What factors influence Privacy Protection Behavior on social media and does the subjects Privacy Protection Behavior match their desired Privacy Protection Behavior?

Job Delfgou S1612271
Date: 01-07-19
Study Program: Management Society and Technology
University of Twente, Enschede
Word count: 15962
First Supervisor: Martin Rosema
Second supervisor: Ramses Wessel
Ethical approval number: 18849

Abstract

In this increasingly digital age, social networking sites have become an essential part of our daily social lives. The rise of these social networking sites is not without issues, as time goes on the harmful effects of social networking sites on personal privacy have come to light. From big data leaks to future employers taking a look on your Facebook page, the topic of privacy protection now is more relevant than ever. This is why this research has looked at digital Privacy Protection Behavior via a quantitative study among students between the ages of 18-29 using an adapted version of the Theory of Planned Behavior as a framework. The research aimed to look at the direct relations between attitudes on Privacy Protection Behavior, injunctive norms, descriptive norms, and perceived control on Privacy Protection Behavior. The research identified that attitudes on Privacy Protection Behavior was the strongest predictor of Privacy Protection Behavior and also revealed some interesting findings for injunctive norms and descriptive norms. The study also identified that among the subjects, there was a desire for better Privacy Protection Behavior. This shows that there is a desire for more Privacy Protection Behavior and that the best way to influence this behavior is via attitudes towards Privacy Protection Behavior.

Table of Content

1. Introduction

Today internet usage is as high as it has ever been, and it is only going to grow. Almost everything we do has at least some digital aspect to it, and our social lives are no different. However, this move to a more digital social life is not without its downsides. As Social Networking Sites have grown, so have the privacy concerns that they bring with them. An example of this is the Cambridge Analytica Scandal; here, data from Facebook users was collected and used on a large scale for marketing and political goals. The scandal was centered around the company Cambridge Analytica, which was a political consulting firm employed by among others the Trump campaign. The company obtained data of 87 million Facebook users through an application they created for this purpose (Chang, 2018). The application they created was a personality quiz called THISISMYDIGITALLIFE. This application was nothing special since there are many of these frivolous personality quizzes online that tell the user which kind of traffic sign you are. For instance. However, in order to be able to do this quiz, you had to give consent for the app to access the users' Facebook profile and the Facebook profiles of their Facebook friends. By doing this, the application gained access to the data of millions of Facebook users. This data would later be used for their political campaigns. Facebook itself permitted the collection of all the data, but they only did so because the creator of the app was a researcher at Cambridge University and he told Facebook the data would only be used for academic and commercial purposes (Propkom, 2018). However, the data was then passed on to Cambridge Analytica which used it for the Trump campaign for which they were paid to target potential voters based on the data they had obtained, thus violating the agreement with Facebook. When the scandal became public many saw this as a threat to democracy and as a significant breach in privacy law; however, it is debated whether this was the case. The company itself claimed that the usage of this data was essential in the Trump victory; however, if this was the case is still disputed (Propkom, 2018). However, what it does show is the ease in which lots of personal data can be leaked without the use of hacking. Furthermore, it is likely that these things will happen again and that with the increasing amount of online private data this problem will only keep expanding.

With this in mind, one would think the problem of digital privacy would be on everybody's mind; however, this does not seem to be the case. Although governments like the European Union has made stricter privacy laws in recent years, consumer behavior has hardly changed, and the number of Social Networking Site users keeps on rising. While stricter privacy laws are good for increasing privacy protection, the biggest problem seems to be consumer Privacy Protection Behavior. This problem is well known in academic circles and has been well researched. A widespread theory was already popularized in 2006; the privacy paradox theory by Barnes (2006) is one of the critical theories on Social Networking Site behavior. Her privacy paradox theory states that while many

Social Networking Site users state that (digital) privacy is important to them their Social Media behavior does not reflect this (Barnes, 2006, pp. 4). One of the explanations the theory gives for this behavior is that many (young) Social Networking Site users treat the Social Networking Site like it is a private space for them and their friends while this is not the case. As the general public knows now a Social Networking Site gathers and stores every bit of data they think will be useful to them and data that could be useful for them in the future.

Furthermore, not just a Social Networking Site is gathering data, but if your profile is public everyone can look at it includes parents' future employers etc.(Barnes, 2006, pp. 4-5). So users give access to parties they might not want to share personal details with. This paradox could explain some of the behavior since they see a Social Networking Site as a private space, they do not feel like they have to protect their privacy as much since its private. This point may not be as relevant now as it was in 2006 since nowadays almost everybody is aware that Social Networking Sites are not private spaces. However, Barnes also concluded that some students might be aware that a Social Networking Site is not a private space but act as if it is a private space. This second point is more relevant for current Social Networking Site users as knowledge about Social Networking Site has become more widespread, but a focus on informing Social Networking Site users of what kind of implications digital privacy infringement has seemed to be lacking.

Furthermore, the teaching of good Privacy Protection Behavior seems to be very decentralized and is left mostly to parents or individuals to do themselves. Thus, if one wants to influence Privacy Protection Behavior, it would begin by influencing the users and general norms on Privacy Protection Behavior. This current research tries to identify what kind of factors influences this individual Privacy Protection Behavior and if the users want to change their Privacy Protection Behavior. Because all users control their own Social Networking Site platforms by no small degree and changes in their behavior can directly influence the degree of digital privacy they have.

However, what is meant when we talk about Privacy Protection Behavior? Privacy Protection Behavior is not just about taking action to protect your privacy, but it is also influenced by the actions that you take that infringe on your privacy. A simple example of this can be posting on a Social Networking Site, when you do this the purpose of the action is not to give away private information you just want to share something with your friends, but when you do this you also directly are giving private details to the company that runs the Social Networking Site. Furthermore, simply not being registered on a Social Networking Site could be considered Privacy Protection Behavior. While Privacy Protection Behavior might not be the primary reason why someone is not on a Social Networking Site. But by not being on a Social Networking Site someone is not sharing their personal data and thus unknowingly protecting their digital privacy. Simply not being on a Social Networking Site is also becoming more and more of a choice as being on a Social Networking Site is becoming

more and more of a social norm as time goes on. Privacy Protection Behavior is influenced by a myriad of variables, and this research will try to look into what the most critical influences on Privacy Protection Behavior are.

This research will find out what influences' Privacy Protection Behavior among current students and to identify what you have to target if you want to change Privacy Protection Behavior in the future. The Theory of Planned Behavior by Ajzen was chosen as the basis for my theoretical Framework. This theory has been widely used in privacy protection research and to great success. I will only use the theory to look at current behavior. Therefore, the variable intention will be excluded and not be used as an intermediary dependent variable this will be further explained in the theory section. However, a separate independent variable will be used to see if subjects are currently happy with their current Privacy Protection Behavior or if they would like to change their current behavior in the future. This variable will be used to see if the subject feels that there is a gap between their privacy concerns and their current behavior, thus if a "privacy paradox" is present within my sample, which leads to the following research question.

Research Question: What factors influence Privacy Protection Behavior on social media and does the subjects' Privacy Protection Behavior match their desired Privacy Protection Behavior?

This research question is an empirical explanatory research question as it can be proven with observations and data. It is about cause and effect. What causes Privacy Protection Behavior or lack thereof among students between the ages of 18 and 29. This research will try to answer the research question by doing a quantitative study using an edited version of the theory of planned behavior by Icek Ajzen as a framework; some changes will be made to the theory in order to fit the research. The Theory of Planned Behavior was selected as a starting point because it is a well-known and proven theory for general behavior research, general Privacy Protection Behavior research (Saeri et al., 2015; Yao, & Linz, 2008) and also in research specifically focused on Social Networking Site users behavior (Baker & White, 2010; Kim et al., 2016). The research question is made up of two parts. The first part of the research question focuses on what factors influence Privacy Protection Behavior. The second part of the question is focused on the relevance of the research. If the factors that influence Privacy Protection Behavior are determined but it appears that subjects do not want their Privacy Protection Behavior to change this will likely reduce the effect of trying to influence Privacy Protection Behavior among subjects. If people are content with their behavior, they are unlikely to change, thus reducing the effect that possible actions trying to influence Privacy Protection Behavior will have. If it turns out that there is a significant difference between desired Privacy Protection Behavior and actual Privacy Protection Behavior, this would increase the relevance of the research

and provides a mandate for people that wish to increase Privacy Protection Behavior. The research question will be supported by five sub-research questions in order to help better answer the research question. The sub-research questions will be defined in the Theory section since they are heavily built on the Theory of Planned Behavior by Ajzen, which will also be further explained in the Theory section.

2. Theory

In this section, the theoretical background of the research will be explored. First, the concept of digital privacy and the concept of digital Privacy Protection Behavior will be explained. Secondly, the concept of social networking sites will be explained for the context of this research. Thirdly, the theory of planned behavior will be explained for the context of the research, and links between the concepts and the variables provided by the Theory of Planned Behavior will be elaborated. Finally, the theoretical model will be shown, and the relations between the independent variables and the dependent variable will be explained.

2.1 Digital privacy & Digital Privacy Protection Behavior.

When researching digital Privacy Protection Behavior, I first have to define the concept of digital privacy for my research. There is however no consensus on a single definition of digital privacy Wisniewski P, et al. (2014) defines the concept of privacy as “an interpersonal boundary process by which a person or group regulates interaction with others, by altering the degree of openness of the self to others” (Wisniewski. et al., 2014, pp. 1). This definition focuses on the autonomy of an individual to share personal details in different degrees for different people or services. Barnes has a similar definition; however, she notes is that this both entail the autonomy to share personal information and especially in the case of digital platforms also the autonomy to stop sharing personal details (Barnes, 2008, pp. 4). This definition, however, is more useful for privacy on a personal level and not on a digital level since in personal lives, people tend to tell different groups of friends more or less personal details based on how good they know them or like them. On social media, however, people tend to mainly share things on their page and thus to all of their connections on that Social Networking Site. The paper itself also shows that very few people engage in this selective sharing (Wisniewski. et al., 2014, pp. 4-6). For this research, a more general definition for privacy/digital privacy by Barnes will be used: “Privacy isn’t just about hiding things. It’s about self–possession, autonomy, and integrity. Privacy is the right of people to control what details about their lives stay inside their own houses and what leaks to the outside” (Barnes, 2006 pp. 4). This definition does not

only focus on the degree of openness but also on the right to control what details about them are revealed to the outside world. This broader definition of privacy allows for room in the questionnaire for questions about topics that do not directly reveal personal information but when large amounts of data are collected can lead social networks to conclusions about personal information. For example, when Facebook takes all the data of things you liked on Facebook, it can determine your interests without you stating your interests directly on Facebook (Facebook).

This definition of digital privacy leads to the definition for digital Privacy Protection Behavior: Digital Privacy Protection Behavior is all people consciously or subconsciously do to protect or not protect their digital privacy. An important distinction is that this definition includes both conscious and subconscious Privacy Protection Behaviors; this was done because of conscious and unconscious choices influence behavior. If you hear about data leaks on a Social Networking Site you may be less inclined to be active on that Social Networking Site, not because you decide to do this but because of increased mistrust towards that Social Networking Site because of the scandal. This shows that Privacy Protection Behavior is not limited to downloading or using tools to protect your privacy but is also influenced by how you behave on Social Media. While a Virtual Private Network might prevent a site from tracking your current location if you make a post about being at a particular event, they will still be able to obtain information about where you are. Besides ones current location, our current age of big data allows for everything you do on social media can be tracked. For example, Facebook can obtain a profile of your interests or even your political alignment simple from the posts you view or like on the platform (Facebook).

Furthermore, by the increasingly connected nature of the internet, slews of data can be obtained by Social Networking Site companies, when you log in on a website by using your Facebook account, you agree to share everything you do on that website with Facebook. Thus, reducing your engagement or the amount of time you spend on social media is becoming increasingly important for protecting your privacy. It also means that the Social Network User themselves are very much in control over their Privacy Protection Behavior. This, however, requires effort in a society in which Social Networking Sites are becoming increasingly more important in the social lives of people. Thus, protecting digital privacy will require a conscious effort from its users, and this is only going to increase as these Social Networking Sites continue to grow and reach into other spaces on the internet. To represent this in the research the questionnaire will both poses both questions about behavior that increases Privacy Protection Behavior and behavior that decreases Privacy Protection Behavior.

2.2 Social Networking Sites vs Social Media

Now that the definitions for digital privacy and digital privacy protection have been defined, a clear definition for Social Networking Sites for this research will be adopted. Barnes uses a definition from a proposed bill by Rep Fitzpatrick, which will also be used for this research. The definition is as follows: a "commercial social networking website" is a commercially operated Internet Website that; "(i) allows users to create web pages or profiles that provide information about themselves and are available to other users; and (ii) offers a mechanism for communication with other users, such as a forum, chat room, email, or instant messenger" (Fitzpatrick, 2006, Section 254(h)(7) of HR5319 IH.).

The best and most well-known example of this is Facebook, although it is sometimes generalized as a Social Media website/application. Because this research does not focus on Privacy Protection Behavior on social media but privacy protection on a Social Networking Site, it is essential to make a clear distinction between Social Media and Social Networking Site. While all Social Networking Site can be classified as Social Media Sites, not all Social media Sites can be classified as a Social Networking Site. For this research, some small details will be added to the definition of a Social Networking Site that was given. First, for a Social Networking Site to qualify for this research, one would have to be able to make a personalized profile with your real name, email address, and some general information about yourself. Secondly, you have to be able to write and share posts among all your contacts that are on the Social Networking Site, and lastly, you have to be able to like/follow things that interest you. Good examples of these kinds of profile-based social networking websites are Facebook, LinkedIn, and in the past things like Myspace and Hyves. While things like Snapchat or WhatsApp can fit the broad umbrella of Social Media, these tools are used more for interpersonal contact and not for sharing things with more than a select group of people.

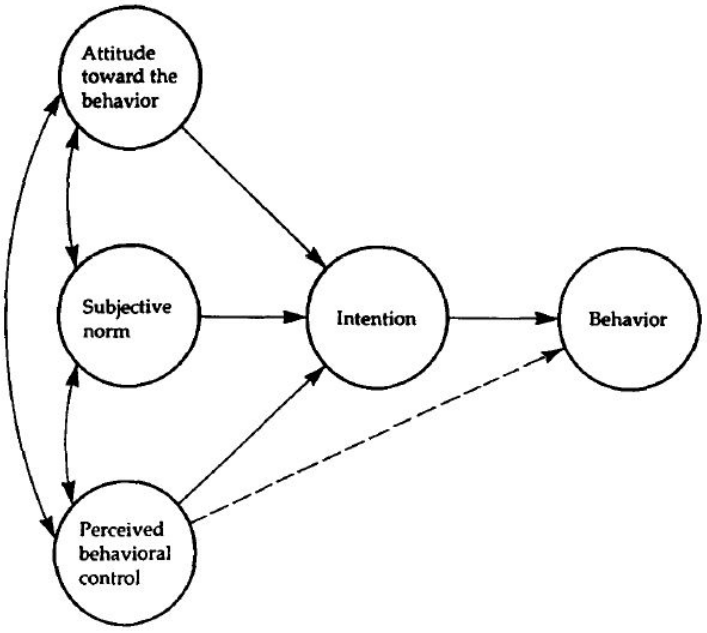
Furthermore, video websites like YouTube can be seen as a Social Networking Site; it is possible to share personal details in video form and interact with your "subscribers" via posts and videos. However, very few people use YouTube as a Social Networking Site, and it is mostly used to consume videos rather than sharing them. Lastly, this research will exclude online forums such as Reddit and Tumblr; this is because, on these websites, relative anonymity can be obtained through the freedom of usernames. While it is allowed to use your name, it is not required as with websites like Facebook and using your name is rarely done. This makes it harder for other users to find out who is behind a profile. This anonymity also makes it harder to form a Social network with other users due to the anonymity of the users on such a website. While all these platforms could gather personal details about you that could infringe your digital privacy for this research, we will focus on websites on which both other Social Networking Site users and the platform itself have access to personal information. Since these Social Networking Sites give the most tangible results for privacy

infringement and Privacy Protection Behavior, subjects will also be more likely to be familiar with these kinds of networks thus this will provide more reliable answers for the survey.

2.3 Theory of planned behavior

Now that the definitions for digital privacy, digital Privacy Protection Behavior, and Social Networking Site for this research have been defined as the framework which will be used to define what influences digital Privacy Protection Behavior. I have chosen the Theory of Planned Behavior as my framework because as stated before the theory already has been used for past studies regarding digital privacy and it is a flexible theory (Saeri et al., 2015, pp. 353; Yao, & Linz, 2008, pp. 615-616). Furthermore, past studies have proven that the Theory of Planned Behavior can be used successfully for the topic of Privacy Protection Behavior (Dieplin & Trepte, 2015; Yao & Linz, 2008).The Theory of Planned Behavior argues that reasonable human behavior can be predicted based on behavioral intention and Perceived Behavioral Control (Ajzen, 1991, pp. 179-186). The theory states that the stronger your intention to perform a particular behavior is the more likely it is that you will perform that behavior. This, behavioral intention, in turn, is based on three variables, attitude toward behavior, subjective norm, and Perceived Behavioral Control. However, the way these three variables interact with behavioral intention differs per behavior and situation; sometimes the attitude only has a significant impact on intention, sometimes attitudes and Perceived Behavioral Control can already predict behavioral intention, and sometimes all three variables make independent contributions to behavioral intention (Ajzen, 1991, pp. 188-189). However, the variable Perceived Behavioral Control also directly influences behavior according to the theory. For the Theory of Planned Behavior has to be reasonable, while you might have the intention to become the best football player in the world if you do not have the talent or the financial means you might not try it. Thus, in research where the subject is not limited by Perceived Behavioral Control, Behavioral Intention is a stronger predictor than in research where Perceived Behavioral Control is limited. The way these relations are framed can be seen in figure 1.

Figure 1: Theory of Planned Behavior.



The theory argues that in order to understand the effect an independent variable has (e.g., attitudes) on behavior, first you have to determine to what extent that independent affects behavioral intention. If the behavioral intention proves to be a relevant predictor for actual behavior the relevance of the independent variables can be determined. Furthermore, the independent variables can also be directly linked to actual behavior, creating a situation where, for example, attitude is both a significant direct predictor for behavior and a significant predictor via behavioral intentions. The way these variables are used, however, differs per research topic. This method, however, mainly looks at the change in behavior and is usually used in interrupted time series research. Because this research will be based on one point of measurement, the theory will be altered in order to fit this research better. The most significant change of this framework will be that the variable behavioral intention will be excluded from the framework. The research will look at direct links between behavior and the independent variables. This itself is not uncommon as in most Theory of Planned Behavior research behavior is explained via a combination of the independent variables and behavioral intention. This alteration on the standard framework was chosen because this research is focused on the direct relationship between the independent variables and Privacy Protection Behavior. For this, the intervening variable behavioral intentions are not necessary. The individual variables of the theory will now be further explained in with regards to the Theory of Planned Behavior and this research.

Attitude toward a behavior is about the willingness of the subject to behave in a certain way ergo do they like the consequences of behaving or not behaving in a certain way (Ajzen, 1991, pp. 191-195). Attitudes have been a reliable indicator for the behavioral intention in past privacy behavior

research (Kim, 2016, pp. 120-121) and have also been linked to directly predict Privacy Protection Behavior (Seari et al., 2015, p. 361). Ajzen defines attitudes in the Theory of Planned Behavior as follows: "According to this model, attitudes develop reasonably from the beliefs people hold about the object of the attitude. Generally speaking, we form beliefs about an object by associating it with certain attributes, i.e., with other objects, characteristics, or events. In the case of attitudes toward a behavior, each belief links the behavior to a certain outcome, or to some other attributes such as the cost incurred by performing the behavior. Since the attributes that come to be linked to the behavior are already valued positively or negatively, we automatically and simultaneously acquire an attitude toward the behavior" (Ajzen, 1991, p. 191). These attitudes are linked to the positive or negative effects that performing a specific behavior will have on the subject. However, attitudes about Privacy Protection Behavior are sometimes difficult to measure if framed in the wrong way. This is because protecting your (digital) privacy is usually seen as a mostly positive behavior. When you ask someone, the question would you like more or less privacy they will almost always answer that they want more privacy. However, if you ask someone if they are willing to give up something they like because it is considered lousy Privacy Protection Behavior, their attitudes with regards to Privacy Protection Behavior will change. Therefore, questions regarding attitudes towards Privacy Protection Behavior were not only focused on attitudes towards Privacy Protection Behavior but also on attitudes towards social media behavior that negatively affects Privacy Protection Behavior. By doing this attitude towards privacy protection should better reflect actual attitudes on Privacy Protection Behavior. This leads to the following sub-research question.

Sub question 1: What is the influence of attitudes on social media and Privacy Protection Behavior on social media subject's Privacy Protection Behavior?

Subjective norm is about the broader society that the user is in, does the society promote this kind of behavior, or is it looked down upon (Ajzen. I, 1991, pp. 195-196)? The significance of subjective norms in Privacy Protection Behavior studies has been debated. Yao & Linz, for instance, used subjective norms to explain attitude rather than intention (Yao & Linz, 2008, pp. 165-166). For this research, subjective norms, however, will be kept as an independent predictor for Privacy Protection Behavior. However, to increase reliability for the variable subjective norms, it was argued that the variable itself should be measured in a survey in two distinct ways: injunctive norms and descriptive norms which then can be merged into the variable subjective norms (Ajzen, 2006, p. 3). These two types of norms both describe the subjective norms in their way and add to the validity of the variable of subjective norms. In the past, the main thing that was being measured when talking about subjective norms was actually about the variable injunctive norms. Injunctive norms are about what the general behavioral norm is for a society. It describes what those who are closest to you see as desirable and undesirable behavior. For example, you should not smoke because smoking is bad.

However, subjective norms are not only influenced by what is seen as the best behavior but also by what significant others around you actually do. Descriptive norms, therefore, are about what is actually done by those significant others. While they may state that you should not smoke, significant others that do smoke will also influence your subjective norm on smoking.

A Meta-analysis by Mark Manning shows that the variable subjective norm should be split into injunctive and descriptive norms for Theory of Planned Behavior research. Furthermore, he states that depending on what kind of behavior is researched either injunctive norms, descriptive norms or both will be a better predictor of the behavior that is being researched (Manning. M, 2009). Saeri et al. used this method in their study and found then when this split is made both injunctive and descriptive norms were significant predictors of behavioral intention (Saeri et al., 2015, p. 354). They argued that making this distinction is especially crucial for privacy protection research as there is a misalignment between injunctive and descriptive norms, as the injunctive norm of protecting your privacy as well as you can is often not reflected by general behavior (Saeri et al., 2015, p. 354). It is expected that both variables are positively related to intention. This led to the following sub research questions.

Sub question 2: What is the influence of injunctive norms on Privacy Protection Behavior on social media subjects' Privacy Protection Behavior?

Sub question 3: What is the influence of descriptive norms on Privacy Protection Behavior on social media subjects' Privacy Protection Behavior?

Sub question 4: Did the split of the variable subjective norms into the variables injunctive norms and descriptive norms result in stronger and more significant independent variables for this research?

Finally Perceived Behavioral Control refers to the control that a subject believes it has over the behavior and if it will have the desired effect (Ajzen, 1991, pp. 196,198). Perceived control has been proven to be a strong predictor of behavioral intent (Yao & Linz, 2008, pp. 166-167). Furthermore, high levels of Perceived Behavioral Control have been linked to high privacy protection intentions and high Privacy Protection Behavior. This research has elected to leave out the financial aspect of Perceived Behavioral Control as most privacy protections solutions are available for all budgets and are usually free. For example, the most effective and free solution is not being or limiting the amount of time spent on the internet.

Furthermore, past research has already explored the effect of cost on Perceived Behavioral Control and while it had a small effect, personal preferences and ease of use showed to have higher effects Privacy Protection Behavior (Athley S. et al., 2017). A focus was placed on technical familiarity and control over their behavior as past research has already shown that experience with online platforms and self-efficacy can have a significant relation with perceived control over behavior

(Yao & Linz, 2008, pp. 615-6). It was assumed that students between the ages of 18 and 29 had a good basic understanding of how Social Networking Sites work and how to change their privacy settings for an instant. Therefore, a focus was placed on whether they found if these tools allowed them to control their Privacy Protection Behavior to the degree that they wanted. A focus was also placed on whether they felt they could stay off Social Networking Platforms or if they felt a constant need to be online. This resulted in the following sub-research question.

Sub question 5: What is the influence of perceived control over Privacy Protection Behavior on social media subjects' Privacy Protection Behavior?

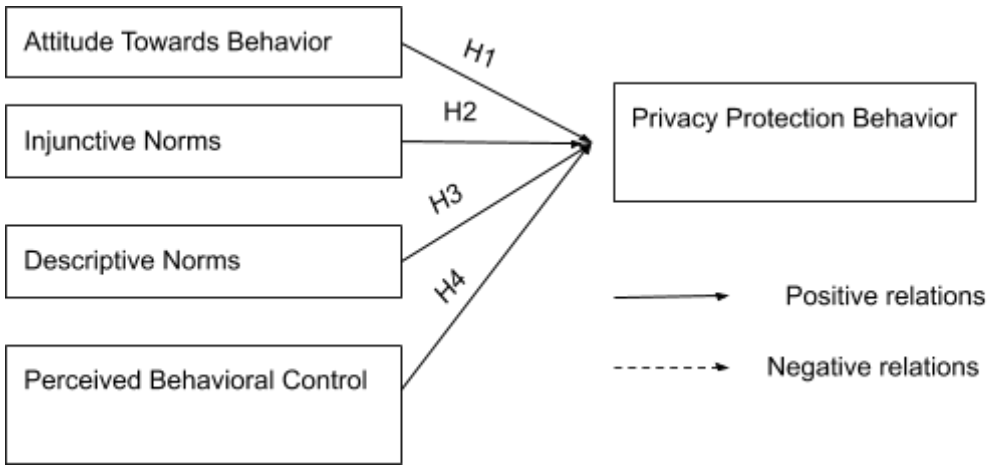
2.4 Theoretical model

The theoretical model is based on the standard model from the Theory of Planned Behavior; however, the behavioral intention was removed as an intervening variable. The hypothesis that the relations between the independent variables and dependent variables are positive was proven in a past study by Kim et al. and is assumed to be the same in this research (Kim, 2016, pp. 6-7), although behavioral intent here is replaced by Privacy Protection Behavior, which leads to the following hypothesis about the independent variables.

I. A positive relation between attitude towards social media and Privacy Protection Behavior is present. E.g. a high score for Attitude Towards Privacy Protection Behavior will lead to a higher score for Privacy Protection Behavior.
II. A positive relation is present between injunctive norms about Privacy Protection Behavior and Privacy Protection Behavior. E.g. if important others believe Privacy Protection Behavior is important this will lead to a higher degree of Privacy Protection Behavior.
III. A positive relation is present between descriptive norms about Privacy Protection Behavior and Privacy Protection Behavior. E.g. if important show high amounts of Privacy Protection Behavior this will lead to a higher degree of Privacy Protection Behavior in a subject.
IV. A positive relation is present between Perceived Behavioral Control and Privacy Protection Behavior. E.g. if the subject feels it has a high amount of control over its behavior this will lead to a higher degree of Privacy Protection Behavior in a subject.

This all leads to the following theoretical model:

Figure 2: Theoretical Model



2.5 Desire to change future Privacy Protection Behavior

While not directly related to the research question, the desire to change future social media behavior can increase the relevance that this research has for future studies, because this survey will also contain questions regarding the desire to change future social media behavior. While it is interesting to see what influences digital Privacy Protection Behavior, the practical implications will be more useful if their subjects are happy about their current Privacy Protection Behavior and thus are not willing to change. The survey will post questions about if you had to set up a new social media account would you change your current Privacy Protection Behavior. The average of this variable will be compared to that of the variable of Privacy Protection Behavior, which will show whether there is an intense desire amongst students to protect their privacy better than they are currently doing. If there is a strong desire to change current Privacy Protection Behavior, the main research question will answer which kinds of variables should be targeted to change Privacy Protection Behavior.

3. Methodology and operationalization

In this section, the methodology and operationalization of the research will be explained. It will start by outlining the research design and look at both the strengths and weaknesses of the research design. In the second part, the case selection and the selected sample will be elaborated on. In the third part, the operationalization of the main concepts and the method which was used to collect the data is further explained. This section also contains the descriptive statistics of the items which will be used in the variables and the reliability scores for the variables. The fourth and final section will show descriptive statistics for the variables and the general information of the sample. This was done to

provide to strengthen the conclusions that will be obtained from the regression analysis in the next chapter.

3.1 Research Design

In order to answer the main research question and the sub research questions, a quantitative research will be done using a questionnaire. This research design was chosen as it suits empirical exploratory research and will result in a higher number of participants than most other research designs. Using the Theory of Planned Behavior, clear independent and dependent variables can be identified, which can be measured and studied via items in a survey. In order to measure the Theory of planned behavior variables a set of questions will be made for each variable, besides these variables age, gender and study program will also be asked for some general information about my study. These general questions will reveal possible biases in the research based on, for example gender or study program. A strength of this design is that you get a relatively high number of participants and that there is a relatively low amount of influence from the researcher on the participants. The downsides of questionnaires are that if the questions are not adequately asked, they can steer the participants, which could result in biased answers and results. Secondly, when a questionnaire is too long participants might get bored and give answers quickly just to be done. This is especially relevant for digital questionnaires since the researcher is not present when the questionnaire is answered, and participants may feel less obliged to answer the questionnaire to the best of their abilities due to researcher not being present. A third downside is that when measuring Privacy Protection Behavior, this is usually done by checking actual behavior. For the scope of this thesis and privacy concerns, this will not be possible in this research and has to be measured using answers given in the questionnaire, this could result in less accurate answers. The questionnaire will use both normal and reverse scored items to prevent bias from positively or negatively phrased questions. The time it takes to finish the questionnaire will also be kept below 15 minutes to keep participants focused and clear and relevant questions will be formulated to test Privacy Protection Behavior concerning digital profiling. The questions will be answered using a 1-7 Likert scale; the research is set up in such a way that high scores indicate high privacy values, and low scores indicate low privacy values.

3.2 Case selection and sampling

For this research a random convenience sample will be selected from people who are currently students, they belong to the larger group of young adults (between 18 - 29 years old) as almost three quarters of this group are shown to use social media, and this percentage is increasing (Lenhart, A., 2010, pp. 17-18). Because my research is focused on people, who use Profile based Social Networking Sites, this will allow for a greater pool of potential participants as to when an older group

of people was selected. Teens have shown similar levels of social network usage; however, young adults were selected as they can give full consent for this research and are generally more aware of the consequences of their actions on social media. To limit skewed results based on an overrepresentation of a group based on the level of education, age, and intelligence, I have elected to look at university students as this will create a more even basis for knowledge and education. This does hurt the overall representation of the study, but this decision was made because the research not looking into the effect of education on Privacy Protection Behavior but on how the variables derived from the Theory of Planned behavior influence Privacy Protection Behavior. The data collected was a convenience sample which I obtained from sharing my survey on Facebook and via WhatsApp. It can be assumed that most participants study at the University of Twente since this is where most students, I know study. The sample was thus drawn from students within my network and eventually resulted in 98 responses.

3.3 Operationalization of the main concepts and data collection methods

To be able to answer my research question, a quantitative study will be conducted using a self-constructed survey. The survey is based on the framework that Ajzen has provided on how to construct a theory of planned behavior questionnaire (Ajzen, 2006, pp. 2-8). The interpretation of Seari et al. of how to apply the Theory of Planned Behavior to Privacy Protection Behavior research was used to specify this framework for the research. For their questionnaire, they used a unipolar 1-7 Likert scale, and reverse scored items were used to increase reliability (Seari et al., 2015, pp. 357-358). The survey has been set up in a way that high scores indicate a high amount of privacy protection, and low scores indicate a low amount of privacy protection. The questionnaire was split into six distinct parts one for each independent and dependent variable of my framework. A final item was added to get some general information about my sample and to find possible biases of the research (N=98). This results in the following measurements for each variable.

Attitudes towards Privacy Protection Behavior. To measure attitude towards social media & Privacy Protection Behavior, the study will measure eleven items related to social using a 7-point Likert scale. Five questions will be about opinions about social media and will measure attitudes on privacy protection (e.g., “I like sharing all my personal experiences online”; Measured on a 1 - 7 scale from 1 agree to 7 disagree). The second set of six questions will be about opportunities that social media platforms have to offer (e.g. “Social media helps you to keep up with current events”; Measured on a 1 - 7 scale from 1 like to 7 dislike). This category will measure attitudes on infringing privacy possibilities that social media platforms offer. The questions asked do not always directly relate to digital privacy but can be indirectly related to the topic of attitude towards privacy or social media. For example, if you like sharing photos online, this means in this aspect, you have a negative

attitude about digital privacy since you like sharing photos more than being private. I have chosen to do this because this will give a complete picture of attitudes towards privacy protection since most people will state they like privacy protection however they might also like functions of social media that limit their privacy protection. Asking their attitudes on these topics rather than just on the vague concept of attitudes on privacy protection will probably lead to more accurate answers. The means of these sets of questions were used to determine the mean score for the category attitude. Both categories contain some reverse scored items and were merged into the variable attitude on social media (α = 0,683). The reliability of the variable was relatively low; however, it could not be further increased. The items that made up the variable attitude can be seen in the table below.

Table 1: Descriptive statistics Attitude Towards Privacy Protection Behavior

Items	N	Min	Max	Mean	Std. Deviation
'Aa1 I like sharing all my personal experiences online.'	98	2	7	5.49	1.494
'Aa2I like posting photographs of me and my friends on social media. '	98	1	7	4.21	1.874
'Aa3 I like to express my opinions via social media.'	98	1	7	5.70	1.541
'Aa4rev Digital privacy is important to me.'	98	1	7	5.581	1.546
'Aa5rev I want to have control over who has access to my personal data.'	98	1	7	6.071	1.461
'Ab6 Social media allows you to see what your friends are doing.'	98	1	6	2.60	1.091
'Ab7 Social media helps you to keep in contact with people who are far away.'	98	1	6	1.90	1.117
'Ab8 Social media is used by advertisers to send you targeted messages.'	98	1	7	5.27	1.762
'Ab9 Social media is used by political parties to send you targeted messages.'	98	1	7	5.45	1.451
'Ab10 Social media helps you to keep up with current events.'	98	1	7	2.46	1.245
'Ab11 Social media informs you of upcoming events for example concerts or football matches you may be interested in.'	98	1	7	2.60	1.258
Valid N (listwise)	98				

Subjective injunctive norms

In order to measure subjective injunctive norms towards digital profiling, the study will measure six items related to digital profiling using a 7-point Likert scale. To measure social norms I chosen to ask subjects about what significant others, like friends, fellow students, parents, teachers and employers expect from their social media behavior (e.g., "Others expect me to be careful in what I share on social media"; Measured on a 1 - 7 scale from 1 they expect this of me to 7 they don't expect this of me). I have chosen for such a large group as the topic of digital privacy is influenced by many different people, and this allows the subjects to select who and what they think is the most important. The category contains reverse scored items to increase reliability, and scores will be averaged to form a reliable scale. After grouping the scores, the Cronbach's alpha for the variable was relatively low (**α** = 0,694). In order to see if this low Cronbach's alpha was the result of the structure within the questions that resulted in distinct dimensions, factor analysis was done with the extraction of eigenvalue greater than 1 and varimax rotation, which resulted in the following Table.

Table 2: Rotated Component Matrix[1] Injunctive Norms

Items	Component	
	1	2
'Ba12 Others expect me to be active on social media.'	0,831	0,054
'Ba13 Others expect me to be careful in what I share on social media. '	-0,074	0,932
'Ba14 Others expect me to be careful who I share my personal data with.'	0,022	0,935
'Ba15 Others expect me to like their posts.'	0,838	-0,057
'Ba16 Others expect me to post about my interests.'	0,871	-0,018
'Ba17 Others expect me to express my political opinions online.'	0,636	-0,056

Extraction Method: Principal Component Analysis.
Rotation method: Varimax with Kaiser Normalization.

1. Rotation converged in 3 iterations

Two item-groups were identified within the variable injunctive norms. The first item-group is: others expect me to be active on social media, Item Ba17 was excluded from the variable to further increase the Cronbach's alpha (**α** = 0,835). The second item-group is: others expect me to be careful on social media (**α** = 0,854). The split of the variable injunctive norm into two separate variables based on the item groups led to better Cronbach's alpha scores and will be used for the rest of the

analysis. Scores for both variables were averaged to form a reliable scale. This resulted in the following table of all items used in the table below, Here the three items bellowing to the variable others expect me to be active are listed as the top three items and the two items for Others Expect me to be Careful on social media are at the bottom.

Table 3: Descriptive statistics Injunctive norms

Items	N	Min	Max	Mean	Std. Deviation
'Ba12 Others expect me to be active on social media.'	98	1	7	4.70	1.766
'Ba15 Others expect me to like their posts.'	98	1	7	4.35	1.878
'Ba16 Others expect me to post about my interests.'	98	2	7	5.34	1.566
'Ba13rev Others expect me to be careful in what I share on social media. '	98	1.00	7.00	4.8367	1.53108
'Ba14rev Others expect me to be careful who I share my personal data with.'	98	1.00	7.00	4.9694	1.57594
Valid N (Listwise)	98				

Subjective descriptive norms

In order to measure subjective descriptive norms towards digital profiling, the study will measure six items related to digital profiling using a 7-point Likert scale. This category will ask similar questions as the injunctive category; however, instead of asking how others expect you to behave on social media, it asks how important others themselves behave on social media. (e.g., "They are active on social media"; Measured on a 1 - 7 scale from 1 they are to 7 they are not). Just as with injunctive norms, the Cronbach's alpha for the group was low (α = 0,624). The similarity between the questions of injunctive and descriptive norms, and the similarity of the results of the factor analysis was done for the variable descriptive norms with the extraction of eigenvalue greater than 1 and varimax rotation.

Table 4: Rotated Component Matrix[a] Descriptive norms

Items	Component		
	1	2	3
‘Bb18 They are active on social media.’	0,848	-0,039	0,221
‘Bb19 They are careful with what they share on social media. ‘	-0,091	0,856	-0,199
‘Bb20 They are careful with whom they share their personal data.’	-0,024	0,896	0,092
‘Bb21 They often like posts.’	0,901	-0,060	-0,065
‘Bb22 They often post about their interests. ‘	0,466	-0,136	0,639
‘Bb23 They often express their political opinions online.’	-0,045	-0,003	0,919

Extraction Method: Principal Component Analysis.
Rotation method: Varimax with Kaiser Normalization.

a. Rotation converged in 4 iterations

The first Item group is Others Are Careful on Social Media (**α** = 0,751). The Item group is Others are careful on social media (**α** = 0,710). The third item group Others post private details (**α** = 0,533) had a low Cronbach’s alpha and was therefore excluded from the rest of the analysis. The split of the variable descriptive norm into two separate variables based on the item groups led to better Cronbach’s alpha scores and will be used for the rest of the analysis. Scores for both variables were averaged to form a reliable scale. The items that were used can be seen in the table below. In it, the two items making up the variable Others Are Careful on Social Media are posted at the top, and the bottom two items are for the variable Others Expect me to be Careful.

Table 5: Descriptive statistics Descriptive Norms

	N	Min	Max	Mean	Std. Deviation
'Bb18 They are active on social media.'	98	1	6	2.76	1.193
'Bb21 They often like posts.'	98	1	7	2.50	1.221
'Bb19 They are careful with what they share on social media. '	98	1	6	3.13	1.297
'Bb20 They are careful with whom they share their personal data.'	98	1	6	3.22	1.272
Valid N (listwise)	98				

Perceived Behavioral Control

To measure Perceived Behavioral Control over Privacy Protection Behavior the study will measure seven items related to privacy protection using a 7 point Likert scale (e.g., "I can control the amount of data gathered about me. "; Measured on a 1 - 7 scale from 1 agree to 7 disagree). Items will then be averaged to form a reliable scale ($\boldsymbol{\alpha}$ = 0,676). The Cronbach's alpha for this variable was relatively low but could not be improved. A factor analysis was done to identify if this was the result of different dimensions being present in the structure of the questions. However, this did not lead to items with higher reliability; thus, the variable maintained its current form. The items that were used in the variable can be seen in table 6.

Table 6: Descriptive statistics Perceived Behavioral Control

Items	N	Min	Max	Mean	Std. Deviation
'C24 I experience a constant need to be online.'	98	1	7	4.35	1.834
'C25rev It is easy for me to put my phone away for several hours.'	98	1.00	7.00	4.6633	1.741
'C26rev I know how to reset my online profile.'	98	1.00	7.00	4.8980	2.108
'C27rev I can control the amount of data gathered about me.'	98	1.00	7.00	3.6020	1.849
'C28rev I know how to set who is allowed to see what on my social media profile.'	98	1.00	7.00	6.3265	1.072
'C29rev I have control over what social media websites do with my personal data.'	98	1.00	7.00	3.1224	1.783
Valid N (listwise)	98				

Privacy Protection Behavior

In order to measure actual Privacy Protection Behavior, eighth questions will be asked regarding the degree of Privacy Protection Behavior participants exhibit. A 7-point Likert scale (e.g., "I frequently like pages that align with my interests"; ranging from 1 agree to 7 disagree). In order to reduce bias because of socially desirable answers, it was elected to put the category Privacy Protection Behavior before the category desired Privacy Protection Behavior. These items will be averaged to form a reliable scale (α = 0,824). The items used to construct the variable Privacy Protection Behavior can be seen in the table below.

Table 7: Descriptive statistics Privacy Protection Behavior

Items	N	Min	Max	Mean	Std. Deviation
'E33 I frequently like pages that align with my personal interests.'	98	1	7	3.33	1.798
'E34 I frequently like posts by others.'	98	1	7	3.21	1.965
'E38 I have downloaded social media apps to my phone.'	98	1	7	2.09	1.856
Valid N (listwise)	98				

Desired Privacy Protection Behavior

To measure desired Privacy Protection Behavior the study will measure seven items related to digital profiling using a 7 Likert point scale (e.g., "I intend to be more careful in expressing my opinions online." ranging from 1 agree, and 7 disagree). The category will mainly ask the same questions as the category behavior but will ask them from a different angle: If you were to set up a new social media profile to what extent would you engage in the following behavior. This is done because the questionnaire wishes to measure similar behaviors to be better able to compare desired Privacy Protection Behavior to current Privacy Protection Behavior. Two items were reversed scored. Scores will be averaged to form a reliable scale (α = 0,708). The items used to construct the variable desired Privacy Protection Behavior can be seen in the table below.

Table 8: Descriptive statistics Desired Privacy Protection Behavior

Items	N	Min	Max	Mean	Std. Deviation
'D41rev I intend to be more careful in expressing my opinions online.'	98	1.00	7.00	4.265	1.875
'D43rev I intend to post fewer messages on social media.'	98	1.00	7.00	3.816	1.986
'D44rev I intend to reduce the amount of information that is collected about me.'	98	1.00	7.00	4.959	1.692
'D45rev I intend to use social media less than I am doing now.'	98	1.00	7.00	4.490	1.8177
Valid N (listwise)	98				

This all led to the following reliability scores for my independent and dependent variables. While the reliability scores for attitude and perceived control were low, they could not be improved by splitting them into multiple new variables or by removing items; thus, the current variables were maintained. These reliability scores are summarized in table 9.

Table 9: Reliability Scores independent variables

Variable	α
Attitude Towards Privacy Protection Behavior	,683
Others expect me to be active on social media	,835
Others expect me to be careful on social media	,854
Others Are Careful on Social Media	,751
Others are careful on social media	,710
Perceived control over social media behavior	,676
Degree of Privacy Protection Behavior	,824
Desire to improve Privacy Protection Behavior	,708

Finally, some general information (gender, age, study program, and social media usage) was asked in order to gain insight in the sample. The results for the general information will be shown and discussed in the next section of the thesis.

3.4 Descriptive statistics

The results from the questions about the general information revealed that the most substantial percentage of the participants were between the age of 18-21. This could cause Privacy Protection Behavior scores to be lower as it was found that younger people usually are less protective of their digital privacy and tend to share more on social networking sites (Barnes, 2006, p. 2). Furthermore, there was a slight overrepresentation of females in the study (58 females, 40 males). This overrepresentation could result in scores for Privacy Protection Behavior being higher as it has been proven that females on average are more careful regarding their digital privacy as their male counterparts (Youn & Hall, 2008, pp.1-3). The question regarding hours on social media was asked to see how familiar participants were with social media. If the majority of the sample did not spend much time on social networking sites it would be problematic. This was, however, not the case; thus, it can be assumed that most of the participants were familiar with social networking sites increases the likelihood that they answer my questions accurately. There was also an imbalance in study programs, as 60% of the participants came from social or medical studies. This is likely because my social network is mostly spread over these two faculties, thus increasing the response from these programs. This means that the results might not fully represent technical or ICT students.

Table 10: Descriptive statistics general statistics

Item	N	Minimum	Maximum	Mean	Std. Deviation
Age	98	18	29	21.88	2.882
Gender (-1 male, 1 Female)	98	-1	1	.184	.988
Hours on Social media (1 0-5, 2 5-10, 3 10-20, 4 20-40, 5 40+)	98	1	5	2.428	1.005
Study Program (1 Technical, 2 Social, 3 ICT, 4 Medical, 5 Other)	98	1	5	3.194	1.404

Table 11: Frequency table general statistics

Item	N	18-21	22-25	26-29		
Age	98	52	36	10		
	N	Male	Female			
Gender	98	40	58			
	N	0-5 hours	5-10 hours	10-20 hours	20-40 hours	40+ hours
Hours on Social media	98	20	32	31	14	1
	N	Technical	Social	ICT	Medical	Other
Study Program	98	11	32	5	27	23

Statistics from the general questions revealed that there was no major overrepresentation from a single gender, or study program. Scores from each item were averaged and set to a 0 to 1 scale with low scores indicating low privacy protection scores and high scores indicating high privacy protection scores. It is interesting to note that the mean scores for injunctive and descriptive norms are very different. This indicates that there is a big difference between what others say you should do and what they do themselves. It is also interesting to note that the mean score for the variable Others expect me to be active on social media is this high. This means that subjects felt that there is a significant amount of peer pressure to be on social media.

Table 12: Descriptive statistics used variables

	N	Min	Max	Mean	Std. Deviation
Attitude Towards Privacy Protection Behavior	98	.12	.86	.551	.119
Others expect me to be active on social media	98	.17	.00	.633	.252
Others expect me to be careful on social media	98	.00	.00	.633	.242
Others Are Careful on Social Media	98	.00	.92	.271	.180
Others are careful on social media	98	.00	.83	.363	.189
Perceived control over social media behavior	98	.11	.94	.582	.181
Degree of Privacy Protection Behavior	98	.00	1.00	.313	.269
Desire to improve privacy protection	98	.00	1.00	.564	.225
Valid N (listwise)	98				

4. Data analysis

In this chapter, I will look at the results of my regression analysis. First, a correlation analysis was done to get an initial view of the relations between the variables. After this, a hierarchical multiple linear regression analysis was done to determine how strong the relationship between each independent variable and the dependent variable is and how much of the dependent variable can be attributed to the independent variables. For the regression analysis, four regression analyses were run to see how the R-squared changed with each additional variable. Each of the variables was added individually with attitudes, injunctive norms second, descriptive norms third, and perceived control fourth. This provides more insight into how the analysis changes with each additional variable. The order in which the variables were added was based on expected prediction values. The strongest predictor from past research was added first, second strongest second, the weakest was last (Seari et al., 2015, pp. 361; Yao & Linz, 2008, p. 616). After this, a closer look was taken at the regressions for each variable individually, and preliminary conclusions were drawn for each of them. Then a closer look will be taken at the second part of the research question and the relation between Privacy Protection Behavior and desired Privacy Protection Behavior will be analyzed. After this analysis,

conclusions will be drawn, and suggestions for future research will be made. SPSS version 25 was used for the analysis.

4.1 Correlations

A bivariate Pearson correlation analysis was done to see the correlation between the dependent and independent variables. The results can be seen in table 4, preliminary findings will also be specified in the table below.

Table 13: Correlation Table used variables

	Degree of Privacy Protection Behavior	Attitude towards social media	Others expect me to be active on social media	Others expect me to be careful on social media	Others Are Careful on Social Media	Others are careful on social media	Perceived control over social media behavior
Degree of Privacy Protection Behavior		.539**	.369**	-0.037	.399**	-0.052	0.122
Attitude Towards Privacy Protection Behavior			.425**	0.143	.236*	-0.029	0.023
Others expect me to be active on social media				0.040	.378**	-0.076	0.101
Others expect me to be careful on social media					0.090	-.325**	0.035
Others Are Careful on Social Media on social media						-0.133	0.043
Others are careful on social media on social media							-0.006
Perceived control over social media behavior							

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

As can be seen in the correlation table 13 above, there are significant and robust correlations for Privacy Protection Behavior and three of the independent variables. The strongest correlation is between Privacy Protection Behavior and Attitude Towards Privacy Protection Behavior R = .539 and

P = .000; this is in line with past researches where the attitude towards behavior and privacy behavior also had a high correlation. Furthermore, there is also a strong correlation between the injunctive and descriptive norms for being active on social media with others expect me to be active on social media R = .369 and a significance of P = .000, and Others Are Careful on Social Media R = .399 and a significance of P = .000. It is interesting to see that the positive variables towards social media (activity on social media) for subjective norms correlate strongly while the negative variables towards social media (being careful on social media) do not correlate strongly and are not significant. Finally, the variable Perceived Control over Social media did not strongly correlate and was not significant.

4.2 Regression Analysis

A hierarchical multiple Regression analysis was done in which each of the independent variables was added separately to get a better view of the change in the model. The result of this is shown in table 14 below. A closer look will be taken at each of the variables after some general findings are listed.

Table 14: Hierarchical Multiple Regression Analysis of Independent variables on Privacy Protection Behavior Coefficients (**β**).

Predictor	Model 1	Model 2	Model 3	Model 4
Attitude Towards Privacy Protection Behavior	.539***	.484***	.465***	.468***
Others Expect you to be Active on Social Media		.168*	.072	.062
Others Expect you to be Careful on Social Media		-.113	-.145*	-.149*
Others Are Careful on Social Media			.269**	.268**
Others Are Careful on Social Media			-.044	-.046
Perceived Behavioral Control				.099
Constant	-.357	-.320	-.294	-.371
R^2	.284***	.306***	.359***	.362***

Note:*p < .05, **p < ,01 ***p < ,001

At first glance, you can already see that the Attitude Towards Privacy Protection Behavior seems to be the strongest predictor for Privacy Protection Behavior. However, when more variables are added, this diminishes slightly. Furthermore, when injunctive norms are added in Model 2, the

variable Others Expect you to be Active on Social Media is stronger and more significant than Others Expect you to be Careful on Social Media. However, when in Model 3, descriptive norms are added; this inverted. It is also interesting to see that for both injunctive and descriptive norms, just one of the independent variables is strong and significant. I will now go past the variables one by one starting with the dependent variable behavior and then the independent variables in the order they were in the analysis.

The independent variables predicted a decent amount of the dependent variable behavior with an adjusted R2 value of .362. The variable is highly correlated with the independent variables Attitude, Others Expect me to be Active, and Others Are Active. Together these variables account for 87,6% of the change in the variable. Past research has shown that the variable attitude has always played an important role in Privacy Protection Behavior. It, however, was not common that the variable subjective norms were a strong and significant independent variable for the dependent variable Privacy Protection Behavior, which is likely the result of splitting the variable subjective norms into injunctive (Others Expect you to be Careful) and descriptive norms (Others Are Active).

Attitude had the highest correlation of the independent variables with Privacy Protection Behavior. In the regression analysis, it also had the highest coefficient value (**β**) in model 4 and was highly significant (**β**Model4 = .468 pModel4 = .000). This result answers the sub-research question 1 as the variable is still a strong and significant predictor of Privacy Protection Behavior, which is in line with most past research on privacy behavior where attitude also play a dominant role. Furthermore, the hypothesis that attitude has a positive relation with Privacy Protection Behavior also is proven by these results.

Both injunctive and descriptive norms were split into two variables resulting in four variables in total. Of these four variables, two variables had a significant effect on Privacy Protection Behavior. For injunctive norms the variable Others Expect me to be Careful on social media (**β**Model4 = -.149 pModel4 = .046) and for descriptive norms Others Are Careful on Social Media (**β**Model4 = .268 pModel4 = .003). When taking into account what these variables stand for, this seems like a logical outcome. Because injunctive norms deal with more “general” social norms, you would expect that things like “you should protect your privacy on social media” play an important role. However, for descriptive norms, you do not actively look for or ask how others protect their privacy, but you rather see what they do on social media. However, you do see their posting behavior on social media and see negative privacy behavior. With regards to this, it makes sense that the variables Others Expect me to be Active and Others are Careful are not significant since they do not fit their respective overarching variables of injunctive and descriptive norms. This proves that splitting subjective norms in the context of privacy protection can give strong and significant variables. However, to test if these variables were stronger than if they were measured for subjective norms, the variables injunctive

norms and descriptive norms were merged. The split between active and careful was maintained for the subjective norms. This resulted in two new variables for subjective norms (SubActive & SubCareful). The results can be found in the table below.

Table 15: Hierarchical Multiple Regression Analysis of Independent variables on Privacy Protection Behavior Coefficients (**β**).

Predictor	Model 1
Attitude towards Privacy Protection/Social media	.442***
Subjective norm Active on Social media	.263**
Subjective norm Careful on Social media	-.122
Perceived Control	.091
Constant	-.361
R^2	.352***

Note: *p < .05, **p < .01 ***p < .001

As can be seen in the table 15, the values for subjective norms are almost the same as when they are split between injunctive and descriptive only now the two weak variables are mixed in. The variables were slightly stronger when they were split; furthermore, the injunctive variable Others Expect you to be Careful on Social Media was also more significant than the subjective variable for Careful on social media ($P_{InjunctiveCareful}$= .046 $P_{SubjectiveCareful}$= .072). This led to the following conclusion for sub question 2. While the difference is not tremendous, results are slightly more significant and stronger when replacing the variable subjective norms with the variables injunctive and descriptive norms. However, there seems to be a positive relation between Social Networking Site activity and Privacy Protection Behavior and a negative relation between being careful on a Social Networking Site and Privacy Protection Behavior. This seems rather strange since logically you would expect it to be the other way around. A possible explanation for this could be that subjects believe they know how to behave on a Social Networking Site and consider others telling them to be careful as nagging. However, the low mean score for Others Are Careful on Social Media could explain the outcome in this relation. Since the perceived activity of others on social media is low, this could encourage a subject to also not be as active on social media and thus protecting their privacy. However, these results could also be the result of unclarity within the questionnaire, and further research would have to be done to clarify this. The hypotheses that both relations would be positive seems to be rejected by these results.

Perceived control turned out to have almost no impact on the dependent variable of Privacy Protection Behavior and also was not significant ($\boldsymbol{\beta}_{Model4} = .099$ $p_{Model4} = .230$). This was in line with for instance the research done by Seari et al. but not with the research done by Kim et al. and Yao & Linz (Kim et al., 2016, p. 12; Seari et al., 2014, p. 361; Yao & Linz, 2008, p. 616). It seems that the more independent variables the research has, the less relevant Perceived Behavioral Control is. The research of Kim used four and Yao two variables to predict intention while Seari used eight variables. My research used six variables, so this could be a reason why the Perceived Behavioral Control gave such a weak result. Lastly, the hypothesis that perceived control is positively related to Privacy Protection Behavior is proven by these results even if the relationship is not that strong.

4.3 The role of Gender in Privacy Protection Behavior

After the results of the regression analysis have shown the main predicting independent variables a closer look will be taken if these results differ per gender or age group. In the research of Seari et al (2014) it was shown that age was a strong predictor for privacy protection intention and that gender was a strong predictor for Privacy Protection Behavior (Saeri et al, 2014, pp. 361-362). Furthermore Youn & Hall showed that females are more likely to engage in Privacy Protection Behavior (Youn & Hall, 2008, pp. 1-3). Therefore, a closer look will be taken at how the independent variables influence Privacy Protection Behavior within different gender and age groups. A separate regression analysis was done for both male and female participants. First the descriptive statics for both males and females will be shown. After this a regression analysis will be done for both males and females with Privacy Protection Behavior as the dependent variable. After these differences between males and females will be discussed and after this preliminary conclusion will be made for the results of the regression analysis.

Table 16: Descriptive statistics used variables Males

	N	Min	Max	Mean	Std. Deviation
Attitude Towards Privacy Protection Behavior	40	0.33	0.86	0.565	0.116
Others expect me to be active on social media	40	0.28	1.00	0.750	0.202
Others expect me to be careful on social media	40	0.00	1.00	0.625	0.253
Others Are Careful on Social Media	40	0.00	0.92	0.302	0.190
Others are careful on social media	40	0.00	0.83	0.387	0.208
Perceived control over social media behavior	40	0.31	0.94	0.625	0.148
Degree of Privacy Protection Behavior	40	0.00	1.00	0.373	0.303
Valid N (listwise)	40				

Table 17: Descriptive statistics used variables Females

	N	Min	Max	Mean	Std. Deviation
Attitude Towards Privacy Protection Behavior	58	0.12	0.79	0.540	0.121
Others expect me to be active on social media	58	0.17	1.00	0.552	0.251
Others expect me to be careful on social media	58	0.17	1.00	0.668	0.234
Others Are Careful on Social Media	58	0.00	0.83	0.250	0.171
Others are careful on social media	58	0.00	0.83	0.346	0.173
Perceived control over social media behavior	58	0.11	0.94	0.553	0.197
Degree of Privacy Protection Behavior	58	0.00	1.00	0.271	0.236
Valid N (listwise)	58				

Table 18: Hierarchical Multiple Regression Analysis of Independent variables on Privacy Protection Behavior Coefficients Male /Female (**β**).

Predictor	Male	Female
Attitude Towards Privacy Protection Behavior	0.359**	0.605***
Others Expect you to be Active on Social Media	0.307**	-0.204
Others Expect you to be Careful on Social Media	-0.001	-0.233*
Others Are Careful on Social Media	0.228	0.406**
Others Are Careful on Social Media	-0.052	-0.088
Perceived Behavioral Control	-0.003	0.127
Constant	-0.577*	-0.285*
R2	.308**	.417***

Note: *p < .05, **p < .01, ***p < .001

When the sample was split between male and female participants this led to some interesting findings. Contrary to past findings male students scored higher for Privacy Protection Behavior than females. Furthermore, males also had higher mean scores for privacy for every independent variable with the exception of others expect me to be careful on social media. The resulting regression analysis also showed some major differences between males and females. The variable attitudes on Privacy Protection Behavior for instance was a way stronger predictor for females than for males. Furthermore, the relation between Others Expect you to be Active on Social Media and Privacy Protection Behavior was positive for males and negative for females. The relation between others expect me to be careful on social media and Privacy Protection Behavior was also almost non-existent for males and quite strong for females. For descriptive norms the direction of the relations seems to be quite similar although for females Others Are Careful on Social Media is both a stronger and a more significant predictor. Finally, perceived control had almost no effect on Privacy Protection Behavior for males while for females the relation was a lot stronger although it was not a significant relation for both males and females. This results in the following preliminary conclusions; males place a bigger importance on Privacy Protection Behavior than females according to this research. Attitudes towards privacy protection are by far the strongest predictor for females while this is a lot lower for males. Males however seem to place a bigger importance on whether important others say that they should or should not be active on social media while females seem to focus more on whether important others warn them about the dangers of social media. With males there seems to be a positive relation

between injunctive norms and Privacy Protection Behavior while with females a negative relation seems to be present. With descriptive norms a negative relation seems to be present for both males and females, but this relation is a lot stronger for females than for males. This would suggest that for this research males seem to behave more in line with injunctive norms while it seems that females act opposite to injunctive norms. This would also be in line with the findings that the negative relation between descriptive norms and Privacy Protection Behavior is stronger and more significant for females.

4.4 Desired Privacy Protection Behavior.

In order to answer the second part of my research question desired Privacy Protection Behavior was also measured in the questionnaire. For clarity the descriptive statistics of the two variables are shown below.

Table 19: Descriptive statistics Privacy Protection Behavior & Desired Privacy Protection Behavior.

	N	Min	Max	Mean	Std. Deviation
Degree of Privacy Protection Behavior	98	.00	1.00	.313	.269
Desire to improve Privacy Protection Behavior	98	.00	1.00	.564	.225
Valid N (listwise)	98				

It seems that there is still a significant difference between desired Privacy Protection Behavior and actual Privacy Protection Behavior. This difference is expected as actually protecting your privacy is harder than saying that you want to protect your privacy, and existing habits can be hard to change. However, this result shows that among the subjects, there is a desire to change their privacy behavior towards a better Privacy Protection Behavior in the future. Furthermore, if you want to influence the behavior of the subjects, this result shows that they would at least be somewhat responsive to it since the desire to change their behavior is already there. This suggests there is at least a slight privacy paradox present within my sample, however, to identify if this was present for both male and female participants a separate analysis was done.

Table 20: Descriptive statistics Privacy Protection Behavior & Desired Privacy Protection Behavior for males.

	N	Min	Max	Mean	Std. Deviation
Degree of Privacy Protection Behavior	40	0.00	1.00	0.5448	0.25360
Desire to improve Privacy Protection Behavior	40	0.00	1.00	0.3736	0.30298
Valid N (listwise)	40				

Table 21: Descriptive statistics Privacy Protection Behavior & Desired Privacy Protection Behavior for females.

	N	MMin	Max	Mean	Std. Deviation
Degree of Privacy Protection Behavior	58	0.13	1.00	0.576	0.203
Desire to improve Privacy Protection Behavior	58	0.00	1.00	0.271	0.235
Valid N (listwise)	58				

The descriptive statistics show that there is almost no difference in desire to improve Privacy Protection Behavior between males and females. However, because females scored lower on Privacy Protection Behavior the gap between desired privacy protection and Privacy Protection Behavior is a lot bigger. Thus, there seems to be a bigger demand from females to improve their Privacy Protection Behavior. Furthermore, this would suggest that for females there is a bigger gap between privacy concerns and current behavior.

5 Conclusion and discussion

In this final chapter, the sub research questions will be concluded, and the answers obtained will be used to support the conclusion of the main research questions. The practical implications of these conclusions will be discussed after this. Finally, the limitations of this research and the possibilities for future research will be discussed.

5.1 Conclusion

To answer the main research question: *What factors influence Privacy Protection Behavior on social media and does the subjects Privacy Protection Behavior match their desired Privacy Protection Behavior?* This research did a quantitative study with a sample of 98 students between the ages of 18 and 29. After the study the independent and dependent variables were created with an as high as possible internal reliability to increase the representativity of the regression analysis and preliminary conclusions were made which now will be used to conclude the research and answer all of the sub research questions and the main research question.

Sub research question 1: What is the influence of attitudes on social media and Privacy Protection Behavior on social media subjects' Privacy Protection Behavior? From the regression analysis, it became clear that attitudes on Privacy Protection Behavior were by far the strongest and most significant predictor for Privacy Protection Behavior. This is not necessarily surprising as past research has also shown that attitudes towards Privacy Protection Behavior are strongly linked with Privacy Protection Behavior (Yao & Linz, 2008, pp. 616). The hypothesis that Attitudes on Privacy Protection Behavior were positively linked with Privacy Protection Behavior was also confirmed. This leads to the conclusion that the research proved that attitudes towards Privacy Protection Behavior had a strong effect on actual Privacy Protection Behavior. This conclusion was also confirmed when the sample was split between both males and females. However, the independent variable attitudes towards privacy protection was a lot stronger for females than for males. Thus, according to the research attitudes on Privacy Protection Behavior had a stronger influence on females than on males.

Sub research question 2: What is the influence of injunctive norms on Privacy Protection Behavior on social media subjects' Privacy Protection Behavior? The variable injunctive norms turned out to be heavily related to items centered around being careful on social networking sites. This seems to be a rather logical relation as general norms usually focus on socially desirable behavior, and protecting your digital privacy is usually seen as a virtue by society. This resulted in the substantial and significant variable Others Expect me to be careful on Social Media. Others Expect me to be careful on Social Media was the third strongest predictor for Privacy Protection Behavior, but the relationship it had with Privacy Protection Behavior was unexpected. The analysis showed that while the mean score for Others Expect me to be Careful was towards more privacy; then it had a negative score concerning Privacy Protection Behavior, which is rather odd. The hypothesis that a positive relationship is present between the two seems to be incorrect since a negative relation was present. A possible explanation for this finding could be that when significant others argue that you should be

more careful on social networking sites, this could be considered as nagging and it could result in subject behaving oppositely. Secondly, it could be the case that the items for Others Expect me to be Careful on Social Media were unclear, and this resulted in conflicting answers from the subjects. It is important to note that the variable was wholly made up of items that were reverse scored, which could be the source of the confusion. To further explore the results an analysis was done that looked at a regression analysis for males and females separate. Here it was found that males and females had completely different regression scores for both Others Expect you to be Active on Social Media and Others Expect you to be Careful on Social Media. While males had a strong and significant relation for Others Expect you to be Active on Social Media females did have a strong score, however there was a negative and non-significant relation for Others Expect you to be Active on Social Media. When looking at the independent variable Others Expect you to be Careful on Social Media the scores for males and females once again differ greatly. For males, the relation was almost zero while for females there was a strong and significant negative relation between Others Expect you to be Careful on Social Media and Privacy Protection Behavior and very similar to the relation in the general regression analysis. This led to the conclusion that while for this research it was proven that injunctive norms had a significant effect on Privacy Protection Behavior via the dimension Others Expect you to be Active on Social Media for males and the dimension Others Expect me to be Careful on Social Media for females. The validity of the relation should be explored further to see if the relation that was found in the research is correct. Further research should also be conducted to see if males and females differ this much regarding injunctive norms in relation to Privacy Protection Behavior,

Sub research question 3: What is the influence of descriptive norms on Privacy Protection Behavior on social media subjects' Privacy Protection Behavior? The independent variable descriptive turned out to be heavily related with items centered around Others Are Careful on Social Media. This is a logical relation since descriptive norms focus on actual behavior by significant others, and social media activity is usually more visible than being careful on social media. However, like with the independent variable injunctive norms, the hypothesis that there is a positive relationship between descriptive norms and Privacy Protection Behavior seemed to be incorrect. As a low mean score for the variable Others is Active on Social Media resulted in a positive coefficient for Privacy Protection Behavior. This result suggests that there is a negative relation between the independent variable descriptive norms and Privacy Protection Behavior. In practice, it would mean that when a subject sees significant others being active on social media sites, it would result in a subject improving their Privacy Protection Behavior. Thus, if a subject sees how not to behave on Social Networking Sites, the subject will want to improve their Privacy Protection Behavior. While this does make sense to a certain degree, this conclusion would also suggest that peer pressure has the reverse effect on the topic of Privacy Protection Behavior. This leads to the conclusion that while descriptive norms were

the second strongest independent variable for influencing Privacy Protection Behavior in the general regression analysis the validity of the variable seems to be questionable at least. Further analysis was done to see if this could have been caused by differences between male and female subjects. This analysis showed that while for females the relation was a lot stronger and more significant the overall relation was the same for both males and females and thus this did not change the conclusion. Further research into the topic would need to be done to clarify whether the relation between descriptive norms and Privacy Protection Behavior is correct.

Sub research question 4: Did the split of the variable subjective norms into the variables injunctive norms and descriptive norms result in stronger and more significant independent variables for this research? The split of the independent variable subjective norms had the desired effect of giving two stronger are more significant independent variables. The effect, however, was not as strong as expected. This is possible because the items in the questionnaire had two different dimensions for both injunctive norms and descriptive norms (Active / Careful). Each category correlated with either injunctive or descriptive norms. It is likely that because of the split between active and careful was maintained for subjective norms that the results were based mainly on the strong parts of both injunctive norms and descriptive norms. A more definite conclusion can likely be obtained when these dimensions are correctly assigned to either injunctive or descriptive norms, and subjective norms are separately tested. For example, half of the participants get a questionnaire where injunctive and descriptive norms are separate, and the other half get a questionnaire where they are together within the variable subjective norms. For this research, the split led to stronger and more significant results and is more likely to show the actual influence of injunctive norms and descriptive norms on Privacy Protection Behavior.

Sub research question 5: What is the influence of perceived control over Privacy Protection Behavior on social media subjects' Privacy Protection Behavior? The analysis showed that while in past researches, there was a significant and strong relation present between perceived control over behavior and Privacy Protection Behavior, this was not the case for this research. A reason for this could be that Perceived Behavioral Control had a low score for internal reliability. This could have resulted in Perceived Behavioral Control being a weak variable. However, it could also be the case that for the subjects Perceived Behavioral Control did not play a part in determining their Privacy Protection Behavior. To see if gender played a role in this weak result a regression analysis with the regression males and females separately was done. This analysis showed that while the relation between perceived control and Privacy Protection Behavior was a bit stronger than in the general while that for males was almost zero. The relation, however, still was one of the weakest predictors for Privacy Protection Behavior and both relations were not significant. Therefore, this did not lead to new insights. Research with a variable for Perceived Behavioral Control with a higher internal

reliability score could clarify whether Perceived Behavioral Control does not play an essential role in Privacy Protection Behavior. This all leads to the conclusion that for this research, the influence of perceived control was rather low for Privacy Protection Behavior.

Research question: What factors influence Privacy Protection Behavior on social media and does the subjects Privacy Protection Behavior match their desired privacy protection? Based on the general regression analysis, the independent variables Attitude on Privacy Protection Behavior, Injunctive norms, and descriptive norms are the main influences on Privacy Protection Behavior within the context of this research. This is in line with the results of Yao & Linz (Yao & Linz, 2008, p. 616). Although the big difference is that their research was on the adoption of privacy protection measures while mine was focused on Privacy Protection Behavior. This research also focused on the direct relation between independent variables on Privacy Protection Behavior and did not include behavioral intention. Research that did include the direct link between Privacy Protection Behavior and the independent variables also did not find strong or significant relations. For example, in the research of Seari et al. (2014) the research did find significant relations between the independent variables Attitudes towards privacy behavior, injunctive norms and descriptive norms and the dependent variable Privacy Protection Behavior, which was likely the case because the research also included other variables that ended up being better predictors for Privacy Protection Behavior for that research. This research chose to not use those values mainly because age or gender while being strong predictors are not that interesting when looking at what influences behavior as they are tough to influence.

Furthermore, the research revealed that both injunctive norms and descriptive norms strongly influence Privacy Protection Behavior. However, the results obtained for injunctive norms and descriptive norms do seem somewhat illogical and may require further research to prove if my results were valid. Finally, the analysis showed that perceived control over social media had neither a strong nor a significant relation to Privacy Protection Behavior. This result is somewhat surprising since the Theory of Planned behavior itself states that perceived control has a direct relation to behavior. A possible explanation for this could be that perceived control on Social Networking Site tends to be slightly habitual (Saeri et al., 2014, pp. 362-363), subjects might still have a high perceived control score because they felt this when they last changed their privacy settings. They might not consider new options to improve their Privacy Protection Behavior because they are happy with what they did in the past even though new possibilities have arisen. Further research will have to be done to explore this topic, as other research has found a significant relationship between Perceived Control and Privacy Protection Behavior (Yao & Linz, 2008, pp. 616-617).

Some of these findings change however when separate regression analyses are done for male and female subjects. It appears that for females all of the relations which were just listed were present

and also a lot stronger than in the general regression analysis. For males all relations were a lot weaker and the relation between the independent variable Others Expect you to be Active on Social Media and Privacy Protection Behavior was a positive strong and significant relation for males while it was a negative weak relation with Privacy Protection Behavior for females. This showed that while most of the relation were similar for both males and females there was a major difference in the strength of the relations between the independent variables and privacy protection behavior. Furthermore, for the independent variable Others Expect you to be Active on Social Media they even had opposite relations. This also showed that a bias towards females was present in the regression analysis as there was an overrepresentation of females in the sample.

To answer the second part of the research question, *do the subjects Privacy Protection Behavior match their desired privacy protection?* Items regarding desired behavior were added to the questionnaire. In the analysis, it was shown that there is a significant difference between Privacy Protection Behavior and desired Privacy Protection Behavior. This shows that there is a desire for more Privacy Protection Behavior amongst students, which leaves room for policymakers to try and help to improve Privacy Protection Behavior further as there is a mandate for this. It also appears that this gap between Desired Behavior and current Privacy Protection Behavior was a lot bigger for females. This can mainly be explained by the difference in Privacy Protection behavior, while both groups scored similar for Desired Privacy Protection Behavior females had a significantly lower score for Privacy Protection behavior. This shows that there is a Desire for better Privacy Protection Behavior from both genders but that a focus on females might be more necessary as the gap between desired and current behavior is a lot bigger.

Furthermore, this also suggests that there is a slight privacy paradox present in my sample. This, however, can also be a result of the framework that was used for this research. If a framework is adopted, that resembles that of Dieplin & Trente (2015) a better conclusion on this can be given since their framework was explicitly created to measure a privacy paradox using the Theory of Planned Behavior (Diepin & Trepte, 2015, p. 295).

5.2 Practical applications Limitations & Future research

The second part of my research question revealed that there is a desire to better Privacy Protection Behavior among subjects. Furthermore, the research question shows that three independent factors influenced Privacy Protection Behavior in the research. However, if one wants to actually influence Privacy Protection Behavior it would work best when this done via a focus on changing attitudes towards Privacy Protection Behavior. This is because the results for injunctive norms and descriptive norms can be considered questionable and should be studied further in depth before definite

conclusions can be given. Furthermore, both injunctive norms and descriptive norms are tough to change. Since both of these variables rely on the behavior and attitudes of many, it would require many people to change their behavior or Attitude Towards Privacy Protection Behavior. While the variables can serve as good predictors of Privacy Protection Behavior, it is also slightly dependent on attitudes towards Privacy Protection Behavior and Privacy Protection Behavior of significant others to influence an individual. It is slightly backward to try to influence behavior through descriptive norms because the reality is that the privacy protection of significant others is what forms descriptive norms. This leaves attitudes towards privacy protection as the primary variable to focus on when you want to make use of this research. When someone wants to influence attitudes towards Privacy Protection Behavior, it is not merely enough to say that Privacy Protection Behavior is okay. This research suggests that the positives of Social Networking Site also influence a subject's attitude on Privacy Protection Behavior thus making people more aware of the effects that actions on Social Networking Site have could be a feasible strategy. For example, you might be less likely to share the fun vacation pictures if you are made aware that this tells burglars I am not at home, please break-in. Thus, the suggestion would be to better inform users of the possible effects of their actions on Social Networking Sites, with the main focus on providing information about the data that is collected on them and of the adverse effects that this data collection could have on them. This strategy would result in a change in attitudes in two distinct ways since it would lower the attitude towards the positives of Social Networking Sites if it is revealed that these positives are not without their downsides. Furthermore, when informed of the data that is being collected on them users' attitude on Privacy Protection Behavior could change when they are shown that Privacy Protection Behavior could be more vital for them than they first thought. This has the added bonus that this focus on Attitudes towards Privacy Protection Behavior would have a stronger influence on females. This could benefit them as this study showed that the gap between Desired Privacy Protection Behavior and current Privacy Protection Behavior is larger than for their male counterparts.

However, this research does have limitations. As the study was done on students from a select area, it is unknown if these findings apply to people from different ages, education levels, or regions. Furthermore, the sample obtained for the research was a convenience sample. A sample from all students in the Netherlands or even the University of Twente could result in different findings because the makeup of the sample could change significantly by including more subjects from different study programs for example. If one wants to test the results obtained in future research, I would suggest changing one of these factors so, for instance, the age group of the subjects. However, it would be advised not to change too many of these factors since this could make it hard to draw valid conclusions. If many factors are changed, and this would result in research in which the results differ a lot from this research, it would be hard to see which of the changes caused the change. For example, if

one changed the age and education level of the sample, differences are harder to account for since the samples have changed in multiple ways.

Further research into the topic could clarify whether the relations between injunctive norms and Privacy Protection Behavior and descriptive norms and Privacy Protection Behavior are correct or if mistakes were made during this research. This could be done by limiting the items on the questionnaire to one dimension per variable. When injunctive norms are linked just to being careful on social media and descriptive norms just to being active on social media, this could reduce possible confusion of participants and could prove or disprove the relations that were found in the current research. Furthermore, when taking this approach, the effect of splitting subjective norms into injunctive norms and descriptive norms can also be researched better, and the conclusion of this research could be better supported or disproven. The role of Perceived Behavioral Control could also be revisited in future research. Because this research seems to contradict results from existing research, a more definite answer could be given when this is researched further. Finally, a second look should be taken at the differences between males and females for Privacy Protection Behavior. This because this research conflicts with findings of past research and shows that there is a large difference in the relations of the independent variables with Privacy Protection Behavior for males and females.

6. References

Ajzen, I. (1991). The theory of planned behavior. Organizational behavior and human decision processes, 50(2), 179-211.

Ajzen, I. (2006). Constructing a theory of planned behavior questionnaire.

Athey, S., Catalini, C., & Tucker, C. (2017). The digital privacy paradox: Small money, small costs, small talk (No. w23488). National Bureau of Economic Research.

Baker, R. K., & White, K. M. (2010). Predicting adolescents' use of social networking sites from an extended theory of planned behaviour perspective. Computers in Human Behavior, 26(6), 1591-1597.

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. First Monday, 11(9).

Chang, A. (2018). The Facebook and Cambridge Analytica Scandal, Explained with a Simple Diagram. Vox, March 23.

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. European Journal of Social Psychology, 45(3), 285-297.

Facebook/ads/about Obtained on 19-10-2018 from: https://www.facebook.com/ads/about/?entry_product=ad_preferences

Fitzpatrick Michael, 2006, Section 254(h)(7) of HR5319 IH.

Kim, E., Lee, J. A., Sung, Y., & Choi, S. M. (2016). Predicting selfie-posting behavior on social networking sites: An extension of theory of planned behavior. Computers in Human Behavior, 62, 116-123.

Lenhart, A., Purcell, K., Smith, A., & Zickuhr, K. (2010). Social Media & Mobile Internet Use among Teens and Young Adults. Millennials. Pew internet & American life project.

Manning, M. (2009). The effects of subjective norms on behaviour in the theory of planned behaviour: A meta-analysis. British journal of social psychology, 48(4), 649-705.

Propkom, A. (2018). Cambridge Analytica shutting down: the firm's many scandals, explained Vox, May 2.

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.

Wisniewski, P., Knijnenburg, B. P., & Lipford, H. R. (2014, July). Profiling Facebook user's privacy behaviors. In SOUPS2014 Workshop on Privacy Personas and Segmentation.

Yao, M. Z., & Linz, D. G. (2008). Predicting self-protections of online privacy. CyberPsychology & Behavior, 11(5), 615-617.

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

7. Appendix

7.1 Survey Social media usage

Thank you for your willingness to participate in this survey. The survey is about the use of profile based social media which is the topic of my bachelor thesis. Profile based social media can be seen as social media like Facebook, Twitter, Instagram, or Linked-in since those all have a visible personal profile for each user. The survey is completely anonymous, which means that the collected data will not be used to identify you, and that my thesis will not report on any individual answers.

To participate in this survey, you will have to be over 18 years of age, by continuing you will state that you meet this age criterion. If you feel uncomfortable answering any questions and want to stop your participation, you can do so at any point. If you have any questions about the survey or my research, you can send me an email at j.delfgou@student.utwente.nl.

- Items used in the analysis

Opinions on social media

This section will ask questions about your opinions on different aspects of social media. This will be done in two parts, the first part is about your opinion on sharing personal information on social media, the second part will be about the possibilities that you think social media has to offer.

Opinions on social media

To start, can you indicate to what extent you agree or disagree with the following statements about sharing personal information on social media.

1. **I like sharing all my personal experiences online.** * *Mark only one oval.*

Agree 1 2 3 4 5 6 7 Disagree

2. **I like posting photographs of me and my friends on social media.** * *Mark only one oval.*

Agree 1 2 3 4 5 6 7 Disagree

3. **I like to express my opinions via social media.** * *Mark only one oval.*

Agree 1 2 3 4 5 6 7 Disagree

4. **Digital privacy is important to me.** * *Mark only one oval.*

Agree 1 2 3 4 5 6 7 Disagree

5 **I want to have control over who has access to my personal data.** * *Mark only one oval.*

Agree 1 2 3 4 5 6 7 Disagree

Possibilities offered by Social media

The following statements are about possibilities offered by social media. Please indicate to what extent you like or dislike these possibilities.

6. **Social media allows you to see what your friends are doing.** * *Mark only one oval.*

Like 1 2 3 4 5 6 7 Dislike

7. **Social media helps you to keep in contact with people who are far away.** * *Mark only one oval.*

Like 1 2 3 4 5 6 7 Dislike

8. **Social media is used by advertisers to send you targeted messages.** * *Mark only one oval.*

Like 1 2 3 4 5 6 7 Dislike

9. **Social media is used by political parties to send you targeted messages.** * *Mark only one oval.*

Like 1 2 3 4 5 6 7 Dislike

10. **Social media helps you to keep up with current events.** * *Mark only one oval.*

Like 1 2 3 4 5 6 7 Dislike

11 **Social media informs you of upcoming events for example concerts or football matches you may be interested in.** * *Mark only one oval.*

Like 1 2 3 4 5 6 7 Dislike

Important others on social media

This section is focused on the expectations that important others have of your social media usage and what they do on social media themselves. Important others can be seen as people close to you, like friends, fellow students, parents, teachers, employers.

What do important others expect of me on social media?

Please indicate to what extent important others like your friends, fellow students, parents, teachers, and employers expect the following things from you when it comes to your online behavior.

12. **Others expect me to be active on social media.** * *Mark only one oval.*

They expect this of me 1 2 3 4 5 6 7 They don't expect this of me

13. **Others expect me to be careful in what I share on social media.** * *Mark only one oval.*

They expect this of me 1 2 3 4 5 6 7 They don't expect this of me

14. **Others expect me to be careful who I share my personal data with.** * *Mark only one oval.*

They expect this of me 1 2 3 4 5 6 7 They don't expect this of me

15. **Others expect me to like their posts.** * *Mark only one oval.*

They expect this of me 1 2 3 4 5 6 7 They don't expect this of me

16 **Others expect me to post about my interests.** * *Mark only one oval.*

They expect this of me 1 2 3 4 5 6 7 They don't expect this of me

17. **Others expect me to express my political opinions online.** *Mark only one oval.*

They expect this of me 1 2 3 4 5 6 7 They don't expect this of me

What do important others do on social media?

Please indicate to what extent these important others like friends, fellow students, parents, teachers, and employers themselves behave on social media in the following ways:

18. **They are active on social media.** * *Mark only one oval.*

They Are 1 2 3 4 5 6 7 They are not

19. **They are careful with what they share on social media.** * *Mark only one oval.*

They Are 1 2 3 4 5 6 7 They are not

20. **They are careful with whom they share their personal data.** * *Mark only one oval.*

They Are 1 2 3 4 5 6 7 They are not

21. **They often like posts.** * *Mark only one oval.*

They do 1 2 3 4 5 6 7 They do not

22 **They often post about their interests.** *Mark only one oval.*

They do 1 2 3 4 5 6 7 They do not

23 **They often express their political opinions online.** *Mark only one oval.*

They are 1 2 3 4 5 6 7 They are not

Control over social media

This section is about how much control you feel you have over different aspects of social media. Please answer how much you agree/disagree with the following statements.

24. **I experience a constant need to be online.** * *Mark only one oval.*

Agree 1 2 3 4 5 6 7 Disagree

25. **It is easy for me to put my phone away for several hours.** * *Mark only one oval.*

Agree 1 2 3 4 5 6 7 Disagree

26. **I know how to reset my online profile.** * *Mark only one oval.*

Agree 1 2 3 4 5 6 7 Disagree

27. **I can control the amount of data gathered about me.** * *Mark only one oval.*

Agree 1 2 3 4 5 6 7 Disagree

28. **I know how to set who is allowed to see what on my social media profile.** * *Mark only one oval.*

Agree 1 2 3 4 5 6 7 Disagree

29 **I have control over what social media websites do with my personal data.** * *Mark only one oval.*

Agree 1 2 3 4 5 6 7 Disagree

30 **I know how to protect my digital privacy.** *Mark only one oval.*

Agree 1 2 3 4 5 6 7 Disagree

Social media behavior

Please indicate to what extent you agree with the following statements about social media platforms you are currently using/have used:

31. **I try to keep my online profile(s) up to date and complete (relationship status, date of birth, current job/education, former high school).** *Mark only one oval.*

Agree 1 2 3 4 5 6 7 Disagree

32. **I have read the terms and services of my social media platform(s).** *Mark only one oval.*

Agree 1 2 3 4 5 6 7 Disagree

33. **I frequently like pages that align with my personal interests.** * *Mark only one oval.*

Agree 1 2 3 4 5 6 7 Disagree

34. **I frequently like posts by others.** * *Mark only one oval.*

Agree 1 2 3 4 5 6 7 Disagree

35. **I participate in online personality tests.** *Mark only one oval.*

Agree 1 2 3 4 5 6 7 Disagree

36 **I have changed my privacy settings to my liking.** *Mark only one oval.*

Agree 1 2 3 4 5 6 7 Disagree

37 **I use my social media account to access websites and other applications, such as games.**

Mark only one oval.

Agree 1 2 3 4 5 6 7 Disagree

38. **I have downloaded social media apps to my phone.** *
Mark only one oval.

Agree 1 2 3 4 5 6 7 Disagree

Future social media intentions

Please indicate to what extent you agree or disagree with the following statements, if you were to set up a new social media profile:

39. **I intend to keep my online profile up to date and complete (relationship status, date of birth, current job/education, former high school).** *Mark only one oval.*

Agree 1 2 3 4 5 6 7 Disagree

40. **I intend to read the terms and services of the social media platforms I use.**
Mark only one oval.

Agree 1 2 3 4 5 6 7 Disagree

41. **I intend to be more careful in expressing my opinions online.** * *Mark only one oval.*

Agree 1 2 3 4 5 6 7 Disagree

42. **I intend to set my privacy settings to my liking.** *Mark only one oval.*

Agree 1 2 3 4 5 6 7 Disagree

43 **I intend to post fewer messages on social media.** * *Mark only one oval.*

Agree 1 2 3 4 5 6 7 Disagree

44 **I intend to reduce the amount of information that is collected about me.** * *Mark only one oval.*

Agree 1 2 3 4 5 6 7 Disagree

45. **I intend to use social media less than I am doing now.** *

Mark only one oval.

Agree 1 2 3 4 5 6 7 Disagree

General information

Finally, I would like you to fill in some general information about yourself. This information will be used to get a better understanding of my sample.

46. **What is your age?**

47. **Gender**

Mark only one oval.

Male

Female

48. **What kind of study program are you currently enrolled in?**

Mark only one oval.

Technical studies

Social studies

ICT studies Medical studies

Other:

49. **Could you indicate how much time you spend on social media per week on average?** *Mark only one oval.*

0-5 Hours

5-10 Hours

10-20 Hours

20-40 Hours

40+ Hours