MASTER THESIS

DETERMINING THE FACTORS THAT INFLUENCE THE USE OF PRIVACY CONFIGURATION SETTINGS ON FACEBOOK

AN EMPIRICAL STUDY AMONG ADOLESCENTS

AUTHOR
Aday Destici

FACULTY
Behavioural, Management and Social sciences

EXAMINATION COMMITTEE
Dr. A. Beldad
Dr. S.A. de Vries

Enschede | November 2015

UNIVERSITY OF TWENTE.

DETERMINING THE FACTORS THAT INFLUENCE THE USE OF PRIVACY CONFIGURATION SETTINGS ON FACEBOOK

An empirical study among adolescents in the Netherlands

''We are rapidly entering the age of no privacy, where everyone is open to surveillance at all times; where there are no secrets from government''
(Douglas, 1966)

Author: Aday Destici

University of Twente
Behavioural, Management and Social sciences | Master Communication Studies | Master Thesis

---

Examination committee
First supervisor: Dr. A. Beldad
Second supervisor: Dr. S.A. de Vries

Enschede | November 2015

PREFACE

After an intensive period of researching, the end-product is finally here. I started in september 2013 with the Master Communication Studies: Media and Communication. After obtaining my Bachelor degree in Business Administration on Saxion University of applied sciences I decided to pursue an academic careeer on the University of Twente. After a sucessful pre-master programme in Communication Studies I was approved to continue with the Master Media and Communication. I have always been fascinated with media and communication and how it effects our daily lives and therefore I chose this specific master programme. During this period I learned a lot about communication theories and how to implement them in practice.

The reason I did this study is because I got interested in social media and how it effects our daily lives. It influences how we communicate with each other and our privacy. The last years different media wrote a lot about privacy issues and how people deal with it. That is why I became interested and wanted to contribute on this subject. I hope you will enjoy reading this report and that people and organizations could benefit from it.

As a final note, I would like to personally thank a few people who were involved in the process of writing my thesis and in my educational career in general. At first, I would like to thank my supervisors Mr. Ardion Beldad and Mr. Sjoerd de Vries, for the help, feedback, support and for being patient with me (it was a long journey). They have supervised me very well during the whole process and I have learned a lot from them. Second, I would like to thank my parents, family and friends for the support and also for enabling me to focus on my academic study career. Last, I would like to thank Christopher Uncu who is a good friend and I learned a lot of the times we studied together. He encouraged me to finish my study and he was always prepared to help and I am grateful for that.

Aday Destici

Enschede, November 2015

ABSTRACT

An increasing number of people are making use of social networking sites (SNS) and this has changed the way how people live their lives. The current study aims at determining the factors influencing the use of Facebook's privacy configuration settings among adolescent users in the Netherlands. The scientific value of the study is that it integrates the Protection Motivation Theory (PMT) and the Unified theory of acceptance and use of technology (UTAUT). Since PMT provides a framework for understanding fear appeals and to understand if individuals are motivated to protect them on Facebook. UTAUT research has been done in information systems and information technology. It aims to explain user intentions. The societal value of this study is to find out what the awareness is of adolescents regarding the possibilities of privacy configuration settings on Facebook. This study is important since understanding their knowledge of privacy configuration settings of Facebook users in the Netherlands can result in implementation of more effective privacy measures. The study had a descriptive design and was done by means of a survey among adolescents between the ages of 13 and 17 from the Avila College and Lyceum the Grundel. Of approximately 300 distributed questionnaires, a total of 220 questionnaires were collected (*response rate = 73%)* between May 1st and July 1st 2015. after removing the incomplete or otherwise unusable questionnaires there were 195 usable questionnaires left. *Perceived severity, Rewards*, *Effort expectancy, Social influence* and *Facebook experience* are the significant factors that influence the use of privacy configuration settings on Facebook by adolescent users in the Netherlands. It can be concluded that the proposed model's strongest predictor of an individual to use privacy configuration settings on Facebook is *Effort expectancy*, or the ability to protect their personal information and the ease of use of privacy configuration settings on Facebook. The second strongest predicting variable is *Perceived severity,* or the conclusion of the severity consequence resulting from a threatening security event. This study contributes to existing theory in a sense that it provided further evidence that the two concepts can be combined. This study performed extensive validity and reliability analyses and showed that all the adapted constructs in the reliability analyses have high reliability factors.

Keywords: Privacy prrotection behavior; Protection Motivation Theory (PMT); Unified theory of acceptance and use of technology (UTAUT); Facebook, privacy configuration settings

INDEX OF ABBREVIATIONS

PMT:	Protection motivation theory
UTAUT:	Unified theory of acceptance and use of technology
SNS:	Social networking site(s)
UPCS:	Use of privacy configuration settings
PS:	Perceived severity
PV:	Perceived vulnerability
RE:	Rewards
PE:	Performance expectancy
EE:	Effort expectancy
SI:	Social influence
GE:	Gender
NW:	Network size
FEXP:	Facebook experience
PCA:	Principal component analysis
KMO:	Kaiser-Meyer-Olkin measure

INDEX OF FIGURES AND TABLES

Figures

Tables

TABLE OF CONTENTS

1. INTRODUCTION

An increasing number of people are making use of social networking sites (SNS) and this has changed the way how people live their lives. SNS are web-based services that allow individuals to: construct a public or semi-public profile; articulate a list of other users; view and negotiate their list of connections and those made by others within the system (Borena, Belanger, and Ejigu, 2013). Kaplan and Henlein (2010) describe SNS as applications that enable users to connect with each other by creating personal information profiles, inviting friends and colleagues to have access to those profiles, and sending e-mails and instant messages between each other. These personal profiles can include any type of infromation, including photos, videos, audio files, and blogs (Kaplan and Haenlein, 2010).

One of the biggest SNS in the world is Facebook with 9.4 million Dutch users (Oosterveer, 2015) and according to Edwards (2014) there are 2.2 billion Facebook users worldwide. That is roughly one third of the entire population of the world. Facebook is a popular website where people can post photos, personal information and news about themselves in a shared space that can be made accesible to others in varying degrees (Saeri, Ogilvie, La Macchia, Smith and Louis, 2014). During the use of SNS, people are confronted with information privacy concerns and consequently privacy protection behavior. Privacy can be understood as the ‘’boundary control process in which individuals regulate when, how and to what extent information about them is communicated to others’’ (Garde-Perik, E. v. d., Markopoulos, Ruyter, Eggen and Wijnand Ijsselsteijn, 2008).

Privacy protection is the ability of an individual to personally control information about one’s self while information privacy concerns are the extent to which an individual is concerned about organizational practices related to the collection and use of his or her personal information (Norshidah and Hawa, 2012). According to Youn (2009) there are two privacy protection behavior strategies: confrontative strategies and avoidance strategies. Confrontative strategies are for example mastering the privacy configuration settings povided by the SNS, or using firewalls and spam guards. Avoidance strategies are for example ignoring the threats or to refuse to use the internet or deleting your Facebook account. The use of privacy configuration settings on Facebook is an example of a confrontative strategy and serves as the basis of this study. The use of privacy configuration settings on Facebook is used since this is a method to protect one’s privacy. According to Christofides, Muise and Desmarais (2012), understanding the factors that influence the use of privacy configuration settings on Facebook is critical, as many individuals fail to protect their privacy on Facebook securely. People are not always aware of the consequences of making use of SNS and what

the possibilities are of privacy configuration settings on SNS. Many users of Facebook are unaware of the potential dangers in terms of privacy, particularly young adolescents can be vulnerable to privacy issues during the use of SNS because of their knowledge and awareness of privacy configuration settings (Christofides, Muise and Desmarais, 2012).

The current study aims at determining the factors influencing the use of Facebook's privacy configuration settings among adolescent users in the Netherlands. The scientific value of the study is that it integrates the Protection Motivation Theory (PMT) and the Unified theory of acceptance and use of technology (UTAUT). Since PMT provides a framework for understanding fear appeals and to understand if individuals are motivated to protect them on Facebook. The PMT literature focusses on privacy protection behaviors on social media, virus protection behavior and people who perceive vulnerability to the threat of virus attacks are more likely to engage in virus protection behaviors (Dinev and Hart, 2004; Norshidah and Hawa, 2012; Milne, Labrecque and Cromer, 2009; Jiang, Heng and Choi, 2013). UTAUT aims to explain user intentions to use privacy configuration settings on Facebook and subsequent usage behavior. UTAUT research has been done in information systems and information technology. It aims to explain user intentions (Venkatesh, Thong and Xu, 2012; Woon, Tai and Low, 2005; Zhang and McDowell, 2009; Lin and Anol, 2008). With these two theories combined, it aims to describe why people are making use of privacy configuration settings and in what kind of situation. The study aims to show that the PMT and UTAUT variables hold in a social media context. Some variables of UTAUT and PMT tend to overlap and these will be further discussed in chapter 2. The societal value of this study is to find out what the awareness is of adolescents regarding the possibilities of privacy configuration settings on Facebook. This study is important since understanding their knowledge of privacy configuration settings of Facebook users in the Netherlands can result in implementation of more effective privacy measures. Institutions could provide training programs to make the people aware of the risks and threats of Facebook. This type of study that focusses on the use of privacy configuration settings has not been done in the Netherlands on adolescent users.

The researcher proposed the following research questions:

RQ1: To what extent do adolescents make use of privacy configuration settings on Facebook?

RQ2: What are the predictors of the use of privacy configuration settings on Facebook among adolescent users?

The structure of the research report is as follows. Chapter 1 one will discuss the goal of the research and research background. Chapter 2 will describe the theoretical framework that sets the context of the research and the research model. Chapter 3 will describe the research design, procedure, participants and measurements that will be used in this study. Chapter 4 displays the results of the study. It starts with the results from the correlation analysis and the remainder of this chapter is dedicated to hypothesis testing results. Chapter 5, discussion discusses the results and how this relates to the findings from the literature. Chapter 6 will describe the conclusions. Chapter 7 will discuss the implications, limitations and suggestions for further research of the study.

2. THEORETICAL FRAMEWORK

This chapter provides an overview of the theoretical framework that is used for the study. First the literature and the hypotheses will be presented and last the research model that will be used for the study.

The theoretical framework will describe the predictors of the use of privacy configuration settings and subsequently the study should give an answer on the significant predictors. Facebook will be used to study the predictors of the use of privacy configuration settings since it is one of the biggest SNS in the world with 9.4 million Dutch users (Oosterveer, 2015) and according to Edwards (2014) there are 2.2 billion Facebook users worldwide. Users have a choice to use privacy measure to protect their information privacy. This behavior will be further mentioned as *'use of privacy configuration settings'.* The study integrates the Protection Motivation Theory and the Unified theory of acceptance and use of technology. Some concepts in the two theories tend to overlap, *effort expectancy* (UTAUT) and *self-efficacy* (PMT), the degree of ease associated with the use of the system. *Performance expectancy* (UTAUT) and *perceived response efficacy* (PMT), if a recommended coping response is effective in protecting the self or others from a threat. Both variables measure the same yet are differently labeled in the two theories.

2.1 Use of privacy configuration settings

According to Youn (2009) there are two privacy protection behavior strategies: confrontative strategies and avoidance strategies. Confrontative strategies are for example mastering the settings povided by the SNS, or using firewalls and spam guards. Avoidance strategies are for example ignoring the threats or to refuse to use the internet or deleting your Facebook account. The use of privacy configuration settings on Facebook is an example of a confrontative strategy and serves as the basis of this study. According to Youn (2009), young adolescents level of privacy concerns will be positively relate to their privacy protection behaviors. Adolescents' concerns about social humiliation or the risks of crimes such as identity fraud do not appear to hinder the exposure of personal information in many different internet areas (Attrill and Jalil, 2011; Cozby, 1973; Wheeless, 1978; Wheeless and Grotz, 1976; Attrill and Jalil, 2011). In older studies of Sheehan and Hoy (1999) and Milne, Rohm and Bahl (2004), they identified that as consumers' concerns over privacy heightened; they adopted voicing behaviors, such as asking for name removal from lists or falsifying information, refusing information disclosure or transactions.

There are specific behaviors that have the focus on the use of privacy configuration settings (Youn, 2009):

- I limit other people's access to my Facebook account using privacy settings.
- I regularly check my privacy settings in Facebook.
- I use Facebook's privacy settings to prevent people from accessing my Facebook account through search engines.
- I use the privacy settings of Facebook to determine who can see and access information I post on my Timeline.
- I use the privacy settings of Facebook to determine who will be able to contact me.

Based on the above discussion the researcher aims to understand the factors that influence the decision to use Facebook's privacy configuration settings, especially among adolescent users in the Netherlands.

2.2 Protection motivation theory

Protection Motivation Theory provides a framework for understanding fear appeals (Rogers, 1985). The main assumption of the theory is that individuals are motivated to protect themselves if they feel threatened in risky situations (Norshidah and Hawa, 2012; Milne, Labrecque and Cromer, 2009)). Proection Motivation Theory proposes that motivation to self protect from risks emerges from *Perceived Severity, Perceived Vulnerability* and *Perceived Response Efficacy* (Boer and Seydel, 1996). These three variables have all a positive function. *Rewards* has a negative function. Applying this theory to the online privacy context, young adolescents level of privacy concerns may be considered protection motivation, which causes them to ensgage in risk-reducing behaviors (Youn, 2009; Hasebrink, 2009). These risk-reducing behaviors will be further mentioned in this study as the use of privacy configuration settings on Facebook.

2.2.1 Perceived severity

Perceived severity refers to conclusion of the severity consequence resulting from a threatening security event (Larose, Rifon, Liu and Lee, 2005). The study aims to show if users of Facebook believe that if losing information privacy through Facebook would be a serious problem for them. Another problem could be that their online identity is stolen through Facebook. Information privacy is the ability of an individual to personally control information about one's self while information privacy concerns are the extent to which an individual is concerned about organizational practices related to the collection and use of his or her personal information (Norshidah and Hawa, 2012).

Privacy protection behavior, specifically the use of privacy configuration settings is often linked with information privacy concerns, which arise from the belief that personal information disclosure is very risky due to high either by the collecting organizations (Beldad, de Jong and Steehouder, 2011; Dwyer, Hiltz and Passerini, 2007). The greater an individuals' concerns about information collection and sharing practices, the more likely an individual is to try to adopt privacy protection behaviors (Youn, 2009; Young and Quan-Haase, 2009). According to Crossler, 2010), *perceived severity* impacts decisions of home wireless network users to implement security features and influences behavior to use anti-spyware software. Individuals who perceive severe consequences as a results of losing information privacy through SNS are more likely concerned with information privacy. Therefore, the researcher proposes that individuals who perceive severe consequences have higher concerns with their information privacy in SNS and therefore will make use of the privacy configuration settings on Facebook. Based on the above discussion the researcher proposed the following hypothesis:

H1: Perceived severity positively influences the use of privacy configuration settings on Facebook.

2.2.2 Perceived vulnerability

Perceived vulnerability is the degree to which an individual believes a threat will occur to him or her (Norshidah and Hawa, 2012). According to Chenoweth, Minch and Gattiker (2009), in the case of virus protection behavior, people who perceive vulnerability to the threat of virus attacks are more likely to engage in virus protection behaviors like for example making use of anti-spyware software. The study aims to show if users of Facebook feel that they could be subjected to malicious computer/information security problems. Or that they feel that their personal information on Facebook could be misused. Another problem could be that they feel that their personal information is made available to government agencies. Therefore the researcher proposes that individuals who perceive the threats of losing information privacy through Facebook have greater concerns with their information privacy and will make use of privacy configuration settings. Based on the above discussion the researcher proposed the following hypothesis:

H2: Perceived vulnerability positively influences the use of privacy configuration settings on Facebook.

2.2.3 Rewards

Rewards refer to benefits expectations in keeping with the choice of behaviors (Norshidah and Hawa, 2012). There are many documented benefits to sharing online, such as the ability to explore different identities (Boyd and Ellison, 2007), create an identity that is shared with friends

(Christofides et al., 2012), and increase one's social capital (Ellison, Steinfled and Lampe, 2007), then there are also many potential and actual risks. Hasebrin (2009) researched the various risks to children and their categorization of these risks provides a useful framework for understanding them (Christofides et al., 2012). Peluchette and Karl (2008) found that the availability of information on Facebook can make it easier for one's own postings to be incriminating, as for example, when adolescents post stories about their drinking and drug experiences or other illegal activities. These stories can lead to to consequenses such as school suspensions and criminal charges. Although these consequenses are indeed negative, some of the other negative consequenses that can be experienced may never be known (Christofides et al., 2012).

According to Jiang, Heng and Choi (2013) the behavior of individuals on SNS is sometimes inconsistent with their privacy concerns, they put their private information on SNS while they are aware of the risks involved with these actions. The study aims to show if rewards have influence on the choice of making use of Facebook. Example of *rewards* could be: getting connected with other people, getting news events, joining social applications. As individuals perceive the benefits in getting connected with others or playing games in SNS, they may consciously expose their personal information toward attaining these benefits. Therefore, the researcher proposes that users perceiving greater *rewards* derived out of Facebook have less concern with their information privacy and therefore do not make use of the privacy configuration settings. Based on the above discussion the researcher proposed the following hypothesis:

H3: Rewards negatively influences the use of privacy configuration settings on Facebook.

2.3 Unified theory of acceptance and use of technology (UTAUT)

The Unified theory of acceptance and use of technology (UTAUT) aims to explain user intentions to use an information system and subsequent usage behavior (Venkatesh, Thong and Xu, 2012). UTAUT has four key variables: *performance expectancy, effort expectancy*, *social influence* and facilitating conditions (Venkatesh, Thong and Xu, 2012). Furthermore, *peformance expectancy, effort expectancy* and *social influence* are going to be used in this study.

2.3.1 Performance expectancy

Performance expectancy is the belief that a recommended coping response is effective in protecting the self or others from a threat (Venkatesh, Thong and Xu, 2012). It measures the same as perceived response efficacy from PMT, both variables tend to overlap. The study aims to show if users of Facebook use privacy protection measures to protect from losing information privacy. Research

proposes that *performance expectancy* explains whether an individual enables a security measure in home wireless security or influences behavior intention to use anti spyware software as a protective technology (Woon, Tai and Low, 2005; Zhang and McDowell, 2009). Therefore, the researcher proposes that an individual who believes that a protective action can be taken to avoid the costs of losing information privacy through Facebook is more likely to be concerned with his information privacy and therefore will make use of the privacy configuration settings. Based on the above discussion the researcher proposed the following hypothesis:

H4: Performance expectancy positvely influences the use of privacy configuration settings on Facebook.

2.3.2 Effort expectancy

Effort expectancy is defined as the degree of ease associated with the use of the system (Venkatesh, Thong and Xu, 2012). It measures the same as self-efficacy from PMT, both variables tend to overlap. It is the belief that a person has the ability to protect their personal information and if it is easy for them to enable privacy measure features on SNS (Winter, Neubaum, Eimler, Gordon, Theil, Herrmann and Krämer, 2014). In context of this study, the activities are explained as the ease of use of privacy configuration settings on Facebook. Empirical researches on *effort expectancy* and self-efficacy continue to dominate the discussion on computer use. According to Chai, Bagchi-Sen, Morell, Rao and Upadhyaya (2009) there is evidence for a positive relationship between *effort expectancy* and motivation to protect information online. According to Lee, Larose and Rifon (2008), *Effort expectancy* is also a predictor of the intention to use virus protection software. When people feel that they are in danger and are confident, they have the abiity to avoid or cope with the danger, that has a big influence on securing their online environment. In the context of Facebook, users could indicate to what extent they can protect their personal information on Facebook with use of the provided privacy configuration settings. Based on the above discussion the researcher proposed the following hypothesis:

H5: Effort expectancy positively influences the use of privacy configuration settings on Facebook.

2.3.3 Social Influence

Social influence is the extent to which consumers perceive that important others (family and friends) believe they should use a particular technology (Venkatesh, Thong and Xu, 2012). *Social influence* that represents certain perceived pressure to perform a behavior. It reflects the extent to which

individuals of a social network influence on another (Lin and Anol, 2008). According to Sánchez, Cortijo and Javed (2014), *social influence* is the most important factor in predicting the adoption of Facebook. Kaba and Touré (2014) state that when it comes to social media, women are more sensitive to social pressure than men and that social pressures are among the dominant factors explaining the use of an technology. Users of Facebook could be influenced by family or friends to make use of privacy configuration settings because of their own experience with Facebook or other SNS. In pararaph 2.4.3, the influence of *network size* will be discussed. This discussion will have the focus on the influence of the quantity of the friends list on Facebook. In context of this study, the influence of important others on the use of privacy configuration settings on Facebook will be studied. Based on the above discussion the researcher proposed the following hypothesis:

H6: Social influence positively influences the use of privacy configuration settings on Facebook.

2.4 Demographics

The demographics of the user will be studied, namely *gender* and network. The difference between *gender* and the use of privacy configuration settings is studied. The *network size* focusses on how many friends the users have and if that influences the use of privacy configuration settings on Facebook.

2.4.1 Gender

Several studies show that *gender* relates to online privacy concerns and state that females show greater concerns than males (Cockcroft and Clutterbuck, 2001; Dinev and Hart, 2004; Hoy and Milne, 2010; Laric, Pita and Katsanis, 2009; Youn and Hall, 2008). The study aims to show if there is a difference between *gender* and the use of privacy configuration settings on Facebook. According to Van Deursen and Van Dijk (2012) SNS are more popular with women than with men. Researchers find that women are generally more concerned about privacy than men. For example, Sheehan (1999) finds that women are more likely than men to be concerned when a website says that personal information will be used by other organizations. Therefore, the researcher proposes that women make more use of privacy configuration settings and how they use privacy configuration settings. Based on the above discussion the researcher proposed the following hypothesis:

H7: Women make more use of privacy configuration settings on Facebook than men.

2.4.2 Network size

Network size and density are two of the mostly studied network properties. *Network size* refers to the number of nodes in that network, and network density is used to address communal connections among these nodes. The denser the network is, the more connected the nodes in the network are (Kivran-Swaine and Naaman, 2011). It has been found that larger and sparser networks are correlated with more sharing of emotion in microblogging. However the relationship is not clearly explained (Lin and Qiu, 2012). Strength of ties and characteristic of a persons social network are known to be associated with sharing of emotions (Kivran-Swaine and Naaman, 2011). Therefore the researcher proposes that the quantity of the friends list on Facebook positively influences the use of privacy configuration settings on Facebook. Based on the above discussion the researcher proposed the following hypothesis:

H8: Network size positively influences the use of privacy configuration settings on Facebook.

2.4.3 Experience

Experience is the passage of time from the initial use of a technology by an individual (Venkatesh, Thong and Xu, 2012). In context of this study, the experience of users on Facebook will be studied in relation with the use of privacy configuration settings on Facebok. Individuals who have prior experience with SNS could have stronger privacy concerns and are more likely to have encountered privacy abuses. (Lankton and Tripp, 2013). Therefore they could have had negative experiences with the SNS. Based on the above discussion the researcher proposed the following hypothesis:

H9: Facebook experience positively influences the use of privacy configuration settings on Facebook.

2.5 Research model

The nine hypotheses are presented in the research model of the use of privacy configuration settings on Facebook (Figure 2.1). The study proposes this model to study the factors that influence the decision to use Facebook's privacy configuration settings, especially among adolescent users in the Netherlands. This model integrated PMT and UTAUT into the research model of the use of privacy configuration settings on Facebook. On the left side of the model are the variables from PMT and UTAUT and on the right bottom side of the model are the demographic variables that are going to be used in this study.

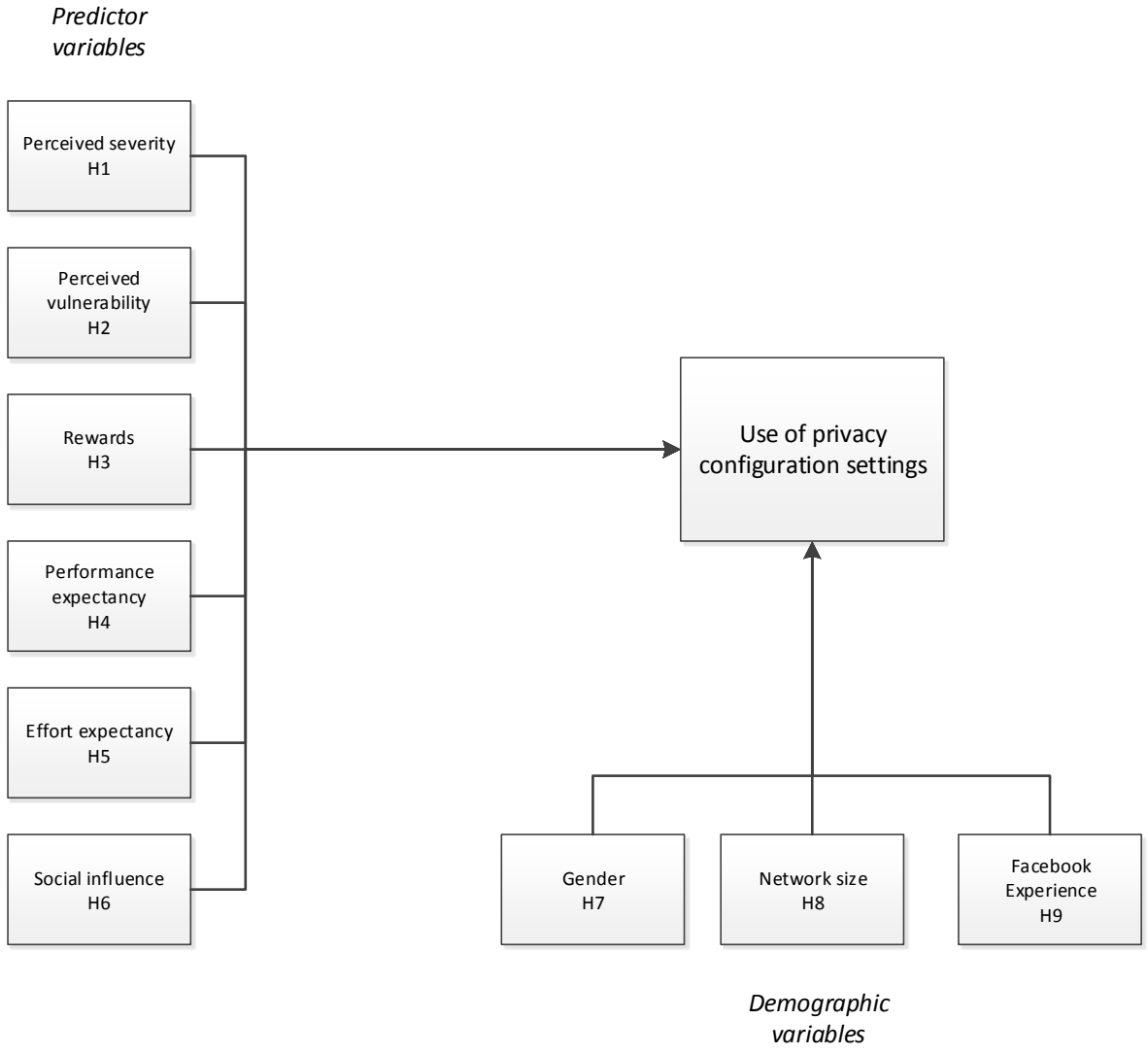


Figure 2.1: Research model of the use of privacy configuarion settings on Facebook

3. METHODOLOGY

This chapter provides an overview of the method to use in the study. Areas covered include the research design, procedure, participants and measurements.

3.1 Research design

The study had a descriptive design and was done by means of a survey. These types of studies are used to describe characteristics of a population being studied. The goal of this study is to understand the factors that influence the decision to use Facebook's privacy configuration settings, especially among adolescent users in the Netherlands. In this context, the dependent variable is the use of privacy configuration settings on Facebook and the independent variables will be discussed in paragraph 3.4.1. An extensive literature review was conducted and focused on gathering the most relevant literature on this subject. The constructs of the research model of the use of privacy configuration settings on Facebook were imported in one survey which was ready to be formed into the research instrument for this study. Questionnaires can be an effective means of measuring the behavior, attitudes, preferences, opinions and intentions of relatively large numbers of subjects (Field, 2009). The context of this study is high schools from the Netherlands and involved young adolescents between the ages of 13 and 17 that make use of Facebook. This study used adolescents since they could give insight on what the awareness is regarding the possibilities of privacy configuration settings on Facebook. This could have practical implications in the future for SNS and governmental organizations in terms of redesign and education. Facebook is used because of the popularity, reach, unique properties, completeness of provided services and complexity and depth that Facebook offers to their users. This study will aim to answer the research questions and hypotheses using Facebook as a representation of other SNS.

3.2 Procedure

In this study a questionnaire was administered to test the use of privacy configuration settings on Facebook by adolescents in the Netherlands. Several steps in the development of the instrument such as pre-test questionnaire, distribution of the questionnaire and data collection are discussed in the next subparagraphs.

3.2.1 Pre-test questionnaire

Qualtrics survey software and insight platform was used for implementing and distributing the online questionnaire. This type of questionnaire is used for this study since you can reach a lot of people

and can collect information about the behaviors, needs, and opinions of respondents. A pre-test has been conducted with five respondents within the age category of 13 to 17 years old to make sure that the questionnaire was understandable and readable. After the pre-test was filled in the respondents were asked for giving their view on the questionnaire. The following feedback was given by the respondents:

- Some words and sentences were difficult to understand.
- There were some typing errors.
- Questions could be shorter.
- Progress bar was added in the online questionnaire.
- Next and previous button are clearly added in the online questionnaire.
- Before starting the questionnaire explain what the goal is of the study.
- Is there an opportunity to view the results of the study?

With help of the feedback from the respondents the researcher could revise the questionnaire.

3.2.2 Distribution of the questionnaire

After the questionnaire was improved, it was sent to the dean or teacher of the first and second year high school students and then he or she would distribute them among their students. The third and fourth year high school students had their own e-mail accounts therefore the questionnaire were sent to their private e-mails. The students and parents were informed by their teachers about the study and if they needed more information they could contact the researcher through phone or e-mail. Qualtrics survey software and insight platform was used for distributing the online questionnaire. The ethical committee of the University of Twente was aware of this study by means of an application form that could be downloaded from the University of Twente website. After the form was filled in it was sent to the first supervisor and then processed through the ethical committee.

3.2.3 Data collection

The data of the questionnaire was collected by using Qualtrics Survey software and insight platform. The license of Qualtrics is provided by the University of Twente software program. After the surveys are completed, the answers are coded in order to process them through a software program named IBM SPSS Statistics 22. The license for IBM SPSS is also provided by the University of Twente. For an extensive view of the SPSS data set (variable view) I refer you to the Appendix C.

3.3 Participants

In a study of qualitative in-depth interviews among teens aged 13-17, Grant (2006) clarified major causes for teens privacy concerns online. Teens were concerned about their online privacy because they were worried about being barraged with unsolicited commercial messages and being trakced down by marketers, resulting in a loss of control over their private information (Grant, 2006). Young adolescents can be particularly vulnerable to information collection practices when promotional messages are skillfully blended with entertainment online (Moore, 2004). More recently, young adolescents' information disclosure on SNS like Facebook has intensified parents' worries about loss of privacy (Romer, 2006; Lenhart and Madden, 2007; Livingstone, 2008). Since the rapid increasing popularity of SNS, the information disclosure of young adolescents on other services has intensified worries about loss of privacy (Romer, 2006; Lenhart and Madden, 2007; Livingstone, 2008). The focus of this study is on adolescent Facebook users from 13 to 17 years old in the Netherlands because of adolescents spent more time on SNS than other groups (Van Deursen and Van Dijk, 2014). A quantitative research method was conducted for this study, based upon online questionnaires. In this study, 300 questionnaires were administered among Dutch adolescents from the Avila College and Lyceum the Grundel. The students could be accessed through personal e-mails or e-mail from their teachers. First and second year students who do not have personal e-mails received the questionnaire through the email of their teacher. The participants could fill the questionnaire in during class or if the participant had a personal e-mail address they could do it at home.

3.4 Measurements

This paragraph provides an overview of the development of measurement scales, response rate, demographics, factor analysis and reliability test.

3.4.1 Development of measurement scales

Table 3.1 shows a summary of the items used in the questionnaire and the source of the items. For a more extensive view of the questionnaire I refer you to Appendix A and B. In order to measure *effort expectancy, perceived severity, perceived vulnerability, performance expectancy, rewards and privacy configuration settings,* items suggested by Dinev and Hart (2004) were used and were modified in such a way that it focusses on the use of privacy configuration settings on Facebook. In order to measure *social influence*, items suggested by Venkatesh et al (2011) were used and were modified that focusses on the influence of others. A 7-point Likert scale was used from completely disagree to completely agree. The items about *gender* and *Facebook experience* are categorical and focus on

gender type and years of experience on Facebook. The item about *network size* is an open question (scale) about the quantity of the friends list on Facebook.

Table 3.1: Measurement scales and items

Variable	*Measurement scale*	*Item*	*Source*
Effort expectancy	7-point Likert scale (1 = strongly disagree to 7 = strongly agree)	I believe I have the ability to protect my personal information on Facebook. It is easy for me to enable privacy measure features on Facebook by myself.	(Dinev and Hart, 2004)
Facebook Experience	Ordinal	How many years of experience do you have on Facebook?	(Venkatesh et all, 2011)
Social Influence	7-point Likert scale (1 = strongly disagree to 7 = strongly agree)	Most people who are important to me think I should use privacy settings on Facebook. My close friends think I should use privacy settings on Facebook.	(Venkatesh et all, 2011)
Perceived severity	7-point Likert scale (1 = strongly disagree to 7 = strongly agree)	I believe that losing information privacy through Facebook would be a serious problem for me. Having my online identity stolen through Facebook would be a serious problem for me.	(Dinev and Hart, 2004)
Perceived vulnerability	7-point Likert scale (1 = strongly disagree to 7 = strongly agree)	I could be subjected to malicious computer/information security problems (e.g. virus, privacy, identity theft, hacking and etc.) on Facebook. I feel my personal information on Facebook could be misused.	(Dinev and Hart, 2004)
Performance expectancy	7-point Likert scale (1 = strongly disagree to 7 = strongly agree)	If I used privacy protection measures in Facebook, I could probably protect myself from losing my information privacy. I can protect my information privacy better if I use privacy protection measures in Facebook.	(Dinev and Hart, 2004)
Rewards	7-point Likert scale (1 = strongly disagree to 7 = strongly agree)	By losing my information privacy in Facebook I could get connected with new friends and friends from the past. By losing my information privacy in Facebook, I could join applications (e.g. quizzes, games, etc.)	(Dinev and Hart, 2004)
Use of privacy configuration settings	7-point Likert scale (1 = strongly disagree to 7 = strongly agree)	I limit other people's access to my Facebook account using privacy settings. I regularly check my privacy settings in Facebook.	(Dinev and Hart, 2004)
Gender	Nominal	What is your gender?	(Venkatesh et all, 2011)
Network size	Scale	How many friends do you have on Facebook?	(Kivran-Swaine and Naaman, 2011)

Note. Appendix A and B shows the questionnaire items that were used in the questionnaire.

3.4.2 Response rate

Of approximately 300 distributed questionnaires, a total of 220 questionnaires were collected (*response rate = 73%)* between May 1st and July 1st 2015. after removing the incomplete or otherwise unusable questionnaires there were 195 usable questionnaires left. Some questionnaires were unusable since some questions were not filled in completely or there were outliers in the answers. The outliers were identified with use of a summary of the descriptive statistics using IBM SPSS. The table gave an overview of the answers and based on the answers that had outliers were deleted from the data set.

3.4.3 Demographics

Table 3.1 shows a summary of the demographic descriptive statistics. Appendix F gives a graphical view of the use of privacy configuration settings on Facebook. After removal of the outliers there was a total of 195 usable respondents left with 46.2% *(n = 90)* male and 53.8% *(n = 105)* female respondents. The respondents showed that they had an average of 197 friends on their Facebook profile. The question: *'How do you make use of the privacy settings provided by Facebook to protect personal information?'* had a mean of 6.40 (7-point Likert scale (1 = strongly disagree to 7 = strongly agree) which indicates that the respondents totally agreed on using privacy configuration settings on Facebook to protect their privacy. The respondents answered on the question: *'Most people who are important to me think I should use privacy settings on Facebook.'* A mean of 3.79 (7-point Likert scale (1 = strongly disagree to 7 = strongly agree) which indicates that the respondents were neutral and are not really influenced by their friends or family. The respondents answered on the question: *'I am concerned about submitting my personal information on Facebook because of what others might do with it.'* A mean of 5.49 (7-point Likert scale (1 = strongly disagree to 7 = strongly agree) which indicates that the respondents totally agreed about their concerns. The average experience of the respondents on Facebook was between two and three years.

Table 3.2: Summary demographic descriptive statistics

Variable	Subgroup	N	%
Gender	Male	90	46.2%
	Female	105	53.8%
Facebook Experience	1 year experience	24	12.3%
	2 year experience	71	36.4%
	3 year experience	53	27.2%
	4 year experience	35	17.9%
	5 year experience	12	6.2%
Network	50 - 100	23	11.8%
	101 - 150	37	18.9%
	151 - 200	51	26.1%
	201 - 250	41	21.0%
	251 - 300	24	12.3%
	301 - 350	13	6.7%
	351 - 400	6	3.1%

Note. Gender: male and female

Facebook experience: years of experience on Facebook.

Network: quantity of friends list on Facebook.

3.4.4 Factor analysis

The factor analysis is used to determine if there are underlying factors in the variables or items. It looks at underlying patterns and correlations between the different items and places the items that have the same patterns together. This way it creates a factor (Thompson, 2004). A principal component analysis (PCA) was conducted for the respondents which in total comprised of 38 items. For an extensive view of the factor analysis I refer you to table 3.3. The PCA was used with oblique rotation i.e. direct oblimin rotation and tested this on all items. All factors below .30 are suppressed. According to Stevens (2002), the significance of the factor loading will also depend on the sample size. According to Tabachnick and Fidell (2007), the authors agree that it is comforting to have at least 300 cases for factor analysis and according to Comrey and Lee (1992); they class 300 cases as a good sample size, 100 as poor and 1000 as excellent. This study collected 220 cases and after the data analysis there were 195 left. According to the authors this sample size is not good or poor; it is an average sample size. Kaiser (1974) recommends accepting values greater than 0.5 as barely acceptable (values below this should lead to either collect more data or rethink which variables to include). It is important to start by testing the assumptions of the factor analysis. The can be done using Bartlett's test of sphericity (Appendix D), this test was significant *(Chi-square: 14144, df: 703, p < .001)* indicating that correlations between items were sufficiently large for PCA. Furthermore, Kaiser-Meyer-Olkin measure (KMO) of sampling adequacy was .757 which is well above the commonly recommended value of 0.5. Hutcheson and Sofroniou (1999) mention that values between 0.5 and 0.7 are average, values between 0.7 and 0.8 are good, values between 0.8 and 0.9 are great and values above 0.9 are superb. So the sample is definitely adequate for factor analysis. The initial factor analysis showed seven components where items are grouped together while there are seven variables tested. All constructs load on a component with a high factor loading. An overall impression of the factor analysis shows that values are between 0.55 and 0.95. According to the literature these are average and good. For an extensive view of the factor analysis and their corresponding values I refer you to table 3.3.

Table 3.3: Factor analysis pattern matrix

	Component						
	1	2	3	4	5	6	7
1.1 EE protect personal information							.767
1.2 EE easy privacy measure							.782
1.3 EE confident							.777
1.4 EE protect current location							.818
1.5 EE confident location services							.890
2.1 SI most people						-.965	
2.2 SI close friends						-.959	
2.3 SI members family						-.879	
2.4 SI peers						-.927	
3.1 PS losing information privacy				-.877			
3.2 PS online identity stolen				-.865			
3.3 PS personal information privacy				-.840			
3.4 PS losing photo privacy				-.855			
3.5 PS location based services				-.827			
3.6 PS data mining				-.824			
4.1 PV malicious computer/information					.595		
4.2 PV personal information misused					.773		
4.3 PV information available companies					.829		
4.4 PV available government agencies					.924		
4.5 PV information inappropriately used					.973		
4.6 PV current location					.995		
5.1 PE protect myself			.752				
5.2 PE privacy protection measures			.812				
5.3 PE ensure information privacy			.878				
5.4 PE lose information privacy			.916				
5.5 PE location based services			.939				
5.6 PE delete Facebook account			.829				
6.1 RW new friends		.873					
6.2 RW join applications		.774					
6.3 RW birthday wishes		.822					
6.4 RW join social groups		.875					
6.5 RW news about events		.821					
6.6 RW research about products		.762					
7.1 UPCS limit people's access	.808						
7.2 UPCS check privacy settings	.863						
7.3 UPCS prevent access	.816						
7.4 UPCS determine who can see	.778						
7.5 UPCS who contact me	.765						

Note. Extraction method: Principal component matrix
Rotation method: Oblimin with Kaiser Normalization
Rotation converged in 12 rotations

3.4.5 Reliability test

The general rule of thumb is that a Cronbach's Alpha *(a)* of .90 or higher is excellent, an *Alpha* from .90 to .80 is good, and an *Alpha* from .80 to .70 is acceptable (Gliem and Gliem, 2003). Table 4.1 shows the Cronbach's Alpha's for the ideal variable compositions. All constructs exceeded the recommended value (a > .70). The overall *Alpha* is .82 (Appendix E). Therefore, overall internal consistency can be assumed.

Table 3.4: Number of items, mean, standard deviation and reliability of variables

Variable	Items	Mean	SD	a
Use of Privacy configuration settings	5	4.16	1.61	.768
Perceived severity	6	5.96	.99	.793
Perceived vulnerability	6	5.52	.93	.801
Rewards	6	5.89	.70	.823
Performance expectancy	6	5.10	.84	.815
Effort expectancy	5	4.95	1.31	.789
Social influence	4	3.73	1.64	.772

Note. Appendix A and B shows the questionnaire items that were used in the questionnaire.

Scale: 7-point Likert scale (1 = strongly disagree to 7 = strongly agree

4. RESULTS

This chapter provides an overview of the results of the study. Areas covered include correlation analysis and hypothesis testing results. For a view on the Model summary and ANOVA table I refer you to Appendix G and H.

4.1 Correlation analysis

Table 4.1 shows the correlation between the different variables. Even though correlation does not imply causation, correlations are useful because they can indicate a predictive relationship between the variables (Cohen, Cohen, West and Aiken, 2013). For this study, the Pearson bivariate correlation is used. A bivariate correlation is a correlation between two variables. Looking at the table, it seems that there is a significant correlation between UPCS and EE *(r = .673),* SI *(r = .591),* PS *(r = .564).* It seems that there is a weak correlation between UPCS and RW *(r = .124)*, PE *(r = .371).*

Table 4.1: Means, standard deviations and correlations of the variables

Variable	Mean	SD	UPCS	PS	PV	RW	PE	EE	SI
Use of Privacy configuration settings	4.16	1.61	-	.564	.347	.124	.371	.673	.591
Perceived severity	5.96	.99	.564	-	.543	.271	.441	.218	.513
Perceived vulnerability	5.52	.93	.347	.543	-	.418	.202	.321	.499
Rewards	5.89	.70	.124	.271	.418	-	.384	.269	.273
Performance expectancy	5.10	.84	.371	.441	.202	.384	-	.285	.314
Effort expectancy	4.95	1.31	.673	.218	.321	.269	.285	-	.516
Social influence	3.73	1.64	.591	.513	.499	.273	.314	.516	-

Note. Correlation is significant at the 0.05 level (1 tailed). UPCS, Use of privacy configuration settings = PS, perceived severity = PV, Perceived vulnerability = RW, Rewards = PE, Performance expectancy = EE, Effort expectancy = SI, Social influence

4.2 Hierarchical linear regression analysis

Hierarchical linear regression was used to fit to predict the value of a variable based on the value of another variable added with demographic variables (Cohen et al, 2013). An overview of the variables and their corresponding predictors, coefficients and significance are shown in table 4.2. The outcome variable is 'Use of privacy configuration settings'.

In model 1, the variables from PMT are used in the hierarchical regression analysis. The analysis shows that out of the three analyzed predictors, *Perceived severity* tested as significant predictors of the *use of privacy configuration settings on Facebook ($p < 0.05$)*. In model 2, the variables from PMT and UTAUT are used in the hierarchical regression analysis. The analysis shows that out of the six analyzed predictors, three tested as significant predictors of the *use of privacy configuration settings* on Facebook *($p < 0.05$)*., namely: *Perceived severity, Effort expectancy* and *Social influence.* In model 3, the variables from PMT, UTAUT and the demographic variables are used in the hierarchical regression analysis. The analysis shows that out of the nine analyzed predictors, five tested as significant predictors of the *use of privacy configuration settings* on Facebook *($p < 0.05$)*. And the table shows that three predictors are not significant *($p > 0.05$).* The variable *'Effort expectancy'* is the strongest predictor of the variable, *use of privacy configuration settings ($\beta = .49$)* followed by the variable *Perceived severity ($\beta = .36$)* and the variable *Experience ($\beta = .26$).*

For the adjusted R squared values I refer you to appendix G. The adjusted R squared compares the explanatory power of regression models that contain different number of predictors. Model 1 explains 31.6% *(adjusted R square: .316)* the *use of privacy configuration settings on Facebook.* Model 2 explains 67.8% *(adjusted R square: .678)* the *use of privacy configuration settings on Facebook.* Model 3 explains 72.7% *(adjusted R square: .727)* the *use of privacy configuration settings on Facebook,* which is very large. In this case, the number of predictors improves the adjusted r squared.

Table 4.2: Coefficients

	Predictor	B	SE B	β	t	Sig
Model 1	*(Constant)*	-1.219	.933		-1.307	.193
	Perceived severity	.829	.121	.508	6.832	.000
	Perceived vulnerability	.227	.140	.132	1.621	.107
	Rewards	-.138	.163	.060	-.848	.397
Model 2	*(Constant)*	-1.387	.691		-2.005	.046
	Perceived severity	.622	.098	.382	6.336	.000
	Perceived vulnerability	-.074	.102	-.043	-.728	.467
	Rewards	-.408	.120	-178	-3.388	.001
	Performance expectancy	.148	.100	.078	1.481	.141
	Effort expectancy	.631	.086	.516	9.515	.000
	Social influence	.207	.059	.211	3.514	.001
Model 3	*(Constant)*	-1.088	.644		-1.690	.093
	Perceived severity	.584	.092	.358	6.374	.000
	Perceived vulnerability	-.043	.095	-.025	-.449	.654
	Rewards	-.404	.111	-.176	-3.643	.000
	Performance expectancy	.122	.094	.064	1.306	.193
	Effort expectancy	.585	.063	.479	9.327	.000
	Social influence	.148	.060	.151	2.446	.015
	Gender	.087	.136	.027	.639	.524
	Network	-.005	.001	-.215	-4.531	.000
	Facebook experience	.086	.086	.269	4.567	.000

Note. Note. Model 1: PMT, Model 2: PMT + UTAUT, Model 3: PMT + UTAUT + Demographic variables

Dependent variable: Use of privacy configuration settings

A significance level at 0.05 was used.

Table 4.3: Hypothesis testing results

Hypothesis		Result
H1	Perceived severity positively influences the use of privacy configuration settings on Facebook	Supported
H2	Perceived vulnerability positively influences the use of privacy configuration settings on Facebook	Rejected
H3	Rewards negatively influences the use of privacy configuration settings on Facebook	Supported
H4	Performance expectancy positvely influences the use of privacy configuration settings on Facebook	Rejected
H5	Effort expectancy positively influences the use of privacy configuration settings on Facebook	Supported
H6	Social influence positively influences the use of privacy configuration settings on Facebook	Supported
H7	Women make more use of privacy configuration settings on Facebook than men.	Rejected
H8	Network size positively influences the use of privacy configuration settings on Facebook	Rejected
H9	Facebook experience positively influences the use of privacy configuration settings on Facebook	Supported

Note. Dependent variable: Use of privacy configuration settings
At a.0.05 significance level.

Table 4.3 shows an overview of the hypothesis testing results. The hierarchical linear regression analysis showed that there was a significant ($p < a$) influence of these independent variables on the dependent variable, *use of privacy configuration settings.* Five out of nine hypotheses are supported.

5. DISCUSSION

This chapter provides an overview of the discussion of the study.

The goal of this study is to determine the factors that influence the use of Facebook's privacy configuration settings among adolescent users in the Netherlands. With use of the research model of the use of privacy configuarion settings on Facebook, it tried to answer the following research questions.

RQ1: To what extent do adolescents make use of privacy configuration settings on Facebook?

The literature suggested that privacy protection behavior and specifically the *use of privacy configuration settings* on Facebook is an example of a confrontative strategy. Confrontative strategies are for example mastering the settings provided by the SNS, or using firewalls and spam guards. This study was able to show that adolescent users of Facebook do make use of privacy configuration settings on Facebook. The study showed that users use the privacy configuration settings on Facebook to limit other people's access, regulate who can contact them, control who can see information on their timeline and accessing their Facebook account through search engines. In order to get more insight in what drives adolescent users to make use of the privacy configuration settings, the researcher proposed the following research question.

RQ2: What are the predictors of the use of privacy configuration settings on Facebook among adolescent users?

In order to test this research question, nine hypotheses were formulated and tested. Overall, five out of nine hypotheses were supported. In the following section the nine independent variables will be discussed.

Significant

This section provides a discussion of the significant factors.

Perceived severity

Hypothesis 1 proposed that there is a positive influence of *Perceived severity* on the use of privacy configuration settings on Facebook. *Perceived severity* contributes to the use of privacy configuration settings, thus supporting hypothesis 1. The literature suggested that the greater an individuals'

concerns about information collection and sharing practices, the more likely and individuals is to try to adopt privacy protection behaviors. *Perceived severity* impacts decisions of home wireless network users to implement security features and influences to use anti-spyware software (Larose et al, 2005; Norshidah and Hawa, 2012). This study was able to show that adolescent users of Facebook believe that losing information privacy would be a serious problem for them. They are aware of the consequences that could arise from using Facebook and therefore make use of privacy configuration settings on Facebook.

Rewards

Hypothesis 3 proposed that there is a negative influence of *Rewards* on the use of privacy configuration settings on Facebook. *Rewards* contribute to the use of privacy configuration settings, thus supporting hypothesis 3. The literature suggested that adolescent users of Facebook are aware of the risks involved then again they make the choice to put their personal information on their Facebook profile. They believe that they perceive greater benefits than costs from using Facebook. For playing social games or joining social applications they need to avoid using privacy configuration settings on Facebook for an optimal experience of these social applications (Boyd and Ellison, 2007; Christofides et al., 2012; Peluchette and Karl, 2008). This study was able to show that users of Facebook consciously expose their personal information on Facebook and therefore do not make use of privacy configuration settings. The users want to experience the full capabilities of Facebook and their apps and games.

Effort expectancy

Hypothesis 5 proposed that there is a positive influence of *effort expectancy* on the use of privacy configuration settings on Facebook. *Effort expectancy* contributes to the use of privacy configuration settings, thus supporting hypothesis 5. The literature suggested that *effort expectancy* explains the belief that a person has the ability to protect their personal information and if it is easy for them enable privacy measure features. It is also a predictor of the intention to use virus protection software. Empirical researches on *effort expectancy* continue to dominate the discussion on computer use (Chai et al, 2009; Venkatesh, Thong and Xu, 2012; Winter et al, 2014). This study was able to show that adolescents in the Netherlands feel that they have the ability to protect their personal information and it is easy for them to enable the privacy configuration settings on Facebook. They have the motivation to protect their information online.

Social influence

Hypothesis 6 proposed that there is a positive influence of *Social influence* on the use of privacy configuration settings on Facebook. *Social influence* contributes to the use of privacy configuration settings, thus supporting hypothesis 6. The literature suggested that *social influence* is the extent to which consumers perceive that important others (family and friends) believe that they should use a particular technology. It represents a certain perceived pressure to perform a behavior. It reflects the extent to which individuals of a social network influence each other (Kaba and Touré, 2014; Lin and Anol, 2008; Venkatesh, Thong and Xu, 2012). This study was able to show that important others of adolescent Facebook users influence the use the privacy configuration settings provided by Facebook.

Facebook experience

Hypothesis 9 proposed that there is a positive influence of *Facebook experience* on the use of privacy configuration settings on Facebook. *Facebook experience* contributes to the use of privacy configuration settings, thus supporting hypothesis 9. The literature suggested that individuals who have prior experience with SNS could have stronger privacy concerns and is more likely to have encountered privacy abuses. Therefore they could have negative experiences with SNS (Lankton and Tripp, 2013; Venkatesh, Thong and Xu, 2012). This study was able to show that the more years of experience you have on Facebook, the greater influence it has on the use of privacy configuration settings on Facebook. Users with more prior experience are more likely to have encountered privacy issues. Therefore they could have had prior negative experiences with Facebook.

Non-significant factors

This section provides a discussion of the non-significant factors.

Perceived vulnerability

Hypothesis 2 proposed that there is a positive influence of *Perceived vulnerability* on the use of privacy configuration settings on Facebook. No support was found of this influence. The literature suggested that in the case of virus protection behavior, people who perceive vulnerability to the threat of virus attacks are more likely to engage in virus protection behaviors, for example making use of anti-spyware software (Chenoweth, Minch and Gattiker, 2009; Norshidah and Hawa, 2012). This study was able to show that adolescent users do not believe that a threat will occur to him or her. They do not feel that their personal information on Facebook could be misused or feel that their personal information is made available to government agencies. Therefore this is not a motivation to make use of privacy configuration settings on Facebook.

Performance expectancy

Hypothesis 4 proposed that there is a positive influence of *Performance expectancy* on the use of privacy configuration settings on Facebook. No support was found of this influence. The literature suggested that *performance expectancy* explains whether an individual believes that using the system will help him or her to attain gains. It explains whether an individual enables a security measure in home wireless security or it influences behavior intention to use anti-spyware software as a protective technology (Woon, Tai and Low, 2005; Zhang and McDowell, 2009). This study was able to show that adolescent users of Facebook do not believe that the privacy configuration settings provided by Facebook is effective in protecting the self or others from a threat like losing your privacy.

Gender

Hypothesis 7 proposed that women make more use of privacy configuration settings than men. No support was found in the study of this difference. The literature suggested that females show greater concerns about their online privacy than males. They find that women are more likely than men to be concerned when a website mentions that personal information will be used by other organizations (Cockcroft and Clutterbuck, 2001; Dinev and Hart, 2004; Hoy and Milne, 2010; Laric, Pita and Katsanis, 2009; Youn and Hall, 2008). This study was able to show that there is no significant difference in the use of privacy configuration settings and *gender* type. The literature suggested that women are more concerned about privacy than men but this did not show in the study among adolescent users in the Netherlands.

Network

Hypothesis 8 proposed that there is a positive influence of *Network size* on the use of privacy configuration settings on Facebook. No support was found in the study of this influence. The literature suggested that larger and sparser networks are correlated with more sharing of emotion in microblogging (Kivran-Swaine and Naaman, 2011); Lin and Qiu, 2012). This study was able to show that the quantity of the friends list on Facebook does not influence the use of privacy configuration settings on Facebook.

6. CONCLUSIONS

This chapter provides an overview of the conclusions of the study.

Perceived severity, Rewards, *Effort expectancy, Social influence* and *Facebook experience* are the significant factors that influence the use of privacy configuration settings on Facebook by adolescent users in the Netherlands. It can be concluded that the proposed model's strongest predictor of an individual to use privacy configuration settings on Facebook is *Effort expectancy*, or the ability to protect their personal information and the ease of use of privacy configuration settings on Facebook. The second strongest predicting variable is *Perceived severity,* or the conclusion of the severity consequence resulting from a threatening security event.

The research provides the evidence that adolescent users of Facebook believe that their private information could be misused nevertheless they make the choice to make use of Facebook. Adolescent users recognize the likelihood of threats on Facebook, especially the negative threats. The users make assessments of the threats and are aware of the privacy configuration settings that are provided by Facebook. They perceive the benefits in getting connected with others or playing games in SNS, they may consciously expose their personal information toward attaining these benefits. Therefore, users perceive greater rewards derived out of Facebook and have less concern with their information privacy. Therefore they do not make use of the privacy configuration settings. Young adolescents' level of privacy concerns positively relates to the use of privacy configuration settings on Facebook. The users feel that they have the ability to protect their personal information with use of the privacy configuration settings provided by Facebook. Important others of adolescent Facebook users influence them to make use of the privacy configuration settings on Facebook.

However, *Perceived vulnerability* was not a significant factor for the use of privacy configuration settings. One could note that adolescents do not feel vulnerable during the use of Facebook. *Performance expectancy* was not a significant factor and therefore you could conclude that adolescent users of Facebook do not feel that the privacy configuration settings on Facebook are effective in protecting their privacy. *Gender* was not a significant demographic factor and therefore could conclude that women do not make more use of privacy configuration settings on Facebook than men. The size of the *network* on Facebook has no influence on the use of privacy configuration settings on Facebook.

7. IMPLICATIONS, LIMITATIONS AND SUGGESTIONS FOR FURTHER RESEARCH

This chapter provides an overview of the theoretical and practical implications, limitations and suggestions for further research of this study.

7.1 Implications

In this section the theoretical implications are discussed. First, this study combined PMT and UTAUT and contributes to the existing theory in some ways. The study adapted several PMT and UTAUT variables to the context of this study and proved that was very well possible. Because the use of only PMT could not be sufficient since only questions specifically on threat appraisals are asked and therefore an extension of the model with some of the UTAUT constructs was proposed to predict user intentions to use a technology. Second, the PMT literature focused on virus protection behavior, people who perceive vulnerability to the threat of virus attacks are more likely to engage in virus protection behaviors. It provides a framework for understanding fear appeals to see if users are motivated to protect themselves on Facebook. This study showed that the PMT variables hold in a social media context. Typically, the UTAUT literature showed that much research has been done in information systems and information technology. It aims to explain user intentions to use privacy configuration settings on Facebook. So this study showed that the UTAUT variables hold in a social media context and furthermore, with adolescents on the use of privacy configuration settings on Facebook. Last, this study contributes to existing theory in a sense that it provided further evidence that the two concepts can be combined. This study performed extensive validity and reliability analyses and showed that all the adapted constructs in the reliability analyses have high reliability factors. This study also assumes that the scales used in this study can also be extended to other SNS and are not only applicable in context of Facebook and adolescents.

In this section the practical implications are discussed. The following organizations or groups could benefit from the results of this study. First, understanding the use of privacy configuration settings on Facebook of adolescent users in the Netherlands can result in implementation of more effective privacy measures. Second, the study could be a start of privacy-measure redesign for Facebook. They could consider emphasizing on the privacy configuration settings by putting them more in front of the user. Third, educators and educational organizations could be used to change the perception of the users about threat appraisals, information privacy concerns and use of privacy configuration settings on SNS. Last, institutions could provide training programs to make the people aware of the risks and threats of Facebook. Training programs can include risks and threats of SNS use, areas of

vulnerabilities, consequences of information loss, information privacy awareness, privacy measures use and use of privacy configuration settings on Facebook.

7.2 Limitations

This study is not without limitations. There are several limitations to be mentioned with regard to this study. First, the variable *facilitating conditions* from UTAUT was not used. During the study it became evident that this variable could be for added value since it measures the degree to which an individual believes that an organizational and technical infrastructure exists to support use of the system. This variable could be added to the research model for a more extensive view of the use of privacy configuration settings on Facebook. Second, this study did not take different age categories into account. Therefore, you could not compare these different age categories in combination with the use of privacy configuration settings on Facebook. Last, this study did not include other educational levels, only high school students. Therefore you could not measure the difference in educational level and the use of privacy configuration settings on Facebook.

7.3 Suggestions for further research

This study is one of the few researches that combined PMT and UTAUT in this specific context of the use of privacy configuration settings on Facebook. However, there are several suggestions for further research. First, future studies should include *facilitating conditions* from UTAUT for understanding the motivating factors that initiate the use of privacy configuration settings on Facebook. Second, future studies in this context should focus more on different age categories. It could be interesting to see if there are differences in the use of privacy configuration settings on SNS and age. Third, future studies should also include different educational levels within the respondents. This study only used respondents from secondary school. It would be interesting to include these other educational levels and to find out if there are differences between educational level and the use of privacy configuration settings on SNS. Fourth, within this study, it would also have been interesting to use different SNS with this research model. This study only focused on Facebook but could also be used on other SNS to be able to do an analysis between the use of privacy configuration settings and different SNS. Last, it would be interesting to replace this study in other geographical settings. This questionnaire was only used on Dutch respondents but could also be used in other European countries to be able to do a cross-country analysis and find out differences between countries and to improve the external validity. In a later stadium, this study could also be extended to a non-European country to see if there are differences with other cultures. The relationship between culture and the use of privacy configuration settings on SNS could be a very interesting direction to research.

REFERENCES

Attrill, A. & Jalil, R. (2011). Revealing only the superficial me: Exploring categorical self-disclosure online. . *Computers in Human Behavior*, 27(5) , 1634–1642.

Beldad, A., De Jong, M., & Steehouder, M. (2011). A. comprehensive theoretical framework for personal information-related behaviours on the Internet. *The Information Society*, 27(4), 220-232.

Boer, H., & Seydel, E. R. (1996). Protection motivation theory.

Borena, B., Belanger, F., & Ejigu, D. (2013). Social Networks and Information privacy: A Model for low income countries. *Research in Progress*.

Boyd, D.M., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication.* , 13(1) , 210-230.

Chai, S., Bagchi-Sen, S., Morrell, C., Rao, H. R., & Upadhyaya, S. J. (2009). Internet and online information privacy: An exploratory study of preteens and early teens. *Professional Communication*, 52(2), 167-182.

Chenoweth, T., Minch, R. & Gattiker, T. (2009). Application of protection motivation theory to adoption of protective technologies. *In Proceedings of the 42nd hawaii international conference on system sciences,*, 1-10.

Christofides, E., Muise, A. & Desmarais, S. (2012). Risky disclosures on Facebook: The Effect of Having a Bad Experience on Online behavior. *Journal of Adolescent Research*, 27(6) , 714-731.

Christofides, E., Muise, A., & Desmarais, S. (2012). Hey Mom, what's on your Facebook? Comparing Facebook disclosure and privacy in adolescents and adults. *Social Psychological and Personality Science*, 3(1), 48–54.

Cockcroft, S. & Clutterbuck, P. (2001). Attitudes towards information privacy. *In Proceedings of the Australasian conference of information systems*.

Cohen, J., Cohen, P., West, S. G., & Aiken, L. S. (2013). Applied multiple regression/correlation analysis for the behavioral sciences. *Routledge.*

Comrey, A. L., & Lee, H. B. (1992). A first course in factor analysis (2nd edition). . *Hillsdale, NJ: Erlbaum.*

Cozby, P.C. (1973). Effects of density, activity, and personality on environmental preferences. *Journal of Research in Personality*, 7(1), 45-60.

Crossler, R. E. . (2010). Protection motivation theory: understanding determinants to backing up personal data. . *In Proceedings of the 43rd hawaii international conference on system sciences,*, 1-10.

Dinev, T., & Hart, P. . (2004). Internet privacy concerns and their antecedents - Measurement validity and a regression model. *Behavior and Information Technology*, 23(6), 413-422.

Douglas, W. O. (1966). *Justice.* Osborn v, United States.

Dwyer, C., Hiltz, S., & Passerini, K. (2007). Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. . *AMCIS 2007 Proceedings*, 339.

Edwards, J. (2014). 'Facebook Inc.' Actually Has 2.2 Billion Users Now — Roughly One Third Of The Entire Population Of Earth. *Business Insider*, http://www.businessinsider.com/facebook-inc-has-22-billion-users-2014-7?IR=T.

Ellison, N., Steinfield, C. & Lampe, C. . (2007). The benefits of Facebook "friends": Social capital and college students' use of online social network sites. . *Journal of Computer-Mediated Communication*, 12(4), 1143-1168.

Field, A. (2009). Discovering statistics using SPSS. *Sage publications.*

Garde-Perik, E. v. d., Markopoulos, P., Ruyter, B. d., Eggen, B., & Wijnand Ijsselsteijn, W. (2008). Investigating privacy attitudes and behavior in relation to personalization. *Social Science Computer Review*, 26(1), 20-43.

Gliem, J. A., & Gliem, R. R. (2003). Calculating, interpreting, and reporting Cronbach's alpha reliability coefficient for Likert-type scales. *Midwest Research-to-Practice Conference in Adult, Continuing, and Community Education.*

Grant, C. (2006). Online Privacy—An Issue for Adolescents? *Retrieved from: http://www.cbs.dk/content/download/41873/616561/*.

Hasebrink, U. (2009). Comparing children's online opportunities and risks across Europe: Cross-national comparisons for EU Kids Online. . *London: LSE, EU Kids Online*.

Hoy, M. G., & Milne, G. (2010). Gender differences in privacy-related measures for young adult Facebook users. *Journal of Interactive Advertising*, 10(2), 28-45.

Hutcheson, G., & Sofroniou, N. (1999). The multivariate social scientist. *Londen: Sage.* .

Jiang, Z., Heng, C. & Choi, B. (2013). Privacy concerns and privacy-protective behavior in synchronous online social interactions. *Information Systems Research*, 3, 579-595.

Kaba, B., & Touré, B. (2014). Understanding information and communication technology behavioral intention to use: Applying the UTAUT model to social networking site adoption by young people in a least developed country. *Journal of the Association for Information Science and Technology*, 65(8), 1662-1674.

Kaiser, H. F. . (1974). An index of factorial simplicity. *Psyhometrika*, 39, 31–36.

Kaplan, M. & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. *Business Horizons*, 53(1), 59-68.

Kivran-Swaine, F., & Naaman, M. (2011). Network properties and social sharing of emotions in social awareness streams. . *In Proceedings of the ACM 2011 conference on Computer supported cooperative work.*, 379-382.

Lankton, N. K., & Tripp, J. F. (2013). A Quantitative and Qualitative Study of Facebook Privacy using the Antecedent-Privacy Concern-Outcome Macro Model.

Laric, M. V., Pitta, D. A., & Katsanis, L. P. (2009). Consumer concerns for healthcare information privacy: A comparison of US and Canadian perspectives. *Research in Healthcare Financial Management*, 12(1), 93-111.

Larose, R., Rifon, N., Liu, S. & Lee, D. (2005). Online safety strategies: A content analysis and theoretical assessment.

Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: A model of online protection behavior. . *Behaviour and Information Technology.* , 27(5), 445–454.

Lenhart, A. & Madden, M. (2007). Teens, Privacy & Online Social Networks. Pew Internet & American Life Project.

Lin, C. P., & Anol, B. (2008). Learning online social support: an investigation of network information technology based on UTAUT. *CyberPsychology & behavior,*, 11(3), 268-272.

Lin, H., & Qiu, L. (2012). Sharing emotion on Facebook: network size, density, and individual motivation. . *In CHI'12 Extended Abstracts on Human Factors in Computing Systems*, 2573-2578.

Livingstone, S. (2008). Internet Literacy: Young People's Negotiation of New Online Opportunities. *In Digital Youth, Innovation, and the Unexpected, edited by Tara McPherson.*, (101–122).

Milne, G. R., Labrecque, L. I., & Cromer, C. (2009). Toward an understanding of the online consumer's risky behavior and protection practices. . *The Journal of Consumer Affairs.* , 43(3), 449–473.

Milne, George R., Andrew J. Rohm, and Shalini Bahl. (2004). Consumers' Protection of Online Privacy and Identity. *Journal of Consumer Affairs*, 38 (Winter): 217–232.

Moore, S. (2004). Moore, Elizabeth S. 2004. Children and the Changing World of Advertising. *Journal of Business Ethics*, 52 (2): 161–167.

Norshidah, M. & Ili Hawa, A. (2012). Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior*, 28, 2366-2375.

Oosterveer, D. (2015). Social Media in Nederland. *Marketingfacts*, http://www.marketingfacts.nl/berichten/social-media-in-nederland-2015-jongeren-haken-af-op-facebook.

Peluchette, J. & Karl, K. (2008). Social networking profiles: An examination of student attitudes regarding use and appropriateness of content. *CyberPsychology & Behavior*, 11(1) , 95-97.

Rogers, R. W. (1985). Attitude change and information integration in fear appeals. *Psychological Reports*, 56(1), 179-182.

Romer, D. . (2006). Stranger Contact in Adolescent Online Social Networks Common but Likelihood of Contact Depends on Types of Web Sites; Open Sites, Such as MySpace, More Prone to Stranger Contact Than Facebook. *The Annenberg Public Policy Center of the University of Pennsylvania*.

Saeri, A. K., Ogilvie, C., La Macchia, S. T., Smith, J. R., & Louis, W. R. (2014). Predicting Facebook users' online privacy protection: Risk, trust, norm focus theory, and the theory of planned behavior. . *The Journal of social psychology*, 154(4), 352-369.

Sánchez, R. A., Cortijo, V., & Javed, U. (2014). Students' perceptions of Facebook for academic purposes. *Computers & Education*, 70, 138-149.

Sheehan, K. B. (1999). An investigation of gender differences in on-line privacy concerns and resultant behavior. *, Journal of Interactive Marketing.*, 13, 4, 24-38.

Sheehan, K.B. and Mariea, G.H. . (1999). Flaming, Complaining, Abstaining: How Online Users Respond to Privacy Concerns. *Journal of Advertising*, 28 (3): 37–51.

Stevens, J. P. (2002). Applied multivariate statistics for the social sciences (4th ed.). *Hillsdale, NJ: Erlbaum*.

Tabachnick, B. G., & Fidell, L. S. (2007). Using multivariate statistics (5th edition). *Boston: Allyn & Bacon.* .

Thompson, B. (2004). Exploratory and confirmatory factor analysis: Understanding concepts and applications. *American Psychological Association.*

Van Deursen, A. J. A. M. & Van Dijk, J. A. G. M. (2012). Trendrapport internetgebruik Nederlands en Europees perspectief. *Universiteit Twente*.

Venkatesh, V., Thong, J. Y., & Xu, X. (2012). Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. *MIS quarterly*, 36(1), 157-178.

Venkatesh, V., Thong, J. Y., Chan, F. K., Hu, P. J. H., & Brown, S. A. (2011). Extending the two-stage information systems continuance model: incorporating UTAUT predictors and the role of context. *Information Systems Journal,*, 21(6), 527-555.

Wheeles, L. (1978). A follow-up study of the relationships among trust. . *Human Communication Research.* , 4(1) , 143-157.

Wheeless, L. & Grotz, J. (1976). Conceptualization and measurement of reported self-disclosure. . *Human Communication Research*, 2, 338-346.

Winter S., Neubaum, G., Eimler, S. C., Gordon, V., Theil, J., Herrmann, J.& Krämer, N. C. (2014). Another brick in the Facebook wall–How personality traits relate to the content of status updates. *Computers in Human Behavior*, 34, 194-202.

Woon, I., Tai, G. W. & Low, R. A. (2005). Protection Motivation Theory approach to home wireless security. In Proceeding of 26th international conference on information systems. . <*http://aisel.aisnet.org/icis2005/31*>, Accessed: 01-07-2015.

Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. .*Journal of Consumer Affairs*, 43(3), 389-418.

Youn, S., & Hall, K. (2008). Gender and online privacy among teens: Risk perception, privacy concerns, and protection behaviors. . *Cyberpsychology & behavior*, 11(6), 763-765.

Young, A. L., & Quan-Haase, A. (2009). Information revelation and internet privacy concerns on social network sites: a case study of facebook. *Proceedings of the fourth international conference on Communities and technologies*, 265-274.

Zhang, L., & McDowell, W. C. (2009). Am I really at risk? Determinants of online users' intentions to use strong passwords. *Journal of Internet Commerce*, 8, 180-197.

APPENDICES

Appendix A: Survey items (English)

Welcome to this study about the use of privacy configuration settings on Facebook by Aday Destici from the University of Twente. The goal of this study is to find out what the behavior is of adolescents on the use of privacy configuration settings on Facebook.

This questionnaire contains personal questions about Facebook. The questionnaire takes about 10 minutes of your time. Complete the questionnaire as best and honest as possible. Your answers will be treated anonymously. You do not need to leave your e-mail address behind. Your participation is voluntary so you can stop whenever you want. Your teacher, parents (Guardian) are aware of this study.

By starting with this survey, you confirm that you have agreed with the previous information.

Thanks you for your time!

Aday Destici
University of Twente

Question	
A. Information privacy concerns (Dinev and Hart, 2004)	1. I am concerned about submitting my personal information on Facebook because of what others might do with it. 2. I am concerned about submitting my personal information on Facebook because it could be used in a way I did not foresee. 3. I am concerned of location based services that are integrated in Facebook. 4. I am concerned about Facebook is using data mining to track your browsing behavior.
B. Effort expectancy (Dinev and Hart, 2004)	1. I believe I have the ability to protect my personal information on Facebook. 2. It is easy for me to enable privacy measure features on Facebook by myself. 3. I feel confident learning skills to protect my privacy on Facebook. 4. I believe that I have the ability to protect my current location on Facebook. 5. I feel confident dealing with the ways that Facebook uses location based services to determine my location.
C. Perceived severity (Dinev and Hart, 2004)	1. I believe that losing information privacy through Facebook would be a serious problem for me. 2. Having my online identity stolen through Facebook would be a serious problem for me. 3. Losing personal information privacy through Facebook would be a serious problem for me. 4. Losing photo privacy through Facebook would be a serious problem for me. 5. Losing my privacy through location based services on Facebook is a serious problem for me. 6. Losing my privacy through data-mining on Facebook is a serious problem for me.
D. Perceived vulnerability (Dinev and Hart, 2004)	1. I could be subjected to malicious computer/information security problems (e.g. virus, privacy, identity theft, hacking and etc.) on Facebook. 2. I feel my personal information on Facebook could be misused. 3. I feel my personal information on Facebook could be made available to unknown individuals or companies without my knowledge. 4. I feel my personal information in Facebook could be made available to government agencies. 5. I feel my personal information on Facebook could be inappropriately used. 6. I feel my current location could be inappropriately used by Facebook or other companies.
E. Performance expectancy (Dinev and Hart, 2004)	1. If I used privacy protection measures in Facebook, I could probably protect myself from losing my information privacy. 2. I can protect my information privacy better if I use privacy protection measures in Facebook. 3. Utilizing privacy protection measures in Facebook works to ensure my information privacy. 4. If I utilize information privacy protection measures on Facebook, I am less likely to lose my information privacy. 5. If I utilize location based services on Facebook, I am less likely to lose my information privacy. 6. If I delete my Facebook account, I am less likely to lose my information privacy.
F. Rewards (Dinev and Hart, 2004)	1. By losing my information privacy in Facebook I could get connected with new friends and friends from the past. 2. By losing my information privacy in Facebook, I could join applications (e.g. quizzes, games, etc.)

	3. By losing my information privacy in Facebook, I get birthday wishes from someone 4. By losing my information privacy in Facebook, I could join social groups. 5. By losing my information privacy in Facebook, I could get news about events. 6. By losing my information privacy in Facebook, I could research information about products.
G. Use of privacy Configuration Settings (Youn, 2009) *How do you make use of the privacy settings provided by Facebook to protect personal information?*	1. I limit other people's access to my Facebook account using privacy settings. 2. I regularly check my privacy settings in Facebook. 3. I use Facebook's privacy settings to prevent people from accessing my Facebook account through search engines. 4. I use the privacy settings of Facebook to determine who can see and access information I post on my Timeline. 5. I use the privacy settings of Facebook to determine who will be able to contact me.
H. Gender (Venkatesh et all, 2011)	What is your gender? 1. Male 2. Female
I. Age (Venkatesh et all, 2011)	What is your age? 1. 13 2. 14 3. 15 4. 16 5. 17
J. Facebook experience (Venkatesh et all, 2011)	1. 1 year experience 2. 2 year experience 3. 3 year experience 4. 4 year experience 5. 5 year experience 6. 6 years or more
K. Social influence (Venkatesh et all, 2011)	1. Most people who are important to me think I should use privacy settings on Facebook. 2. My close friends think I should use privacy settings on Facebook. 3. Most members of my family think I should use privacy settings on Facebook. 4. My peers think I should use privacy settings on Facebook.
L. Network size (Kivran-Swaine and Naaman, 2011)	How many friends do you have on Facebook?

Appendix B: Survey items (Dutch)

Welkom bij het onderzoek over het gebruik van privacy configuratie instellingen op Facebook door Aday Destici van de Universiteit Twente Enschede. Het doel van dit onderzoek is om er achter te komen wat het gedragspatroon is van jongeren op Facebook wat betreft privacy configuratie instellingen.

Deze enquête bevat vragen over uw persoonlijke ervaringen op Facebook. De enquête neemt ongeveer 10 minuten in beslag. Vul de vragen zo goed en eerlijk mogelijk in. Uw antwoorden zullen anoniem en vertrouwd behandeld worden. U hoeft niet uw e-mail adres of naam achter te laten. Uw participatie is vrijwillig dus u kunt stoppen wanneer u wilt. Uw docent, ouders (voogd) zijn op de hoogte van deze enquête.

Door te starten met deze enquête, bevestigt u dat u bent akkoord gegaan met de voorgaande informatie.

Bedankt voor uw tijd!

Aday Destici
University of Twente

Question	
A. Information privacy concerns (Dinev and Hart, 2004)	1. Ik ben bezorgd over het inleveren van persoonlijke informatie op Facebook door wat anderen er mee kunnen doen. 2. Ik ben bezorgd over het inleveren van persoonlijke informatie op Facebook omdat het kan worden gebruikt op een manier die ik niet had kunnen voorzien. 3. Ik ben bezorgd over locatie gebaseerde functies die zijn geïntegreerd op Facebook. 4. Ik ben bezorgd over Facebook die functies gebruikt om uw surfgedrag te volgen.
B. Effort expectancy (Dinev and Hart, 2004)	1. Ik geloof dat ik de bekwaamheid heb om mijn persoonlijke informatie op Facebook te beschermen. 2. Het is gemakkelijk voor mij om privacy maatregel functies op Facebook in te schakelen door mijzelf. 3. Ik ben zeker van mijzelf dat ik methoden ken om mijn privacy te beschermen op Facebook. 4. Ik geloof dat ik de bekwaamheid heb om mijn huidige locatie te beschermen op Facebook. 5. Ik voel mij goed met het feit dat Facebook locatie gebaseerde functies gebruikt.
C. Perceived severity (Dinev and Hart, 2004)	1. Ik ben van mening dat persoonlijke informatie verliezen op Facebook een ernstig probleem zou zijn voor mij. 2. Mocht mijn persoonlijke identiteit via Facebook gestolen worden dan zou dat een ernstig probleem zijn voor mij. 3. Persoonlijke informatie verliezen via Facebook zou een ernstig probleem zijn voor mij. 4. Het verliezen van foto privacy via Facebook zou een ernstig probleem zijn voor mij. 5. Het verliezen van mijn privacy door middel van locatie gebaseerde functies is een ernstig probleem voor mij. 6. Het verliezen van mijn privacy door middel van functies die mijn surfgedrag volgen is een ernstig probleem voor mij.
D. Perceived vulnerability (Dinev and Hart, 2004)	1. Ik kan het slachtoffer worden van kwaadaardige computer/informatie veiligheid problemen (bijvoorbeeld: virus, privacy, identiteit diefstal, hacking etc.) op Facebook. 2. Ik heb het gevoel dat mijn persoonlijke informatie zou kunnen worden misbruikt door Facebook. 3. Ik heb het gevoel dat mijn persoonlijke informatie op Facebook beschikbaar zou kunnen zijn aan onbekende personen of bedrijven zonder mijn medeweten. 4. Ik heb het gevoel dat mijn persoonlijke informatie op Facebook beschikbaar zou kunnen zijn voor overheidsinstanties. 5. Ik heb het gevoel dat mijn persoonlijke informatie op Facebook verkeerd zou kunnen worden gebruikt. 6. Ik heb het gevoel dat mijn huidige locatie op Facebook verkeerd zou kunnen worden gebruikt.
E. Performance expectancy (Dinev and Hart, 2004)	1. Als ik privacy bescherming maatregelen gebruik op Facebook, kan ik waarschijnlijk mijzelf beschermen tegen het verliezen van persoonlijke informatie. 2. Ik kan mijn persoonlijke informatie beter beschermen als ik gebruik maak van privacy bescherming maatregelen op Facebook. 3. Door gebruik te maken van privacy bescherming maatregelen op Facebook waarborg ik mijn persoonlijke informatie. 4. Als ik gebruik maak van privacy bescherming maatregelen op Facebook verminder ik de kans op het verliezen van mijn persoonlijke informatie. 5. Als ik locatie gebaseerde functies configureer op Facebook dan verminder ik de kans op het verliezen van mijn persoonlijke informatie.

	6. Als ik mijn Facebook account verwijder dan verminder ik de kans op het verliezen van mijn persoonlijke informatie.
F. Rewards (Dinev and Hart, 2004)	1. Door het verliezen van mijn persoonlijke informatie op Facebook, zou ik in contact kunnen komen met nieuwe vrienden en vrienden uit het verleden. 2. Door het verliezen van mijn persoonlijke informatie op Facebook, zou ik gebruik kunnen maken van applicaties (bijvoorbeeld: games, video's etc.). 3. Door het verlezen van mijn persoonlijke informatie op Facebook, zou ik felicitatie berichten kunnen krijgen van mensen. 4. Door het verliezen van mijn persoonlijke informatie op Facebook, zou ik kunnen toetreden tot sociale groepen. 5. Door het verliezen van mijn persoonlijke informatie op Facebook heb ik toegang tot informatie over evenementen. 6. Door het verliezen van mijn persoonlijke informatie op Facebook kan ik informatie verkrijgen over producten en diensten.
G. Use of privacy configuration settings (Youn, 2009) *Hoe maak je gebruik van de privacy configuratie instellingen die wordt aangeboden door Facebook?*	1. Ik gebruik de privacy configuratie instellingen zodat anderen beperkte toegang hebben tot mijn Facebook account. 2. Ik controleer regelmatig mijn privacy configuratie instellingen op Facebook. 3. Ik gebruik de privacy configuratie instellingen van Facebook zodat mensen mijn Facebook account niet kunnen vinden via zoekmachines. 4. Ik gebruik de privacy configuratie instellingen van Facebook zodat ik kan bepalen wat voor informatie op mijn tijdlijn toegankelijk is voor andere gebruikers. 5. Ik gebruik de privacy configuratie instellingen van Facebook zodat ik kan bepalen wie contact kan opnemen met mij.
H. Gender (Venkatesh et all, 2011)	Wat is uw geslacht? 1. Man 2. Vrouw
I. Age (Venkatesh et all, 2011)	Wat is uw leeftijd? 1. 13 2. 14 3. 15 4. 16 5. 17
J. Facebook Experience (Venkatesh et all, 2011)	Hoeveel jaar ervaring heeft u met Facebook? 1. 1 jaar ervaring 2. 2 jaar ervaring 3. 3 jaar ervaring 4. 4 jaar ervaring 5. 5 jaar ervaring 6. 6 jaar ervaring of meer
K. Social influence (Venkatesh et all, 2011)	Sociale invloeden 1. Veel mensen die belangrijk zijn voor mij zeggen tegen mij dat ik gebruik moet maken van privacy configuratie instellingen. 2. Mijn goede vrienden zeggen dat ik gebruik moet maken van privacy configuratie instellingen. 3. Leden van mijn familie zeggen dat ik gebruik moet maken van privacy configuratie instellingen. 4. Mijn leeftijdsgenoten zeggen dat ik gebruik moet maken van privacy configuratie instellingen.
L. Network size	Hoeveel vrienden heeft u op Facebook?

Appendix C: SPSS Variable view

Name	Label	Measure
Respnum	Respondentnummer	Scale
Vraag_1_1_IPC	1 Information Privacy Concerns	Ordinal
Vraag_1_2_IPC	2 Information Privacy Concerns	Ordinal
Vraag_1_3_IPC	3 Information Privacy Concerns	Ordinal
Vraag_1_4_IPC	4 Information Privacy Concerns	Ordinal
Vraag_2_1_EE	1 Effort Expectancy	Ordinal
Vraag_2_2_EE	2 Effort Expectancy	Ordinal
Vraag_2_3_EE	3 Effort Expectancy	Ordinal
Vraag_2_4_EE	4 Effort Expectancy	Ordinal
Vraag_2_5_EE	5 Effort Expectancy	Ordinal
Vraag_3_1_PS	1 Perceived Severity	Ordinal
Vraag_3_2_PS	2 Perceived Severity	Ordinal
Vraag_3_3_PS	3 Perceived Severity	Ordinal
Vraag_3_4_PS	4 Perceived Severity	Ordinal
Vraag_3_5_PS	5 Perceived Severity	Ordinal
Vraag_3_6_PS	6 Perceived Severity	Ordinal
Vraag_4_1_PV	1 Perceived Vulnerability	Ordinal
Vraag_4_2_PV	2 Perceived Vulnerability	Ordinal
Vraag_4_3_PV	3 Perceived Vulnerability	Ordinal
Vraag_4_4_PV	4 Perceived Vulnerability	Ordinal
Vraag_4_5_PV	5 Perceived Vulnerability	Ordinal
Vraag_4_6_PV	6 Perceived Vulnerability	Ordinal
Vraag_5_1_PE	1 Performance expectancy	Ordinal
Vraag_5_2_PE	2 Performance expectancy	Ordinal
Vraag_5_3_PE	3 Performance expectancy	Ordinal
Vraag_5_4_PE	4 Performance expectancy	Ordinal
Vraag_5_5_PE	5 Performance expectancy	Ordinal
Vraag_5_6_PE	6 Performance expectancy	Ordinal
Vraag_6_1_RW	1 Rewards	Ordinal
Vraag_6_2_RW	2 Rewards	Ordinal
Vraag_6_3_RW	3 Rewards	Ordinal
Vraag_6_4_RW	4 Rewards	Ordinal
Vraag_6_5_RW	5 Rewards	Ordinal
Vraag_6_6_RW	6 Rewards	Ordinal
Vraag_7_1_UPCS	1 Use of privacy Configuration Settings	Ordinal
Vraag_7_2_UPCS	2 Use of privacy Configuration Settings	Ordinal
Vraag_7_3_UPCS	3 Use of privacy Configuration Settings	Ordinal
Vraag_7_4_UPCS	4 Use of privacy Configuration Settings	Ordinal
Vraag_7_5_UPCS	5 Use of privacy Configuration Settings	Ordinal
Vraag_8_Gender	Gender	Nominal
Vraag_9_Age	Age	Ordinal
Vraag_10_FEXP	Facebook experience	Ordinal
Vraag_11_1_SI	1 Social Influence	Ordinal
Vraag_11_2_SI	1 Social Influence	Ordinal
Vraag_11_3_SI	1 Social Influence	Ordinal
Vraag_11_4_SI	1 Social Influence	Ordinal
Vraag_12_NW	Network	Scale

Appendix D: Factor analysis KMO and Bartlett's test

KMO and Bartlett's Test	
Kaiser Meyer-Olkin Measure of Sampling Adequacy	.757
Barlett's Test of Sphericity Approx chi square	14143.730
Df	703
Sig	.000

Appendix E: Cronbach's Alpha SPSS and crosstabs

Cronbach's Alpha	Cronbach's Alpha based on standardized items	N of items
.821	.825	7

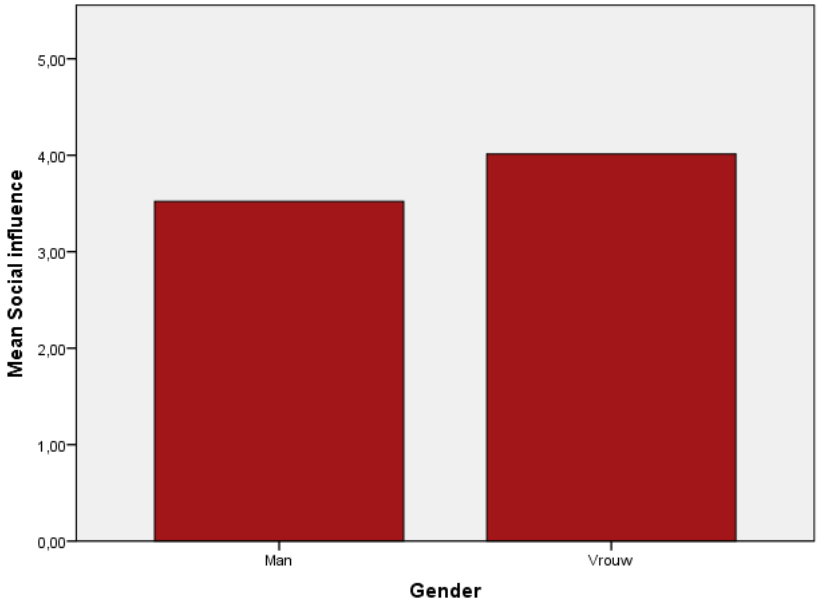
Note. Reliability statistics

Information privacy concerns

	Gender		
	Male	Female	Total
Completely disagree,	4	0	4
Mostly disagree,	4	0	4
Somewhat disagree	8	11	19
Neutral	0	8	8
Somewhat agree,	16	12	28
Mostly agree,	46	48	92
Completely agree	12	28	40
Total	90	105	195

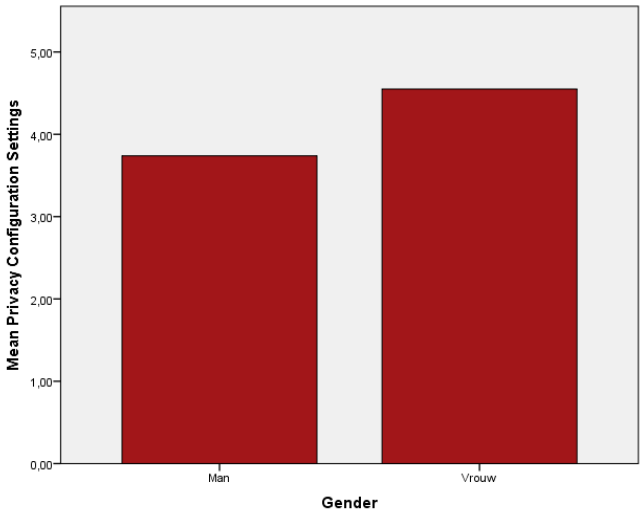
Note. Cross tabulation of information privacy concerns and gender

Appendix F: Additional graphs



Note. Most people who are important to me think I should use privacy settings on Facebook.

7 point Likert scale: 0.00: completely disagree, 1.00: mostly disagree, 2.00: somewhat disagree, 3.00: neutral, 4.00: somewhat agree, 5.00: mostly agree, 6.00: completely agree



Note. I use Facebook's privacy settings to prevent people from accessing my Facebook account through search engines.

7 point Likert scale: 0.00: completely disagree, 1.00: mostly disagree, 2.00: somewhat disagree, 3.00: neutral, 4.00: somewhat agree, 5.00: mostly agree, 6.00: completely agree

Appendix G: Model summary

Model 1 has only the UTAUT variables, Model 2 has the PMT and UTAUT variables and Model 3 has the PMT, UTAUT and demographic variables. The *R* value represents the simple correlation and can measure the quality of the prediction of the dependent variable and is *.572* for model 1, *.831* for model 2 and *.861* for model 3 which indicates a high degree of correlation. The R^2 value (The ''R square'' column) indicates how much of the total variation in the dependent variable (Use of privacy configuration settings) can be explained by the independent variables. In this case *.328* for model 1, *.689* for model 2 and *.741* for model 3 can be explained, which is very large.

Model summary

Model	R	R Square	Adjusted R Square	Std error of the Estimate
1	.572	.328	.316	1.32869
2	.830	.689	.678	.91223
3	.861	.741	.727	.83892

Note. Model 1: PMT, Model 2: PMT + UTAUT, Model 3: PMT + UTAUT + Demographic variables

Dependent variable: Use of privacy configuration settings

Appendix H: ANOVA table

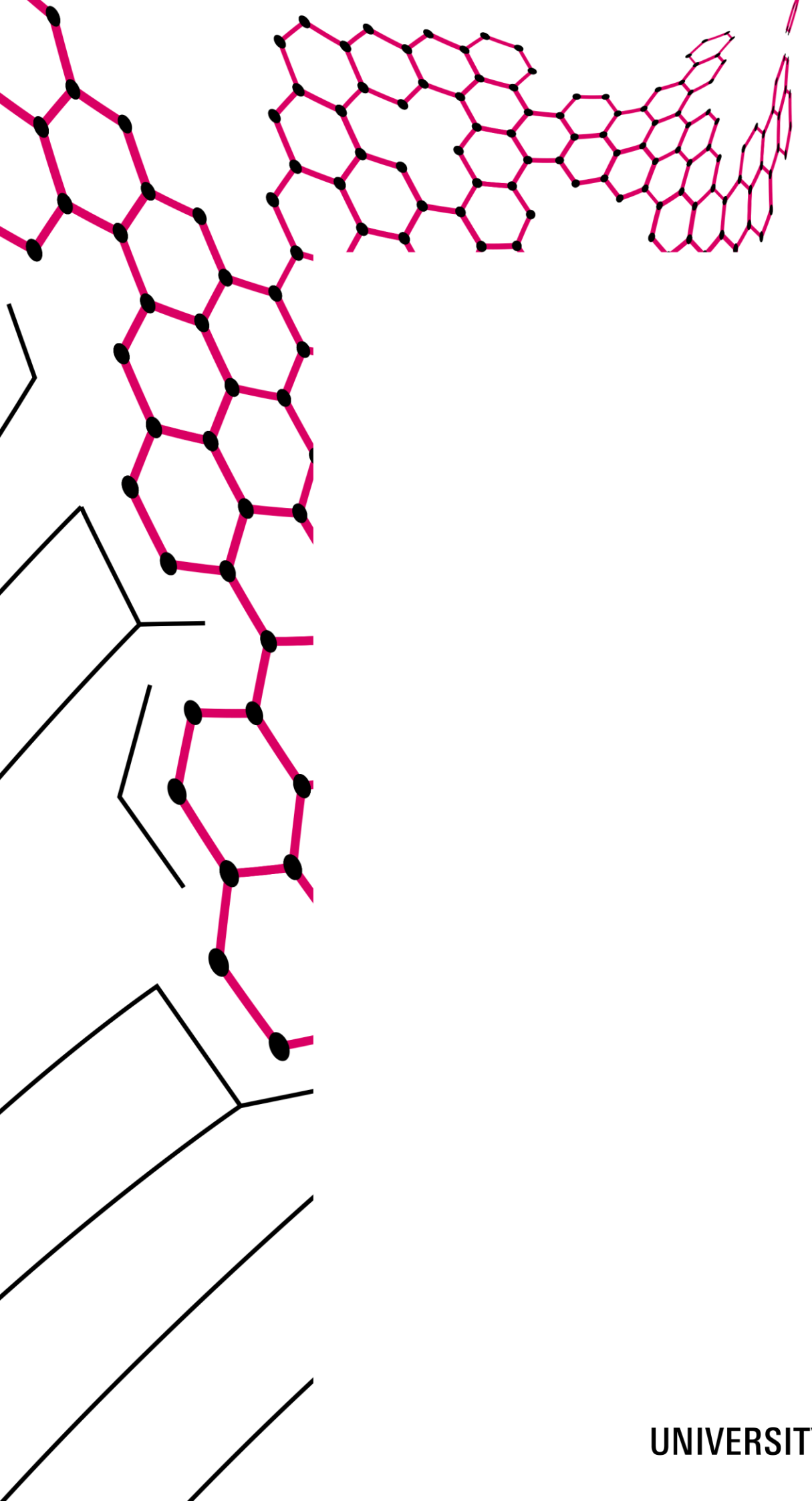
The *F* ratio in the ANOVA table tests whether the overall regression model is a good fit for the data. The table shows that the independent variables statistically significantly predict the dependent variable (Use of privacy configuration settings), Model 1*, F = 28.088, p < 0.05 (sig = .000).* Model 2*, F = 62.629, p < 0.05 (sig = .000)* and model 3, *F = 53.149, p < 0.05 (sig = .000).* There is no difference in significance for model 1, 2 and 3.

ANOVA table with F ratio, sum of squares and significance level

Model		Sum of squares	df	Mean square	F	Sig
1	Regression	148.759	3	49.586	28.088	.000
	Residual	305.417	192	1.765		
	Total	454.176	195			
2	Regression	312.708	6	52.118	62.629	.000
	Residual	141.459	189	.832		
	Total	454.176	195			
3	Regression	336.645	9	37.405	53.149	.000
	Residual	117.532	196	.704		
	Total	454.176	195			

Note. ANOVA. Model 1: PMT, Model 2: PMT + UTAUT, Model 3: PMT + UTAUT + Demographic variables

Dependent variable: Use of privacy configuration settings. Predictors (constant), Social influence, Effort expectancy, Perceived severity, Perceived vulnerability, Performance expectancy, Rewards, Gender, Age, Network, Facebook experience



UNIVERSITY OF TWENTE.