exposed privacy.

4.2.4 Conclusion for RQ1

To summarize how these three concepts have answered the first research question: What are the main reasons for university students to use Facebook despite of privacy risks? Three concepts are introduced: necessity of communication and connection, knowledge of privacy risks, and acceptance of personal data usage. First of all, as university students, the participants consider that the use of Facebook is a necessity based on their needs and desire of online communication, connection and information access, as well as the influence of Facebook popularity. Although privacy risks on Facebook takes certain places that should be concerned. Yet the use of Facebook has already became a part of their daily lives based on necessary online communication involvement. Secondly, as the other important reason to use Facebook despite of privacy risks, participants have certain extent amount of privacy awareness and risks knowledge. In general, participants claim that they are privacy concerned but from the analysis, we found out their relevant risks knowledge is fairly low. It is affected by their life experiences and educational background. Participants with particular education of
privacy and/or media technology have higher risks knowledge. As the third major reason, participants are aware that their personal data is mainly used for business such as advertising, for which they express the acceptance based on the understanding of Facebook’s necessary profits to offer free service. The generous acceptance also refers to government access for state security reason, but the one of the reasons for their acceptance of personal data usage is user’s limited ability to do anything against the situation. Even privacy risks exist but user still decide to use Facebook is partly because of their acceptance of certain risks, and these kind of the risks are reflected on personal data usage or access by Facebook, third parties or government authorities. All in one, despite of privacy risks the main reasons for university students to use Facebook are the necessity of online social interaction in today’s modern society and, certain privacy knowledge to handle potential risks, as well as user’s generous acceptance of personal information that used by different parties.

4.3 Research question 2

RQ2: How university students’ perspectives of privacy exposure affect the use of Facebook?
This question will be answered by following concepts:

1. Individual privacy boundary
2. Personal information control
3. Maintain balance usage
4. Choice and prepare for consequences

4.3.1 Personal Privacy Boundary

To begin with the first concept individual privacy boundary, it includes three categories: individual privacy definition, change according to environment and trust friends. The key word of this concept is boundary. First concept gives the fundamental understanding for user’s perspective of their privacy boundary. During the interview, we can sense that privacy has different definition according to individual’s value. Each participant’s privacy definition gives fundamental understanding of what is his/her boundary for privacy, for instance privacy definition in general and in online environment such as Facebook platform. This boundary sets the limit for every individual user of how much and which type of information is acceptable for her/him to intentionally share. It has been observed that this boundary is very flexible and highly depended on variety of factors present in one’s life. The most influential factors has been identified is environment, available technology and knowledge of possible privacy risks. Through the analysis of their profiles data and relevant findings can be seen in tables 7 and 8, they illustrate which information commonly present on Facebook profile is perceived as private enough to make it visible only for friends. Table 7 presents what information is available on public profiles that are accessible for every Facebook user, and table 8 demonstrates information that is available only for their Facebook friends. In these two tables, ✗ means information is not available and ✓ refers to information that is available. It is evident that eight participants out of ten are generous to share information about their education and/working places, but information about family and information that is more than profile and cover photo are only available just seldom.
It is obvious that user’s sharing attitude towards certain information is more open to friends they have on Facebook. It is important to mention that the categories as shared at least partial information has presented on participant’s profile. For example in terms of family information, it means at least one family member is presented instead of completed information about family members. Table 8 also demonstrates the number of pictures that are available on participants profiles varies with large extend. This information shows the difference each participant privacy boundary in sharing personal information and life photos. Interestingly, when every participant had the question of “do you consider yourself over sharing?” all the answers were no. Their answers prove the different privacy boundary one has, but it can also implies the low privacy risks one perceive.

Table 7: Information shared publicly

<table>
<thead>
<tr>
<th>Participants</th>
<th>Family information</th>
<th>Full friend list</th>
<th>Places lived</th>
<th>Education and/or work</th>
<th>More than profile and cover picture</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>x</td>
<td>x</td>
<td>v</td>
<td>v</td>
<td>x</td>
</tr>
<tr>
<td>2</td>
<td>v</td>
<td>x</td>
<td>v</td>
<td>v</td>
<td>x</td>
</tr>
<tr>
<td>3</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>4</td>
<td>x</td>
<td>v</td>
<td>v</td>
<td>v</td>
<td>x</td>
</tr>
<tr>
<td>5</td>
<td>v</td>
<td>x</td>
<td>v</td>
<td>v</td>
<td>x</td>
</tr>
<tr>
<td>6</td>
<td>v</td>
<td>v</td>
<td>x</td>
<td>v</td>
<td>x</td>
</tr>
<tr>
<td>7</td>
<td>x</td>
<td>v</td>
<td>v</td>
<td>v</td>
<td>x</td>
</tr>
<tr>
<td>8</td>
<td>x</td>
<td>v</td>
<td>v</td>
<td>v</td>
<td>x</td>
</tr>
<tr>
<td>9</td>
<td>x</td>
<td>v</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>10</td>
<td>x</td>
<td>v</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>

Table 8: information shared with friends (*has albums with multiple participants)

<table>
<thead>
<tr>
<th>Participants</th>
<th>Family information</th>
<th>Full friend list</th>
<th>Places lived</th>
<th>Education and/or work</th>
<th>Privately has similar number of pictures</th>
<th>Number of shared pictures exceeds</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>v</td>
<td>x</td>
<td>v</td>
<td>v</td>
<td>x</td>
<td>100</td>
</tr>
<tr>
<td>2</td>
<td>v</td>
<td>x</td>
<td>v</td>
<td>v</td>
<td>x</td>
<td>750</td>
</tr>
<tr>
<td>3</td>
<td>v</td>
<td>v</td>
<td>v</td>
<td>v</td>
<td>x</td>
<td>450</td>
</tr>
<tr>
<td>4</td>
<td>v</td>
<td>v</td>
<td>v</td>
<td>v</td>
<td>x</td>
<td>50</td>
</tr>
<tr>
<td>5</td>
<td>v</td>
<td>v</td>
<td>v</td>
<td>v</td>
<td>x</td>
<td>450</td>
</tr>
<tr>
<td>6</td>
<td>v</td>
<td>v</td>
<td>v</td>
<td>v</td>
<td>x</td>
<td>2500*</td>
</tr>
<tr>
<td>7</td>
<td>v</td>
<td>v</td>
<td>v</td>
<td>v</td>
<td>x</td>
<td>150</td>
</tr>
<tr>
<td>8</td>
<td>x</td>
<td>v</td>
<td>v</td>
<td>v</td>
<td>x</td>
<td>150*</td>
</tr>
<tr>
<td>9</td>
<td>v</td>
<td>v</td>
<td>v</td>
<td>v</td>
<td>x</td>
<td>50</td>
</tr>
<tr>
<td>10</td>
<td>x</td>
<td>v</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>350*</td>
</tr>
</tbody>
</table>

As the other important category that supports this concept is change according to environment, the evident can be found both from data analysis and interviews. As some of the international students explain, their sharing behaviour changed since they moved to Sweden. It is shown from their Facebook data file that there is a significant part of
pictures were shared in Sweden, this influenced factor has also been discussed during interview conversation when participants described that information they share is affected by environment they live in. “I only do it in Sweden at home not so often”, says by Participant 1. “...all my new friends were sharing all the time so you felt a bit odd when you don't share stuff or you don't discuss with them on Facebook, But it is not the same in Germany”, says by a German participant. This has to do with the strong Facebook sharing culture in Sweden as presented in the earlier concept. Also, one’s sharing behaviour gets influence also depends on the community they live offline and online. In other words, what they share and how they share can affect by their campus life and friends he/she has on Facebook community. As Participant 6 expresses, “I share things by watching what my community normally share or don’t share”. “I was kind of forced by the situation because all my friends were posting things regarding their studies and their campus lives on Facebook”, says by Participant 10.

Another factor that influences how much participant shares personal information on Facebook is the enormous technology development in recent years. The quality of cameras presents in today’s smartphones and the accessibility of mobile Internet play an important role in the amount of information user decides to share. This factor can leads to extension of their privacy boundary just because it is convenient to engage more on Facebook with dynamic content possibilities to share. Like Participant 6 says, “I didn’t have the media to make the pictures in good quality and post it immediately”. And Participant 6 also admits, “I share more now because we have the technology, it is easier to share video or something you record with your phone. Ten years ago, smart phone was not for everyone yet”.

Besides, we have found one more factor that shapes participants’ privacy boundary is: trust friends. Trusting friends on Facebook is an important aspect that influences individuals’ sharing behaviour. To some certain extent, how user build up privacy boundary very much depends on what friends they have on Facebook. “I trust my friends on Facebook in general. I mean they are all people I know personally”, Participant 10 emphasises. “I don’t have restriction to agree with every picture that I’m tagged. I believe that my friends will not post harmful pictures regarding to me, or at least not so often”, says by Participant with laughs.

Overall, it has been identified that participants’ privacy boundary varies depends on individuals’ value, different participant has his/her own definition of privacy. More, privacy boundary affects by their changed environment when Facebook using culture gets stronger in Sweden, and changes also happened according to their community as a student when most of the their surrounding people is engaged on Facebook. Further, technology possibilities offers another trend of active sharing when smartphones and mobile Internet access is widely covered. Together with the factor of trusting friends on Facebook the privacy boundary gets even larger. At this point, we can say that participants’ privacy boundary extended and it can adjust the principles in their original privacy definition. To answer the second research question, individuals’ privacy boundary gives basic understanding of what are the privacy principles according to different individuals. One can identify that user’s privacy boundary is one of the essential aspects that affects their actual engagement on Facebook in terms of privacy concern.
4.3.2 Personal Information Control

The concept of personal information control includes three categories that are: restrict shared content, privacy setting management and future career concern. The key word is control. The concept represents the attitude towards users’ personal information control in relations to the shared content. It also describes methods participants use to control the information they share and information other users might share about them on Facebook. It has been already presented that usage of Facebook is perceived as necessary part of daily life and therefore it is important to maintain a certain level of control over the information they decide to share and/or others decide to share about them. In the second scenario, the ability to control what other users share about them are very limited. First category describes ways participants use to limit the amount of information that is available about them on Facebook and also the limitation of audience that can access it.

The privacy settings management is clearly very important for every privacy-concerned individual and proper management will certainly help to keep required control. Facebook offers possibilities for customized privacy settings according to user’s needs. These privacy settings are mainly about assigning people into different groups such as friends, family or colleagues; and the restriction of whom can access user’s profile or specific shared content. According to most of the participants, one of the effective ways to maintain control over their private information is to limit people who have access to it. For example, it is important to carry regular control of who are in their friends list and, to delete irrelevant friends from time to time. Table 9 contains number of friends each participant has deleted from their friends list. As the table illustrates, one can see how much the management of controlling friends list is used. It is important to mention that the numbers of current friends is not the exactly correct because we intentionally made it as a rounded number in order to maintain higher level of participants’ privacy, since the exact numbers would not benefit the validity of this example in any way.

<table>
<thead>
<tr>
<th>Participant</th>
<th>Current number of friends (approximately)</th>
<th>Removed friends</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>600</td>
<td>6</td>
</tr>
<tr>
<td>2</td>
<td>700</td>
<td>440</td>
</tr>
<tr>
<td>3</td>
<td>500</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>550</td>
<td>43</td>
</tr>
<tr>
<td>5</td>
<td>1000</td>
<td>63</td>
</tr>
<tr>
<td>6</td>
<td>1100</td>
<td>111</td>
</tr>
<tr>
<td>7</td>
<td>1750</td>
<td>252</td>
</tr>
<tr>
<td>8</td>
<td>200</td>
<td>1</td>
</tr>
<tr>
<td>9</td>
<td>1300</td>
<td>9</td>
</tr>
<tr>
<td>10</td>
<td>200</td>
<td>2</td>
</tr>
</tbody>
</table>

From the table we can see that not all participants manage their friends list and to remove friends on Facebook. At this point, it might be difficult to imagine the exact reason of why some users delete more friends and some of them barely do it. For some of the participants could be that this process is not needed since they consider precisely
whom they will add to friends list at the first place. Yet for some participants, this method is important since they deleted more than 100 users from his/her friends list. There can also be the case that when participants neither want to remove friends nor share previously posted content they would just make specific content only visible themselves. As Participant 1 states, “for example there are people I used to be good friends with but after some years we are not very good friends anymore and I don't want to have it public but I want to have it as a memory because it was a good time”.

Moreover, for seeking more evident for this research, we have also asked participants to provide the screenshot of their privacy settings. Through screenshots, two main groups of their privacy settings were identified. One group of the participants did not change their privacy setting from default settings, which means they allow everyone that can access the Internet to view all his/her profile information on Facebook such as email, phone numbers and birthday. Also, within this group, every participant has the option to link search engines outside of Facebook to his/her profile was set as “yes”. In contrast to this, participants from the other group has changed the privacy settings from default ones, which it does not allow searching possibility to find his/her email and phone number that are posted on Facebook profile since this information was restricted only to Facebook friends. The example of the second group can be seen in figure 6.

One of the main identified reasons why participants do not want to have their profile linked to search engines was the future career concern. Some of the participants especially explain that their concerns about future employer would have the possibility to seek for job candidate’s information easier online if they made their personal information public shared, or if they do not have an efficient privacy setting management on Facebook. Participants are aware of this a reality that has been reported several times by media. There were employers who intentionally checked job candidates’ social life information through their Facebook account and these cases are no longer news in the society. Based on that concern, Participant 1 says, “I want to be serious when my employer has a look at me or something like that”, “Things you share would affect your future job”, says by Participant 8. Participant 2 also underlines that “I make sure that they cannot Google me”.

<table>
<thead>
<tr>
<th>Privacy Settings and Tools</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Who can see my stuff?</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Who can contact me?</strong></td>
</tr>
<tr>
<td><strong>Who can look me up?</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

*Figure 6: Example of changed privacy settings*
In all, personal information control is the concept that covers variety of possible approaches how one can limit the amount of information available about him/her on Facebook, as well as their privacy attitude behind, such as their concern of future career. The restriction of shared content tells participants’ consideration of what to and not to share. Together with proper privacy setting management it helps the efforts of controlling personal information to a great extent. As another common concern of future career builds up this concept since the relevant attitude affects user’s decision of what information should be available on Internet through their use of Facebook. The concept gives response to the second research question, that personal information control is one of the key aspects that impact their use of Facebook. The control is mainly based on user’s attitude towards how one should restrict shared content and privacy setting that offers by Facebook, as well as their further career concern. However, an effective personal information control will be able to support their usage of Facebook to maximize the benefits without losing control of their privacy.

4.3.3 Maintain Balance Usage

The concept of maintaining balance usage includes three categories: comparison between benefits and risks, positive influence with evident and hidden negatives impact. The key word for the concept is balance. As analysed earlier, each participant has his/her own perception of risks and list of identified benefits when using Facebook. The comparison between benefits and risks is one of the main factors that affect their use of Facebook. Some of the participants believe it is important to keep balance in relation to their utilization of Facebook. In order obtain the positive influential usage from Facebook service without giving away too much privacy, it is very important to have the knowledge of consequences to balance the benefits and risks. As Participant 5 underlines, “you have to be aware of some people are often share too much on FB without knowing the consequences, only you know what you are doing, how to escape”. It means that one has to find the balance point based on his/her individual privacy value. The value determines the boundary of one’s privacy and it impacts all relevant decision-makings in how one should engaged on Facebook. Also, how users balance between benefits and risks decides the balance of actual performance on Facebook, for example how often and how much they share, what to share and share with whom. If one perceives risks or consequences are more than what Facebook offer as benefits, then relevant changes would be conducted to maintain enough control and to “escape” from potential risks or consequences.

In addition, the finding also shows that positive influence plays a vital role in their active engagement on Facebook. We have found in many cases that participants perceive more benefits when using Facebook with large amount of visible evidence such as convenience communication and connection between individuals, public figures and all different organisations from everywhere in the world. Users believe their use of Facebook is positively influenced with those evident benefits. Like we have analysed in the very beginning, Facebook usage became a necessity and it thus motivates further involvement. From another perspective, users prefer to see benefits more, since risks and consequences are somehow hidden in a way that are distance from them. As risks are hidden so the influence is not as strong as with benefits. Also, the probability of consequence would affect an individual is still relatively small when compared with all the positive impacts that one can easily identified. This perception of balance being more in favour of benefits establishes an environment where users tend to be more
Participants’ activity is illustrated in table 10 that contains information about their timeline activities and one can see how active each participant engaged on Facebook. In this table, the timeline action includes:

- went to an event and/or interested in an event
- added to groups
- are now friends with someone
- likes
- picture posts
- added a new video
- in “location”
- reviewed
- updated profile picture
- updated cover photo
- listened songs on Spotify

<table>
<thead>
<tr>
<th>Participant</th>
<th>Timeline actions</th>
<th>Time period</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1520</td>
<td>8/5/2010-25/3/2016</td>
</tr>
<tr>
<td>4</td>
<td>868</td>
<td>13/2/2010-31/3/2016</td>
</tr>
<tr>
<td>10</td>
<td>712</td>
<td>8/7/2013-13/4/2016</td>
</tr>
</tbody>
</table>

Besides, user tends to believe that their personal data is not important or interesting since he/she is an ordinary person in the society. Like Participant 2 states, “because of my position in society that I am an average student who don't really have a place in public eye, I don't work within a field where my personal information would be any value”. Participant 5 also says, “what are they going to do with my data if I’m not the folk”. “I don't think there is someone sitting there twenty-four seven to go through my data, they are just too large”, Participant 6 believes. Participants’ privacy awareness is closely connected to their social position, which they don’t consider their exposed privacy on Facebook will cause serious attention or consequences. For the worse case, they will just have to prepare for consequences, and this topic will be deeper analysed in the next concept.

Overall, with the comparison between benefits and risks, participants prefer to perceive more benefits than risks since the negative impacts are hidden. But in the meantime, participants still realize there are definitely potential risks that need to be aware of. Therefore user needs to balance the benefits and risks according to his/her privacy value in order to achieve balance usage. Hence, maintain balance usage is considered as one of the most important perspectives that affect the use of Facebook among university students.
4.3.4 Choice and Prepare for Consequences

The last concept we have identified is choice and prepare for consequences, it is created by three categories: decision-making, change difficulty and prepare for consequences. The key words of the concept is prepare for consequence. To begin with decision-making, the findings have shown the freedom to make personal decision is presented even on Facebook. In general, participants of the study accept that all information is shared voluntarily. It is personal choice that determines how much should one restrict her/his sharing behaviour. Even though it is perceived as necessary to be a part of Facebook everyone still has control over intentionally shared information and therefore she/he should be prepared to face the consequences caused by such disclosed data. Some participants also mention that they have limited competence to change the media technology where shared information on the Internet is impossible to delete. Besides, because of that their privacy definition is changing due to capabilities of modern technologies which also brings the uncertainty about what exactly are the consequences one should be prepare for.

Almost every participant has similar perspective about his or her choices of what and how their private information is shared. Some participants even realize that they also have the choice of not to use Facebook anymore to prevent privacy invasion and relevant risks. Yet the fact of their personal data would not be permanently disappeared even when they decide to delete the account, because the media technology just make it impossible so which makes this choice does not have much meaning for privacy protection. One can certainly decide not to have a Facebook account from the beginning to decrease the possibility of online privacy invasion, but then the relevant benefits of people’s modern lives, such as convenient communication and connection globally, will also be decreased. Besides, if one talks about the choice between different social media platforms than Facebook, it will not make so many differences in privacy exposure. Like Participant 4 express, “You can’t get out of it...you can sit in a forest writing letters and sending pigeons but then you are not a person of the 21st century”. Participant 9 believes that “I could take away my Facebook account, that wouldn’t be very convenient since I already signed up with their little contract. Based on that, privacy is concerning, but not concerning enough, at least for me to get rid of convenient”. Therefore, to be a part of Facebook seems like a simple choice to make for most of the Internet users, especially for young adults as university students.

Moreover, many participants trust their own judgment and believe that most of shared content has defined purpose. The choice to share is commonly justified by usefulness or entertainment for intended audience. As participant 1 says, “I do it to let my friends at home know what I am doing”, and Participant 2 shares “I normally share article or a text that I feel other people could also contribute to or get something from”. If some information is perceived to be potentially harmful in any way and that applies even to the future, participants tend to not share it at all or only in closed groups. “If there is something I don’t want anyone to know I just don’t say it”, says by Participant 3, and Participant 9 states “I have some private groups... friends that I grow up with, I have another private group here that I share with”, This illustrates how some participants make decisions in what should and what should not be shared on Facebook or whether to share it publicly. These day-to-day choices are very important to control the information available about them even in long term.
Further, change difficulty as another important category in this concept, it refers to the limitation and challenges of current situation of Internet based social interactions. The situation where it is not possible to delete any data once shared on Facebook or Internet, and the possibility to spread these data all over the world. The data shared through Facebook will stay their archives and will be available to anyone with required skills, and this situation is very unlikely to change. Once this fact is taken into consideration it becomes clear why it is so important to think about all information that is shared. When we asked participants what they see as possible solution for privacy protecting, they believe that relevant changes to defense online privacy would be very difficult. The Participant 2 says, “I think if you look at the structure...that the entire massive construction of this was build...it is very hard to change it”. Also, Participant 4 states, “We need law changes but somehow I don't see that coming.”

The most critical category in this concept, prepare for consequences is being highly recognized among the participants. It symbolizes the attitude towards their continually usage on Facebook. When standing in front of Facebook’s visible benefits and potential consequences, one rather to enlarge the benefits and ignore the risks or consequences since potential risks are somehow distant from them. Those potential consequences somehow cannot defeat the necessity of Facebook usage. However, the ability to predict future consequences is limited since the possible capabilities of analytical algorithms remain unknown. Besides, future consequences are very important, users might be aware of information once shared on the Internet, but it will never be deleted and what they have shared on Facebook could be used against them now or in the future. Therefore, many participants emphasise that they need to use Facebook to gain benefits although there are potential consequences, and they believe they just have to prepare for consequences for the worst-case scenario.

The uncertainty of future development plays important role on how participants use Facebook. We identified that the awareness about data collection and analysis on social media is perceived as relatively new phenomena and therefore also the consequences are still not clear. “I think we don't know the consequences yet, we don't know how important profiling of people or the behaviour on the Internet is going to be”, Participant 4 expresses. Therefore users believe they normally share content that they could stand for. “I know what I am doing and I should follow the consequences of that based on my own choices”, says Participant 2. Also the Participant 6 thinks “The system is set up for every individual to care about privacy, if you are stupid to post everything that could be used against you, then you probably need a lesson”.

To sum up the concept of choice and prepare for consequences, we have recognized participants realize that there are always choices for whether they should use Facebook, what to share and how much they share on Facebook. Then when they compare the visible benefits provided by Facebook, participants consider it is a necessary decision to be part of modern society. In the meantime, participant also notice the fact that social media environment makes the change of privacy invasion a challenging situation. In general, users believe they can prepare for consequences for the worst cases. In connection to second research question, this concept offers another important understanding of user’s attitude towards privacy exposure on Facebook, it is about personal choice of how to engage on Facebook and prepare for potential consequences. These user opinions impact their continuously usage on Facebook to a stronger level.
4.4.5 Conclusion for RQ2

For the second research question: *How user’s perspectives of privacy exposure affect the use of Facebook?* There are four concepts identified to answer the question: *individual privacy boundary, personal information control, maintain balance usage, choice and prepare for consequences.* Fundamentally, the actual engagement on Facebook is first affected by user’s perspectives of privacy, how one define his/her privacy boundary and it is varied among individuals. User’s privacy boundary can be extended for the reason of changed environment with stronger Facebook usage culture, and their trust for friends. Moreover, individuals’ perception of privacy exposure could build up certain risks knowledge and impact how user implement personal information control through privacy setting management and restrict shared content. Further, participants believe it is important to maintain balance usage of Facebook based on individuals’ measurement between benefits and potential risks or consequences. This is the critical perception from users to affect a positive usage on Facebook without surrounding by privacy risks. Besides, user’s information control is also affected by the concern of career as it could prevent future employers to access information with negative impacts. With enough privacy concerned, a well management of privacy setting can be carried out for maintaining practical control of how personal information is disseminated. Ultimately, user’s point of view of privacy exposure is all about personal decision-making of whether one should be part of Facebook or how much one share and share with whom. And to take part in modern social life and to be involved with the popularly used Facebook became a natural choice among university students. Because of the necessity and benefits Facebook bring, it is believed that users have to prepare for relevant consequences, for the change of Internet based social interaction is relatively difficult. In general, participants believe they can prepare for consequences once for the worse scenario. Overall, users’ perspectives of privacy exposure affect the usage of Facebook significantly. Their privacy attitude decides what and how one should engage on Facebook from different layers as described above, it fundamentally affect the usage under a limited of scope and detail methods of privacy control.
5 Discussions

The discussion section will be divided into three subsections. First, we will carry a deep discussion based on the empirical findings and results that are presented above. The discussion will be presented through our own reflection and understanding of what exactly does the finding have shown and what the results means for the study. Also the connection of these results to presented literature review and previous research will be discussed. Second, besides the seven critical concepts as the main findings, we have also found three special outcomes that are outside of the patterns or general findings. These special outcomes are: misinterpretation, opinion manipulation and no tolerance for government access, which we will conduct a close analysis as well. In the last subsection, we will present general overall reflections based on the findings and outcomes from the detail discussion.

5.1 Findings Discussions

The goal of this study is to gain more knowledge about reasons why the university students use Facebook despite privacy risks. As well as how do the perspectives of privacy exposure affect their usage on this social media platform. These topics are covered by RQ1 and RQ2 with corresponding concepts. In this subsection, we will discuss our reflections about the presented concepts in the empirical findings section, and will further explain the meaning and connection between them.

5.1.1 Discussion of RQ1

*RQ1: What are the main reasons for university students to use Facebook despite of privacy risks?*

First of all it is important to mention the *necessity of communication and connection*. This concept illustrates the importance of these two on desire for an online life in today’s modern society. Obviously the process of communication and connection is not necessarily associated just with Facebook since modern technology provides many possibilities. In current time period and in environment chosen for our study Facebook is one of the most convenient choices among all the social media platforms. We believe that even if Facebook would vanish, another ‘Facebook’ will replace it and it will probably be even more convenient. This belief is based on the needs of communication, connection and social interaction with other people, which is present regardless of available technology (Cacioppo and Patrick, 2009). Since we perceive the usage of Facebook or similar platform as necessity it is very important to ensure that everyone that decides to participate in this system will have proper knowledge of possible risks to avoid the unwanted consequences. After the analysis process we realized that our participants has some basic understanding of potential risks, but they could not express their knowledge or identify concrete privacy risks in a good way. We also noticed that they were not confident in what they say. As example the Participants 8 reaction on question about potential risks “I don’t know really, if someone share too much, people can know everything about it, but how they going to do it, I’m not sure”. These results correspond with previous research conducted by Zhang et al. (2014b) and Ngeno et al. (2010). The difference between these two is that Ngeno et al. (2010) identify users’ awareness of insufficient control over personal information and Zhang et al. (2014b) point out that some users do not even realize the risks of personal information
disclosure. Our results are closer to Zhang et al. (2014b), but limited awareness as described in Ngeno et al. (2010) is also identified. Overall, getting more knowledge about potential privacy risks in the world of social media is certainly one of the possible ways to enhance privacy awareness and personal privacy protection.

One of the general factors that influence how users perceive risks and their sharing behaviour is the strong Facebook culture. Studies that investigate the differences of Facebook usage in different countries have already been conducted, during our study we confirmed that culture differences has direct and significant impact on how users are utilizing Facebook. For example article from Jackson and Wang (2013) describe differences between the usage of SNSs by college students from USA and China, one of the results is that Chinese students use SNSs less since “in collectivistic cultures the importance of the family, friends and one’s groups may be partly responsible for Chinese participants’ lesser use of SNSs”. Although some participants come from countries where the usage of Facebook is not as common as in Sweden, change according to environment happened. Normally, users quickly adjusted their behaviour and started sharing more frequently once they moved to a community with active Facebook usage. It is not necessary to look at such diverse examples as USA and China, the difference is certainly visible even between Germany and Sweden. These two countries are culturally close, yet the difference in Facebook culture is substantial. It is a common practice in Germany that people usually do not use real names on Facebook. Overall, during our research it became clear that Facebook culture is much stronger in Sweden and usage is in comparison to Germany very extensive. Since all the universities, student organisations or companies share so much information through Facebook. This corresponds with previous research where the differences between Facebook usage in UK, USA, France, Italy and Greece were also identified (Vasalou et al., 2010, p. 727). The rejection of Facebook usage would cause complications in order to get these information in a convenient way. “I didn’t use it like a social media really. I started now in Sweden.” says Participant 10. This applies to international students even more than to anyone else, since without Facebook or any other similar platform, it would be much more complicated to create new connections in a country where Facebook takes the dominant place.

Another identified concept is acceptance of personal data usage. It is partially caused by lack of knowledge and partially by users’ understanding that Facebook is a free service and they need to have a profit to run the company. Clearly the usage of personal data is accepted only in certain scenarios, as most commonly mentioned is advertisement, and even for these purposes the type of used data can change the attitude, since the analysis of personal messages is not perceived as acceptable even for advertisement. Facebook even faced a lawsuit once it was accused of possible private message scanning (Raymond, 2014). Participant 3 justifies this attitude as follows, “When we talk about very private things and this is not so much because it is dangerous that they have this information but it is very personal information”. Apart from that, participants express that they have limited ability to influence how Facebook decides to use their data. In general, users feel that they are in a vulnerable position. It leads to the outcome of acceptance even when user realizes their personal data usages are not comfortable.

Even though privacy is changing which we will discuss more later on, it should not be the price we pay for the participation in services such as Facebook or other social media
sites. There is an urgent need to set appropriate rules that will protect vulnerable users against potential invasions of privacy commonly justified by commercial gains. The rules promoting ethical and correct moral usage of data will probably originate from state level but what is even more important is international agreement upon these rules, since it is in the nature of the Internet to ignore or decline the national borders. “Because Internet is worldwide it is a bit lawless and in every country it is a bit different. Every country has its own laws but it is not like everything is specific for the Internet”, says Participant 4. The issue of data protection regulations developed by EU is investigated in Rubinstein’s (2013) article where he argues, “Big Data tsunami is likely to overwhelm these reform efforts”. Rubinstein’s (2013) argues that regulators should cooperate with businesses to enhance the “consumer empowerment”.

While we were searching for the information about participants privacy perception we realized one shift in our own perspective on privacy. Some people say that privacy is dying in today’s Internet driven society (Vlemmix, 2013). While we would not use such a strong words for our findings, the certain change in what does privacy mean in a modern world is certainly happening. As participant 9 says “People are much more willing to share more information”. However, it does not necessarily mean an negative change, as Participant 5 puts it “You can also use innovation to ensure privacy, you can develop software application or other technology to ensure people’s privacy. We should see it this way not the other way around”. So as long as we agree that the meaning of privacy is changing, with proper rules, technology and effort by all involved parties, social media privacy is possible to preserve at least a certain amount of it.

5.1.2 Discussion of RQ2

RQ2: How university students’ perspectives of privacy exposure affect the use of Facebook?

During the analysis of gathered data we came up with previously described concepts which illustrates how participants in our study adjust their behaviour in connection to information privacy risks they perceive on Facebook. All the four concepts are mutually interconnected and influence each other. Once they identify their privacy boundary the personal information control techniques are used to keep the information according his/her boundary. The control over user’s personal information also helps them to keep the Facebook usage balance which is based on choices they make according to the positives and negatives impacts. Throughout the whole process takes place to protect their privacy in present time as well as to prepare for future consequences.

First concept defined in our findings is privacy boundary. This boundary can be seen as an imaginary line which is defined mainly based on perceived risks and benefits which connects this concepts also to first question. The important factor to keep in mind is that boundary is not stable at any time and it moves according to current live situation. For example, when participant moves from a country where Facebook sharing culture is not popular to a new environment where surrounding people are actively engaged on Facebook, his/her privacy boundary expands quickly. This concept corresponds with Communication Privacy Management (CPM) theory developed by professor Petronio (2002). More, it was mentioned by Participant 10 that “some people share everything and they have this public and some people show it only for face to face situations because they don’t want to share it”, which pretty much sums up two opposite
approaches that are possible. We also identified in our results that our participants tend
to trust their friends and this trust also reflects on more open information sharing with
them. The danger of this approach is simple. Not only that users tend to add even people
they barely met, but also the information they share with the “trusted friends” might be
available to friends of their friends. Moreover it is also mentioned by Zhang et al. that
this information could be collected by local service providers (2014b, p. 379). As Post
and Walchli (2016) underlines, SNSs providers encourage user to post personal
information publicly and it raise the concern of whether people will have control of it if
they just rely on the trust of friends. What happen if friends unexpectedly post the
related personal information to public? The effects of inappropriate information control
and trust friends will affect “the way people perceive privacy risks and failures of social
networks” (Post and Walchili, 2016, p. 115). This phenomenon is even more
problematic for international students, because in order to create the new circle of
acquaintances they tend to add everyone as their Facebook friend is the basic social
connection at the new environment they live in.

This unintended loss of control can be mitigated by implementation of methods that are
presented in personal information control concept. This information control is
influenced by many factors which has been previously researched and identified
(Christofides et al., 2009; Peluchette and Karl 2008). The protection of personal
information is clearly important as we could see on reactions when we asked
participants to share the Facebook data file as one of the research methods for our
research. First reaction was usually slightly surprised since none of our participants was
aware of the possibility to gather the data about them on Facebook. Secondly
participants were impressed how much information is available about them. It is
however important to remind that the file provided by Facebook does not contain all
information available about the user. Taking this fact into account it is obvious that even
though participants claim their knowledge and awareness is on good level, the reality is
still more surprising than what is expected. It is worth mentioning the fact that several
participants have slightly changed their behaviour on Facebook after the interview and
confrontation with Facebook data file. Some of the participants after the interview
decided to change their privacy settings to protect their private information. Also, many
of them expressed that this topic is very important and relevant in their everyday life
even though they do not think about it too often. This shows that even when users have
needed knowledge it can be unused because the risks tend to be hidden and benefits are
present much more visible. Therefore we think it is useful to start the public discussions
which could lead to further strengthening of public awareness of online privacy and
social media privacy. The passive knowledge about possible privacy risks is not
sufficient in many cases.

5.2 Special Outcomes

Besides the main findings we have discussed above there are also some special
outcomes we have found during the research process which does not fit in the main
concepts. Therefore, In this section we would like to discuss three special concepts we
have identified based on our analysis that were specifically pointed out by one or few
participants. These special findings are misinterpretation, opinion manipulation and no
tolerance for government surveillance. They will be briefly presented as following.
5.2.1 Misinterpretation

When asked about potential risks participants perceive during usage of Facebook only one of our participants mentioned the possible misinterpretation that can occur if one’s personal information from social media is used incorrectly. The possibility that someone will use limited amount of information available about a person on Facebook and interpret it in a wrong way or that someone could use a quote posted long time ago in different context and by that change the original meaning. These are general examples of misinterpretation mentioned by Participant 2, “if they just would take the random information out of context it could definitely misrepresent people”. Overall it is not just a usage of information from individual users but also the validity of results in social network analysis is very important challenge researchers have to face. Just because we have access to bigger amount of information it does not automatically provide needed validity for our results in same cases it could even be the opposite (Gayo-Avello 2011).

5.2.2 Opinion Manipulation

Next topic that was briefly mentioned by two participants is the possibility to use Facebook as opinion manipulation tool. Participant 10 used example of possibility to use French flag skin over profile picture after terrorist attacks in Paris in 2015. While there is clearly nothing bad about expression of solidarity with victims from Paris, it was mentioned that the inability to create similar skin also for other countries affected by terrorist attack “is kind of influential for the way people think” (Participant 10) in certain situations. This example shows how Facebook itself is able to create opinion trends in a society. One of the former Facebook employees even claims that Facebook “routinely suppressed news stories of interest to conservative readers” (Nunez, 2016)

Speaking of influence and opinion manipulation it is important to keep in mind the third person effect (TPE) which describes how users fell “invulnerable” since risks are mainly affecting others (Paradise and Sullivan, 2012).

5.2.3 No Tolerance for Government Surveillance

As one participant said, “I knew that company could collect those things. but government, that’s more concern for me than other companies”. This attitude is partly caused by the special political situation at this participant’s country and also by number of interventions government tend to execute in a world of social media sites. The justification for this clear intolerance of government data collection was explained this way, “I don’t like that government know everything about me, I don’t want them to have any information about me, because more personally, in my home, government can collect all information about people”. Further this participant follows by explaining the concern of future career because the situation where companies are “only hiring people who have the same political ideas” based on the specific government party. Through this example one can see how a convenient communication tool can turn into a possible surveillance system for government authorities to seek citizens private information for their benefits (Greenwald and MacAskill, 2013).
5.3 Overall Reflections

Based on findings and the detail discussion above, there are some key points we would like to underline in the overall discussion which is mainly from two perspectives: individuals and societal angles. From individual’s perspective, we believe it is fundamentally important for SNSs users to carry privacy awareness and relevant risks knowledge for the usage of online social interactions. The level of potential risks and media technology knowledge could enhance the management and protection of personal information in social media engagement. This has been shown in Ngeno’s et al. (2010) study which explored how knowledge background influences user’s privacy perception. Through the analysis, we realized the role of the concrete privacy education shapes high level of privacy awareness and risks knowledge. These effects could thus facilitate individual users to build up essential privacy boundary according to one’s cultural values and beliefs. With concrete boundary one would like to have for his/her privacy, individual users would be able to have the minimal value and standard to rely on for any involvement in privacy issues. Further, although many users claim they are privacy concerned and do have proper privacy setting on SNSs, it is vital to note that privacy setting management on SNSs could probably limit information accessibility and privacy invasion from other individual users to certain extent, but it does not limit the possibility of personal data collection and usage by service providers such as Facebook and/or third parties (Stutzman et al., 2012, p. 31). Therefore individual users shall also have knowledge of media technology such as sentiment or trend analysis algorithms and its capabilities in terms of personal data protection (Stieglitz et al., 2014). Besides, some users believe they can prepare for potential risks and consequences if they lost control over their personal information. Yet the questions arise: how can one prepare for consequences when user does not know what are the possible effects. However, we believe that one of the most critical ways to enhance personal privacy protection is the balance of SNSs usage based on appropriate evaluation between benefits and risks that SNSs offer. Balance usage on SNSs among individual users is a significant approach to positively engage in SNSs without disclosing unnecessary amount of personal information. The sufficient balance of SNSs usage could also be an effective method to confront social media privacy challenges the society has today.

From societal perspective, we consider it is essentially vital for modern society to positively understand people’s needs of online social interaction in the digital age, and the fact that SNSs do offer communication and connection benefits and convenience for its users. As principle, before we address online privacy issues, we cannot ignore people’s desire of online social interaction and the positive impacts it brings (Ellison et al., 2007). Also, people and society need to recognize users’ generous acceptance in exchange for usage benefits. This attitude is based on people’s understanding of SNSs providers need to gain benefits in some way and vulnerable position to change the situation. It is therefore particularly important to carry out transparency and consent of personal data usage among service providers and third parties. It is also the expectation from users in terms of their privacy data usage. The transparency and consent of personal data usage is considered as an ideal approach to enhance individual’s privacy protection, we believe the endeavors by different parties would make it possible. As a good example, Facebook has already launched privacy transparency for their advertising data usage, “At Facebook, we know transparency is key to keeping people’s trust, so we’ve created ways to help you understand and take control of the ads you’re shown” (Facebook, 2016). Certainly, privacy protection also needs to implement the

45
ethical rules among different parties that also includes government authorities in terms of citizen surveillance through SNSs (Greenwald and MacAskill, 2013). Ethics should definitely be the crucial principle for all parties and actors in the society that are involved in personal information privacy. Finally, online privacy policies and legislations should be carried out among national and international level. Most importantly, these regulations should be implemented with action-oriented approaches and solutions that contribute by all relevant actors throughout the society (Bradley, 2010).
6 Conclusion

The section is divided into four subsections. We will first sum up the key purposes of the study and the main results the research has found. Then we conclude the special outcomes and major argumentations of this thesis in the second subsection. Further, the third subsection will summarize what we have learned during the research process and what are the main contributions the thesis has accomplished for the area of social media privacy. Finally, the section ends with the suggestion for further researches of social media privacy area based on the important results we have found.

6.1 Main Purposes and Findings

Overall, the main purpose of this thesis is to address online privacy issues among individual SNSs users by investigating why university students still decide to utilize Facebook despite of privacy risks. The research also examines what are these young adults’ perspectives of online privacy exposure and how these opinions affect the use of Facebook. Within the main purposes, we want to find out what are user’s privacy perception and pertinent risks knowledge of Facebook usage, and how the perception influences his/her approaches for personal information control and protection. Hence, based on the motivation of raising social media privacy awareness among the society, the study decided to explore the issue by focusing on Facebook as representative of the most popular SNS in Sweden, and selected young adult users as the target group. Therefore the research has explored privacy awareness and risks knowledge of Facebook usage among ten university students at Linnaeus University in Sweden. The adopted methodology is qualitative research with the interpretive paradigm and is based on the methods of interview and Facebook data analysis. As results, we have identified seven important concepts that are mainly based on the three Cs (coding, category and concept) analytical strategy as introduced in the methodology section. These seven concepts are:

1. Necessity of communication and connection
2. Knowledge of privacy risks
3. Acceptance of personal data usage
4. Individual privacy boundary
5. Personal information control
6. Maintain balance usage
7. Choice and prepare for consequences

With the first three concepts, our study has found answers for the first research question: *What are the main reasons for university students to use Facebook despite of privacy risks?* By detail analysing, we have found that there are three major reasons to explain why users still decide to utilize Facebook although privacy risks exist. As the most fundamental reason, people’s needs and/or desires of online social interaction in today’s digital era are identified. Based on the needs of online communication and connection, users desire to be part of popular SNSs is an obvious choice. It is an inevitable phenomenon for online communication, connection convenience and necessity, even the use of Facebook can increase personal information exposure and cause relevant privacy risks. The second important reason is that users consider that they have certain risks knowledge to manage their privacy on Facebook. In general,
users claim they are privacy concerned yet large amount of private information is shared. However, users believe the shared private information on Facebook is in a controllable level. The third critical reason is users’ acceptance of usage for certain amount of personal information by different parties, such as Facebook, third parties or government authorities. Personal data usage acceptance, such as advertising or government security surveillance, is mainly based on their generous understanding or limited ability to change the situation. However, these three reasons give an essential and decent understanding of why people still use Facebook despite of privacy risks.

In addition, through the last four concepts the thesis has also found responses for the second research question: How user’s perspectives of privacy exposure affect the use of Facebook? Through the comprehensive analysis, we have recognized four significant aspects that affect the use of Facebook among college students based on their perspective of privacy. One of the main aspects is reflected on each user has his/her privacy definition according to individuals’ value, and people’s privacy boundary can be expanded when surrounding environment changes to a stronger Facebook usage culture such as in Sweden. Therefore users’ sharing behaviour is fundamentally affected by privacy boundary. More, the utilization of Facebook is also affected by user’s attitude on how one could manage privacy settings by controlling shared content and audiences. As another major factor, users comparison between benefits and privacy risks on Facebook impact how they could maintain balance usage. However, users believe that the utilization of Facebook in regards to privacy concern depends on personal choice of what kind of social life one would like to have. For the worst cases, the user just has to prepare for relevant privacy consequences. However, all these four concepts have shown that people’s perspectives of privacy and relevant risks influence the use of Facebook significantly.

6.2 Special Outcomes and Argumentation

Despite of the main findings that are summarized above, we have also found three special outcomes during the research process, and they are: misinterpretation, opinion manipulation and no tolerance of government surveillance. Through these three special outcomes we find out there is user who considers his/her private information available on Facebook to have the potential for the misinterpretation by someone else intentionally. Few participants even believe that Facebook has the power to influence users opinion to a certain direction. The last particular outcome has shown the intolerance of government surveillance because it invades citizen’s privacy for certain political intention.

Based on the results, we would first like to argue that university student’s needs and desires of online social interaction outweigh the fear of losing personal information through Facebook usage. Because Facebook offers obvious benefits in many ways while privacy risks remain only as a hidden possibility. In general, users have weak privacy awareness and risks knowledge to identify possible consequences in relation to their exposed privacy. The findings also help us to claim that university students are willing to accept certain part of risks and prepare for possible consequences in exchange for online communication and connection convenience. However, through the discussion, we have found how can user enhance privacy protection from individual perspective. As Clarke (2006) underlines, privacy protection “is a process of finding appropriate balances between privacy and multiple competing interests”. It is believed
that balance between benefits and risks could enable balance usage that will enhance privacy protection on Facebook without losing control of personal information privacy. From the societal perspective, it is important to carry out personal data usage transparency and consent as the way to gain user trusts and enhance personal information privacy. This ideal approach will be possible with transparency and ethical efforts among SNSs providers such as Facebook and all the third parties.

6.3 Contributions

Theoretically, we explored individual users’ perception of privacy risks on SNSs. This topic raised public attention of relevant scientific researches due to rapidly growing capabilities of modern media technologies. However, many studies are mainly focused on how organisation assesses information security or privacy risks but individual perspective of risks assessment is still underexplored. As result, we have identified seven crucial concepts for answering why individual users utilize Facebook despite of privacy risks, and how user perception of privacy risks affect the usage of Facebook. Some of the concepts have confirmed the findings and arguments other studies have also claim, for example privacy boundary (Petronio, 2002), personal information control (Christofides et. al. 2009), risks perception and acceptance of personal information usage on SNSs (Ngeno et al. 2010). The confirmation studies give contribution to the scientific field because it enhances the trustworthiness of the results. Further, by exploring those concepts we also contributed a comprehensive understanding of first party perception and actions of privacy in PIP model (Conger’s et. al. 2012).

Practically, the target group of university students has complemented young adult demographic research for the topic of social media privacy. We interviewed ten international students who are studying in Sweden. We believe participants have provided valuable facts and perspectives for the research. By that we generated better knowledge and understanding of their perception and engagement on Facebook. The two research methods of interview and Facebook data file analysis have provided not only rich understanding but also authentic sources that are based on facts. In other words, the findings of this thesis are supported by reliable data. Besides, during the research process, we noticed participants have developed better understanding of privacy risks and their privacy awareness increased. Therefore, it is believed this research with its findings will be able to enhance privacy awareness and risks perceptions.

6.3.1 Authors’ Contribution

There are two authors in this thesis work, Mr. Martin Charvát and Ms. Silvia Anderchen. Our knowledge and researches for the thesis are equally contributed. All studies and work for the thesis are evenly divided and closely collaborated between two authors. Based on that principle, Anderchen focuses more on the design of the introduction section, researches of social context and background of the phenomena with comprehensive analysis, while Charvát is mainly concentrating on the development of research methodology/methods and contributes his research ideas from technological/security perspectives. Apart from that there is not a clear boundary between the two authors for different parts of entire thesis since the two researchers are closely working together and are responsible for all parts of the thesis. As the principle we have built up for the research, we decide to carry out all the data collection together,
which means both of the researchers are part of every initiated interview. One of the researchers mainly guides the conversations and the other one is responsible for the important notes taking during the interview process. Besides, all the data collection and results is deeply discussed between two researchers. However, we implement all researches and studies as a whole in order to produce a complete and quality thesis as our contribution.

6.4 Future Research Suggestion

As the main findings for our research there are seven concepts identified. During the analysis process, we realized the close connection between those concepts and some of the concepts are interconnected. From a theoretical perspective, we therefore propose a further research to investigate the clear connection between these concepts and how they influence each other. It is possible that these concepts can build up a privacy model or theory for individual’s perception on SNSs usage. Furthermore, our study has identified the culture differences as one of the important factors that affect personal privacy awareness and the use of SNSs. So from a practical level, further researches can be focused on the comparison between different countries among individual SNSs users based on their cultural differences. To be more specific, to explore knowledge how users recognize privacy value based on their diverse cultural backgrounds. As Charlie Ess (2013) believes, it is important to explore how the diversity of cultural views and beliefs shapes people’s value of privacy to better understand privacy issues in digital media age, and to reflect on possible solutions. However, it is fundamentally important to raise privacy awareness throughout the society, researchers in relevant fields should be endeavour to solve the online privacy issues by providing practical suggestions or solutions to contribute a sustainable Information and Communication Technology (ICT) society. As Gunilla Bradley (2010) emphasizes, “The visions and goals for the Good ICT society for Human Beings need a stronger recognition and action strategies on all levels of society – including the global level” (p. 189).
7. References


Facebook, 2016. Data policy. [online] Available at: <https://www.facebook.com/about/privacy/> [Accessed 23 May 2016].


Appendices:

Appendix A.

General Introduction by researchers

1. Thank participant to take part of the research.
2. Introduce main research topic.
3. Notice participant about the voice recording (for transcript).
4. Notice participant about interview questions length (18 questions, around 30 minutes)
5. Present participant has the right to not answer certain questions if she/he does not want to, and the right to leave the research anytime. We ensure participant's personal information security. Participant will be anonymous according to our profession ethics and agreement.
6. Researchers and participant sign the agreement.

Participant X

Name:
Age:
Gender:
Nationality:
Education background:
Date:

Interview questions

Warm up questions
1. Are you a Facebook user?
2. How long have you been using Facebook?
3. How often do you use Facebook?

Main Questions:
1. What do you normally share/post on FB?
   Do you consider yourself over sharing?
2. With whom you usually sharing on FB?
3. Does this kind of sharing behaviour changed during the time when you using FB? Why?
   Sub: Any changes regarding to your privacy concern?
4. Are you concerned that what you share on FB would affect your information privacy? Why?
5. Are you concerned that what your friends’ share would affect your information privacy? Why?
6. How do you see your private information is being exposed on FB?
7. How do you control your private information on FB? Why?
8. Do you think it is possible to permanently delete the content that you shared? Why?
9. What benefits would you consider when using FB?
10. Is there any risks or consequences you recognized for your exposed private information?
11. How do you see the balance between these benefits and risks/sequences? 
   Would this affect your usage of FB?
12. Did you read the privacy policy on FB? Why?
13. Do you know that Facebook, third parties and government authorities can collect 
   your private information for their benefits? (Third parties: data collection 
   companies)
14. In your opinion, what can be changed or improved in terms of your privacy 
   protection?
15. Regarding to the topic of information privacy on FB, do you have something 
   more to add?
Appendix B.

Hi, our names are Silvia Anderchen and Martin Charvát. We work on Degree project in Informatics at Master Level.

The initial motivation of the thesis is to understand a critical social phenomenon through an in-depth study of information privacy based on individual users perspective. The contribution of the thesis is aiming for generating more knowledge of information privacy on social media and, provide findings of risks perception by individual SNSs users. We planed to generate this knowledge through interviews and analysis of data provided on Facebook profiles.

We are students of Information Systems Master Programme at Linnaeus University and both of us are equally responsible during this research. You can contact us by email (mc222ks@student.lnu.se, sc222eg@student.lnu.se) or on a mobile phone (+46 72 846 40 21) to ask any questions. We appreciate that you are willing to participate in our research. Before we start with the interview it is important to reassure you that you have following rights:

1. Your participation is entirely voluntary.
2. You can withdraw at any time without giving a reason.
3. You are free to refuse to answer any question at any time.
4. Your name will not be used in the thesis and all information will be kept strictly confidential.

Since the main focus of our research is in the privacy area it is possible you might feel psychical discomfort or higher stress level than usual due to some answers you provided during the interview or because of some data you have available on your Facebook profile. We would like to assure you that in these cases you can contact us and these informations will not be included in our thesis.

Please sign this document to show that you were informed about your rights and understand our research plan.

Participant’s signature: Date:
Participant’s name (in CAPITALS)

Researcher’s signature: Date:

I would like to receive the final version of this thesis. (circle one)

YES NO