

August 7<sup>th</sup>, 2017

University of Twente  
European Public Administration  
Moritz Frederik Vor dem Berge (s1741594)  
[m.f.vordemberge@utwente.nl](mailto:m.f.vordemberge@utwente.nl)  
Module: 201500162 - Bachelor Thesis  
Bachelor Circle No. 1: Digital Privacy

## **Bachelor Thesis**

### **Digital Privacy**

*Behaviour and anxieties of a young digital generation*

Final Version: August 7<sup>th</sup> 2017

1<sup>st</sup> Supervisor: Dr. Jörgen Svensson

2<sup>nd</sup> Supervisor: Dr. Giedo Jansen

### **Abstract**

The topic of digital privacy and the question whether it will be persistent in times of increasing digitalization occupied many areas of science. Especially teenagers face difficulties dealing with their privacy and finding a balance between the benefits of SNSs (Social Networks) and self-disclosure. However, the correlation and influence of technical proficiency on the privacy behaviour of young people remains rather unexplained which is why this study targets that very subject. By asking 340 German secondary school pupils (aged 10-19) about their skills, concerns and digital behaviour, correlations between technical competencies, privacy concerns and digital privacy behaviour were uncovered. The results indicate that the skills of young people lead them to behave less carefully while using the Internet. Most of the findings support some previous studies but on the other hand contradict some others as well. For example, the societies' common sense that the existence of better personal digital skills raise the awareness and thus lead to a cautious online behaviour seems to be false. Furthermore the study comes up with some recommendations for German teaching personnel concerning their future strategies in our digital world.

*Keywords: online privacy behaviour, online privacy concerns, technical proficiency, young people, SNS*

**Table of Contents**

	Page
Part 1. Introduction .....	2
Part 2. Theory .....	5
2.1 What is Digital Privacy? .....	5
2.2 What is Privacy Behaviour? .....	7
2.3 What are Privacy Concerns? .....	9
2.4 What is Technical Proficiency? .....	11
2.5 Causal Diagram / Hypotheses .....	13
Part 3. Methodology and Operationalisation .....	15
3.1 Description of Survey and Data Set Overview .....	15
3.2 How is Technical Proficiency Measured? .....	16
3.3 How is Privacy Concerns Measured? .....	17
3.4 How is Privacy Behaviour Measured? .....	17
Part 4. Analysis .....	19
4.1 Descriptive Analysis .....	19
4.2 Correlations .....	20
4.3 Path Diagram based on the regression model .....	21
4.4 Analysis of the Hypotheses .....	22
4.4.1 Analysis of the main Research Question .....	22
4.4.2 Analysis Sub-Research Question No. 1 .....	24
4.4.3 Analysis Sub-Research Question No. 2 .....	25
4.4.4 Analysis Sub-Research Question No. 3 .....	27
Part 5. Conclusion and Discussion .....	30
5.1 Limitations .....	32
5.2 Policy and Strategy Recommendations .....	32
6. Literature/References .....	34
7. Appendices .....	36
8. Honesty Declaration .....	39

## **Part 1. Introduction**

Thinking about the omnipresence of the Internet nowadays there are aspects considered as both positive and negative. It is not unusual to share pictures of our latest holidays online. We communicate via E-mail and find partners with the help of dating applications or study via online courses (Acquisti, 2015). We associate these behavioural patterns especially with young adults or teenagers. The flip side of all these benefits to our daily life is that we reveal intimate information to people we know and do not know as well as to companies, governments etc. in an uncontrollable manner. While we are able to disguise private information in the real life by physical restrictions we often fail to do the same with digital information. Finding a balance between beneficial online services and the share of private data needed for using these very services poses one of today's greatest challenges for *SNS* (Social Networking Service) users (Acquisti, 2015; Sheehan, 2002; Youn, 2009). Hence, the term digital privacy which is prior to this thesis paper has its relevance for a good reason.

In this paper I will examine whether technical proficiency of young people at the age of 10 to 19 has an influence on their awareness or solicitousness towards online privacy issues and thus their online-behaviour. The study will focus on pupils of German secondary schools. Therefore I will conduct a cross-sectional study to estimate the influence of technical proficiency (or digital skills) on their online privacy behaviour. The study will be based on a survey conducted together with my bachelor-circle colleague Jeff Harrower (s1614681), who will focus on social communicational aspects related to digital privacy concerns and behaviour. By combining our surveys we are able to reach far more participants and thus make it more representative.

As Frees (2015) shows in his study the internet usage among young people (14-19 years old) in Germany has significantly increased within the last years. While in 2013 roughly 87% of this age group made use of the Internet, in 2015 about 94% of this age group with internet-access used the Internet on a daily basis. Hence, the people who are subject of this study can be seen as the most frequent users of this medium and might depict a generation of digital natives

(Helsper & Eynon, 2010; Vodanovich, 2015). Since the *NSA Spying Scandal* and numerous cases of cyber attacks on databases full of intimate information digital privacy became an issue for everyone who uses the Internet - not only for the technical elites. The misuse of private digital content is not always performed by (in a certain degree anonymous) entities such as governments or companies - the term 'Cyber bullying' has raised a lot of attention within the last years and essentially threatens young adults and pupils (Ybarra, 2012). However, there might be differences in behaviour between technically proficient and technically less versed individuals concerning their privacy concerns and online behaviour as Buchanan (2007) proposed in his study. Digital or online privacy has been discussed extensively in a vast number of scientific journals as well as in the media in general.

After developing a theoretical framework on which my hypotheses are based on I intend to conceptualise the central variables (Privacy Behaviour, Privacy Concerns, Technical Proficiency) to show how I applied them in the questionnaire. In the central section, the analysis (Part 4.), the gathered data will be used to answer the central research question (*To what extent does technical proficiency of young people (ages 10-19) in Germany have an influence on their online privacy behaviour?*) as well as further sub-questions. Owing to the fact that anxieties (concerns) are somewhat connected to the way people live their digital life (Chen, Beaudoin, & Hong, 2017) one could furthermore pose the question: *With regard to their online behaviour in what way do online privacy concerns have an influence on young people in Germany?* Some scholars (Moscardelli & Divine, 2007) discuss potential differences in online concerns and behaviour by virtue of gender. Thus one sub-research question could ask for differences between boys and girls: *In how far do the level of technical proficiency and the online behaviour differ between boys and girls?* This question has to be discussed in the (regression) analysis and might be substantiated by the results of it. As my study comprises a wide age span an additional aim of this paper could be to distinguish the effect of age on young people's online privacy behaviour. Previous studies have investigated teenager's privacy concerns (ages 14-18). The results indicated that younger adolescents (11-13) are very much unsought with regard to

their online behaviour (Youn, 2009). “*In how far, does age have an influence on technical proficiency and hence the online privacy behaviour of young people in Germany?* “ could thus pose an interesting sub-research question.

What makes this research unique is that it focuses on pupils at a very young age. This could furthermore lead to new findings concerning the necessity of specific education and reasonable usage of digital (or online) tools within education facilities. Since smart phones or social media are omnipresent in the present young generation (Frees, 2015) the necessity of a solution that combines old and new societal structures is not discussible. In addition to that the conducted research could bring up new findings about the importance of technical proficiency while talking about online privacy issues. The existing research papers deal with potential correlations between digital literacy and online behaviour (Baruh, 2017; boyd, 2014; Park, 2013) rather than actual technical skills. It might be important to implement school subjects dealing with these issues to ensure the wellbeing of young adults and prepare them for the requirements of a digital age (DeVries, 2003). The following sections will explore that. In order to do so I set out to answer the following questions in this research:

1. To what extent does technical proficiency of young people (ages 10-19) in Germany have an influence on their online privacy behaviour?
2. In what way do online privacy concerns have an influence on young people in Germany with regard to their online behaviour?
3. In how far do the level of technical proficiency and the online behaviour differ between boys and girls?
4. In how far does age have an influence on technical proficiency and hence the online privacy behaviour of young people in Germany?

## **Part 2. Theory**

There are plenty of studies dealing with digital privacy and the question of what influences the online privacy behaviour of young individuals. This section will try to review some of the most relevant and recent literature (due to its topicality) in order to set a theoretical framework for the remainder of this thesis. The definitions and hypotheses given in this part will be then conceptualized in Part 3.

### **2.1 What is Digital Privacy?**

The overarching term of this paper, *privacy*, is quite complex and difficult to define briefly. Due to the fact that *privacy* is multi-dimensional it is essential to assign it to one specific aspect. This section can be seen as an introduction to the theory that has evolved around this topic so far including some literature besides digital privacy with regard to SNS, as well. The following pages will then specify and focus on digital privacy in SNS.

A very broad definition is delivered by Warren and Brandeis (1890). According to them the right to privacy in a legal context can be associated with “a right to be let alone” (p. 193). Due to the fact that law as well as technology and thus the society has changed drastically over the last century and especially in the last decades we can consider their approaches as very much outworn. However, their basic assumptions about what constitutes privacy can be applied to today’s society and its values. While Warren and Brandeis claimed a right to be let alone the demands of our (digital) generation go way further. In times of massive data preservation “the right to be forgotten” (Newman, 2015) is much more of an issue on the agenda of many digital natives. But the Internet does not forget and our online behaviour can be traced back to times which we do not feel confident to show e.g. our current employer. Photos, court records, and letters that used to get lost in file cabinets are neatly organised and accessible from our laptops. A childhood foible can haunt someone for a lifetime (p. 507).

In times when Internet has not been essential in everyone's daily life it was easy to close or hide private documents, photos or any other intimate items in boxes or even safes.

But not only SNS-users frequently deal with digital privacy issues - in the last four decades the health care system of the U.S. for example has undergone revolutionary changes driven by advances in IT and legislation (Appari, 2010). A patient's medical record is then shared with payer organisations such as private insurances or used to manage operations and generally improve service quality (p. 281). And even though the intensified use of technology is beneficial for state (the U.S. makes an estimated saving of \$81B per year) and patient (p. 280) the rise of this improvement of healthcare information systems has its downsides as well. Concerns accrued that for their own benefits external and (system-) internal individuals could misuse health data. Based upon this example one can say that digitalisation has found its way into almost all of our areas of life. It furthermore illustrates that *digital privacy* always constitutes *concerns* of losing it. But is the sheer existence of *privacy concerns* influencing the behaviour of people using the health care system and, even more interesting, SNS-users? Having set up this question it is important to include the terminology of *privacy concerns* whenever the need occurs to analyse why people give up or protect their own digital privacy. Since this is the core part of this thesis *privacy concerns* ought to be defined too (see Part 2.3 - What are Privacy Concerns?). I assume that concerns indeed have an influence on the online behaviour of young people:

**H6: *The more concerned someone is in terms of privacy the more careful the/she behaves online.***

Privacy in general underwent an immense shift from analogue to digital. The term itself became multidimensional which impedes a clear definition. This research aims on understanding young individuals' attitude towards online privacy on SNS and what constitutes this attitude which allows curtailing the definition. Livingstone (2008) identified a paradox between the privacy concerns of young adults on the one hand and their willingness to disclose personal

information on the other hand. This paradox is resolved by a definition of digital privacy ‘not tied to the disclosure of certain types of information but instead a definition centred on having control over who knows what about you.’ Stein and Sinha (2002) rendered the term more precisely as ‘the rights of individuals to enjoy autonomy, to be left alone, and to determine whether and how information about one’s self is revealed to others’ (p.414).

With these definitions as a basis the following sub-items will examine the existing literature about young people’s behaviour when it comes to their online privacy, their online privacy concerns and potential influences of technical proficiency on these aspects.

## **2.2 What is Privacy Behaviour?**

The *reasoned action approach* by Fishbein and Ajzen (2011) is used as theoretical foundation to explain the (privacy) behaviour of young people in Germany. The authors themselves stated that the model could be applied to any other domain in which behaviour is subject to an analysis as well (p. 27). Hence, I will use it as a very basic approach for this study. They developed several models that allow predictions for the behaviour and deliver strategies to influence or change this very behaviour. In order to apply this model to certain behaviour the behaviour itself has to be investigated and operationalised in the first place. For this paper the online privacy behaviour of young people (10 - 19) in Germany is the subject of interest. It is investigated with the help of a 38-item survey (See Part 3.1 - Description of Survey and Data Set Overview) and operationalised with adopted as well as self-made models.

In terms of behavioural determinants Fishbein and Ajzen assume that human social behaviour follows reasonably and often spontaneously the information or beliefs people possess about the behaviour under consideration (p. 20) which in this case is online privacy behaviour. The authors furthermore deliver an explanation for the different sources which *beliefs* can derive from. This proves quite interesting and could officiate as a fundament for the remainder of this paper. For them personal experiences, formal educations as well as media have an influence on someone’s beliefs and individual differences (e.g.

demographic characteristics or personality) (p. 20). From this the first gender- and age-related hypotheses can be derived:

**H2b: *Girls behave more careful when it comes to online privacy.***

**H3b: *The older someone is the more time he/she spends online.***

These are not prior to my research which is why I additionally marked both of them with the abbreviation “b”. The hypotheses prior to the ones above include the variable of technical proficiency and will be part of Part 2.4.

In addition to the sources Fishbein and Ajzen distinguish between three different sorts of beliefs: 1. *Behavioural beliefs* - People hold beliefs about positive or negative consequences associated with certain behaviour. 2. *Normative beliefs* – People’s behaviour is influenced by their social surroundings and their attitudes towards behavioural patterns. 3. *Control beliefs* - for this paper this sort of belief might be the most valuable one. The authors argue *that people form beliefs about personal and environmental factors that can help or impede their attempts to carry out the behaviour* (p. 21) and will then result in a perceived behavioural control. These three kinds of beliefs form the *intentions* that determine whether the behaviour will be performed or not. The stronger the intention the higher the probability that the behaviour will be adopted. Besides the environmental factors which are subject to the research of my fellow colleague Jeffrey Harrower), actual skills and abilities have an influence on control beliefs and respectively the perceived behavioural control. Fishbein and Ajzen, however, assume that *actual control* (such as skills, abilities and environmental factors) is not only affecting the perceived behavioural control but the *intention* that leads to certain behaviours, too. A lack of skills and abilities can prevent people from acting in favour of their intentions which has a major influence on people’s demeanour. boyd (2014), on the other hand, found a paradox between young people’s actual knowledge (in terms of IT) and their awareness of potential threats on the Internet: Teens may make their own media or share content online but this does not mean that they inherently have the knowledge or perspective to critically

examine what they consume. Being exposed to information or imagery via the Internet and engaging with social media do not make someone a savvy interpreter of the meaning behind these artefacts (p. 177). Based on this assumption, I derive to my main hypotheses that aims on answering my overarching research question:

**H1: *The more technical proficient someone is, the less careful he/she behaves while using the Internet.***

This hypothesis predicts a negative correlation between the actual skills and the online behaviour of young people and will be analysed in the analysis part of this thesis. The relevant literature is going to be further examined in Part 2.4 - What is Technical Proficiency?

### **2.3 What are Privacy Concerns?**

There are various forms in which privacy concerns can occur to young people using SNS. To name a few: the misuse of data (companies, hackers, etc.), Cyber-Mobbing, unwanted contact to strangers or unintentionally being watched by their parents. The following section targets on illuminating the potential sources and potential effects on the online behaviour that will then be tested within the analysis part of this paper.

In order to do so it is of utmost importance to deliver a definition of *privacy concerns*. Buchanan (2007) states that privacy concerns *express the desire to keep personal information out of the hands of others* (p. 158). Youn (2009) distinguished online privacy concerns into different levels and views these levels of privacy concerns as protective motivation that activates coping behaviours to deal with privacy risks (p. 393). Considering this to be valid it furthermore supports my main hypothesis that concerned SNS-users tend to behave more careful on the Internet which I developed in section 2.1. Many scholars associate privacy concerns with numerous privacy risks teens are facing. Besides the ones that are mentioned at the beginning of this section Youn (2009) includes emotional discomfort, potential monetary loss and the potential misuse of private data by companies (p. 396). In her study she mainly focused on online-marketing-

related concerns thus making it important to consider other studies as well. Krasnova et al. (2009) however, shared the idea of this categorisation and also added that many teens are concerned about unwanted audiences who have access to their shared content. This process can shift when pictures or intimate information are shared without the aggrieved party's permission in order to harm them as it is defined by Ybarra (2012). Cyber-Mobbing or -bullying according to Ybarra and colleagues is underestimated as a potential threat among scientific researchers. They furthermore found it difficult to develop a standard definition for the term and conceptualise cyberbullying as bullying communicated through the online mode. The results of the study showed that an average of 25% reported being bullied at least monthly in person compared with an average of 10% bullied online, 7% via telephone (cell or landline), and 8% via text messaging. These results demonstrate the presence of cyberbullying and their definition can be adapted to the present study as well as a major sub-category of online privacy concerns.

Since the unwanted contact to strangers is a big issue for teens as discussed by Krasnova et al. (s.a.) one has to consider sexual predators as another source of fear and thus online privacy concerns. boyd (2014) discusses sexual threats intensively and concludes that from the advent of social media it has been impossible to talk about teens' engagement without addressing the topic of online safety and sexual predators (p. 102). As far as Boyd is concerned the issue as such is made up by the media but it remains relevant to talk to teens and inform them about it. Having identified the different forms in which concerns can occur identified it is now important to illuminate the sources and what constitutes online privacy concerns and their intensity which might differ from person to person. Youn (2009) adopted the *protection motivation theory* by Rogers (1975) as a theoretical framework to identify determinants of young adolescents' level of privacy concerns. Rogers's theory assumes two different cognitive appraisals, threat and coping appraisals as major elements that determine privacy concerns and risk reducing behaviours resulting from these. He furthermore includes intrapersonal and environmental sources which potentially affect these cognitive processes into his theory. And indeed later studies which focused on teen's online

behaviour reassured the existence of differences due to gender, age, general knowledge, etc... Moscardelli and Divine (2007) for example found significant differences between boys and girls in terms of their level of online privacy concerns and thus their behaviour. This supports my assumption that girls tend to behave more carefully than boys which is expressed in hypothesis H2b. Another intrapersonal source privacy knowledge or technical knowledge in particular (to be discussed in section 2.4 - What is Technical Proficiency?) which has been discussed by Dommeyer and Gross (2003). Their findings show that people who understand privacy protection mechanisms are suggested to be less concerned because they think that they have full control over their private data. This leads me to another assumption:

***H5: The more technical proficient someone is, the less concerned he/she is in terms of privacy.***

The frequency and variety in which online privacy concerns are discussed in recent as well as in more dated literature illustrates the presence of online privacy concerns as an influencer of online privacy behaviour. The assumptions connected to these variables that were mentioned in this and the previous sections are tested to be true in the analysis part. Technical proficiency as an independent variable, however, still needs to be classified in scientific literature.

## **2.4 What is Technical Proficiency?**

As the previous section has indicated technical knowledge with regard to online privacy issues can be seen as an intrapersonal guidepost for privacy behaviour on the Internet. In order to use this variable within this study it needs to be defined and discussed. This section will conclude the theoretical framework this study is based upon.

Instead of *proficiency* most scholars discuss the terminology of *digital literacy* (Park, 2013) or *privacy literacy* (Trepte et al., 2015). Essentially they all define the same competencies SNS-users should have in order to control their private data while using these very systems. As far as Trepte et al. (2015) are

concerned online privacy literacy may be defined as a combination of factual or declarative (“knowing that”) and procedural (“knowing how”) knowledge about online privacy (p. 7). For the present study the second approach of procedural knowledge will be adapted to assess the (perceived) technical proficiency of the participants. Park (2013) divided digital privacy literacy into three dimensions: Technical familiarity, awareness of institutional practices and policy understanding. He furthermore delivers a basic definition and describes digital literacy as individual knowledge regarding computer-related functions. The results of the study show that there are significant differences between boys and girls when it comes to technical familiarity. In this study females had less technical skills than boys which is why I assume that the same applies to my study:

**H2: *In digital affairs boys are technically more proficient than girls.***

Due to the fact that this paper concentrates on young people (age 10-19) and the competencies (in terms of IT) this age group might be associated with the term *digital natives* (boyd, 2014; Helsper & Eynon, 2010; Vodanovich, 2015) or *millennials* (describes people that were born around the turn of the millennium and hence grew up in times of digitalization)(van den Braber, 2016) were applied to them. Because teens grew up in a world in which the Internet has always existed many adults assume that young people automatically understand new technologies. From this perspective teens are “digital natives whereas adults who are supposedly less knowledgeable about technology and less capable of developing these skills are considered “digital immigrants” (boyd, 2014, p. 176). Since this study’s focus is on millennials or young people an age-related knowledge-gap between millennials and non- millennials as it has been investigated by van den Braber (2016) is not as interesting as potential age differences within the age group of 10 to 19. While Park’s results showed that older users consistently scored low on the technical familiarity items Livingstone, Ólafsson, and Staksrud (2013) came up with contrary findings. In the EU-wide study about children’s risky behaviour on SNS older participants (15-16 years

old) tended to have a higher level of know-how (*find safety info, block messages, change privacy settings*), than younger participants (11-12 years old). Due to the fact that the study of Livingstone and her colleagues is more applicable to the present study (participants were from EU countries instead of the U.S., total N of participants is higher) I assume a positive correlation between age and technical proficiency:

**H3: *The older someone is the more technically proficient he/she is.***

Another interesting determinant for technical proficiency could be the time the participant spends online. Park's study results indicate a correlation between daily Internet usage (logged time) and technical skills. Even though the support for the hypotheses that saw a strong correlation between these variables was far from robust because none of the interaction terms showed significance in the tech dimension (p. 230) I assume that this association will be existent in this study as well. From here the following hypothesis can be derived:

**H4: *The more time someone spends online the more technically proficient is he/she.***

This hypothesis sums up my theoretical explanations and the literature review. The following section will deliver a final overview of my theoretical construct as well as an overview for all the hypotheses.

## **2.5 Causal Diagram and Hypotheses**

Based upon the theoretical framework and hypotheses resulting from that, I developed up the following causal diagram (*Figure 1*). The correlations between the different variables will be overhauled in analysis (see Part 4).

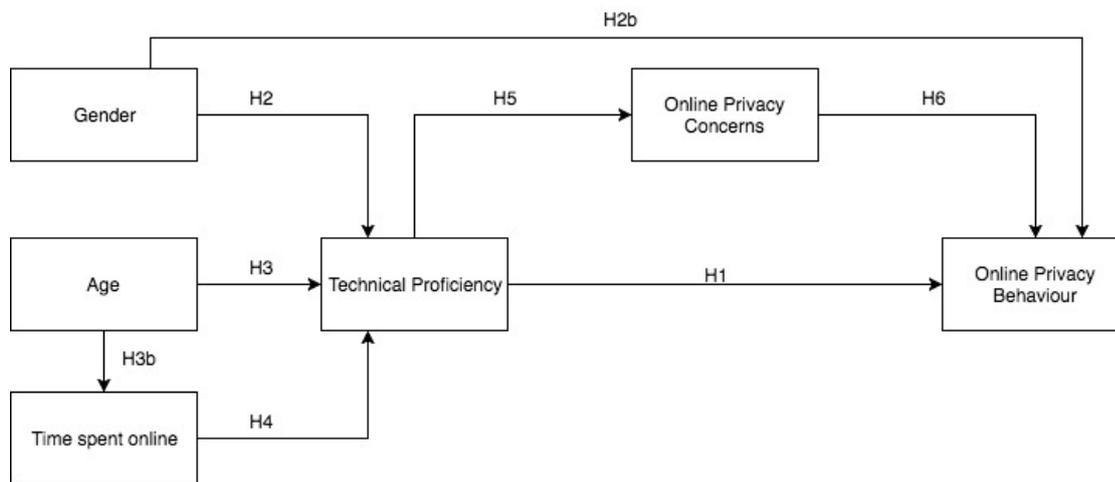


Figure 1: Causal Diagram

As we can see the main hypothesis (H1) assumes a relation between technical proficiency and online privacy behaviour which is predicted to be negative. Alongside this connection online privacy concerns somehow depict a control variable on which H5 and H6 are built upon. Gender, age and time spent online function as independent variables and intrapersonal predictors for the rest of my model. They are connected to several hypotheses (H2, H2b, H3, H3b and H4) as well. The results of the regression analysis will be added to the model later in this paper. Before the methodologies and measurements are going to be explained all hypotheses that resulted from the literature review are recapitulated down below:

H1: The more technically proficient someone is the less carefully he/she behaves whilst using the Internet.

H2: In digital affairs Boys are technically more proficient than girls.

H2b: Girls behave more careful when it comes to online privacy.

H3: The older someone is the more technically proficient he/she is.

H3b: The older someone is, the more time he/she spends online.

H4: The more time someone spends online the more technically proficient he/she is.

H5: The more technically proficient someone is the less concerned he/she is in terms of privacy

H6: The more concerned someone is in terms of privacy the more carefully he/she behaves online.

## **Part 3. Methodologies and Operationalisation**

In the following sections an overview and a description of the data set will be given. Furthermore, the different concepts and their variables will be explained with respect to their operationalisation within the questionnaire. This chapter also includes some statistical remarks to provide the reader with needed information in order to fully understand the analysis which depicts the core part of this paper.

### **3.1 Description of Survey and Data Set Overview**

As already mentioned in the introduction I conducted a questionnaire to gather the required data. The questionnaire was merged with the questions of my fellow student Jeffrey Harrower in order to reach more participants in an efficient way. The initial survey was rather basic and was improved step-by-step together with our supervisors. In the final version of the questionnaire the participants were asked to rate several statements on different 5-point Likert scales. In all scales *one* was equal to *strong disagreement*, *three* was *neutral* or *no statement*, *five* was equal to a *strong agreement*. Besides the questions that were answered on the Likert scale the questionnaire included demographic questions (age, gender, education), open-scale questions (internet usage measured in hours) as well as one item concerning their most frequently used SNS. In total the survey had 38 items. 32 of them were used to gather data for the variables I wanted to measure. After eliminating void questionnaires (6) the data set had a total size of 340 responses. With regard to its demographics the sample I used for the analysis consisted of 53.5% (N = 182) female and 46.5% (N = 158) male participants. The mean of the sample was 14 years old. The youngest participant was 10, the oldest 19 years old. The largest age group (17.4%, N = 59) was 17 years old. Another question aimed on measuring the educational level by asking for the school branch the participant is currently attending. This might be irrelevant for the further analysis (see Part 4) but it still is important in order to get an overview of the sample. The vast majority (86.4%, N = 293) of participants visited the Gymnasium considered as the highest educational branch. Just a small percentage attended the Real- (8.2%, N = 28) or Hauptschule (5.3%, N = 18) in which pupils receive lower graduations.

The questionnaire was paper based because I wanted to reach non-digitals as well as frequent users. A survey conducted online would not facilitate that and the results would be biased due to the fact that it would solely reach people with Internet access. However, 98.2% of the participants used the Internet at least one hour per week. To analyse the data SPSS v22.0 software has been used.

### **3.2 How is Technical Proficiency Measured?**

As well as most of the measures having been applied in the questionnaire the questions concerning technical proficiency were used in this questionnaire for the first time and not adopted from other studies. Hence, there was no opportunity to check whether they were reliable or not. The variable of technical proficiency however, was originally measured with a 4-item question and another 5-item question to differ between the perceived and the actual proficiency of the participants. In the first question the participants were asked how they behave or whom they ask in case they want to change their privacy settings. The second set of questions asked for their actual knowledge (“I know how to ...”). For reliability analysis Cronbach’s Alpha was calculated to test the internal consistency of the subscales for positive affect which consisted of four (“When I want to change my privacy settings ...”) and five (“I know how to ...”) questions. Unfortunately the internal consistency of the first question set was not satisfying with a Cronbach’s Alpha of only = .471. After having erased one question (“I know how to block other persons in SNS”) the second set of items had a satisfying score with Cronbach’s Alpha for positive affect = .766.

Even though the model was not directly adopted from other studies the second item set is a modified version of the *Technical Protection* model by Buchanan (2007) who researched potential differences between technical and non-technical students in terms of their privacy protection behaviours. To measure technical proficiency is still difficult due to the fact that there is no possibility to really assess actual skills of young people within a questionnaire.

Besides the multi-item questions mentioned above there were two separate single “statement”-questions measuring the self-assessed technical proficiency. In

the analysis part high scores will indicate high technical proficiency while low scores represent no technical knowledge.

### **3.3 How is Privacy Concerns Measured?**

To measure privacy concerns I used 6 items asking the participants how concerned they were about certain online privacy issues on a 5-point Likert scale. A high score indicates that the participant is very concerned about the issue, a low score is equal to no or low levels of concerns. The basic construct was adopted from Youn (2009) and then extended by several items. The participants were asked about Cyber-Mobbing, unwanted sharing of intimate data (e.g. pictures), misuse of private information for advertisement and threats caused by strangers. As well as with the technical proficiency variable a test for the internal consistency was conducted. With all six items included the variable was satisfying Cronbach's Alpha for positive affect = .891.

### **3.4 How is Privacy Behaviour Measured?**

The privacy behaviour variable consists of three questions. Two of them are divided into 6 and 3 questions. The items for the first section ("Would you ...") were adopted from the model Dwyer, Hiltz, and Passerini (2007) used in their study about privacy concerns within SNS. They for instance measured the willingness to publish private content or to meet with strangers they met online. In the data analysis a "No" is coded with the value 2 and a "Yes" with the value 1. Hence, the scores for that model range between 6 (for very low self-disclosure) and 12 (for very high self-disclosure). In terms of interpretation a high score can be considered as careful online behaviour and a low score as rather unmindful online privacy behaviour. The second section asked for the participant's behaviour in case that they are asked to uncover *too* private information by online services (e.g. SNS). There were three different statements given which could be answered on a 5-point scale from "*does not apply at all*" to "*totally applies*". To add a self-assessment question the last item of the survey asks for the participant's perceived privacy settings on the Internet in general which could be answered from *low* to *high*.

The first two questions had to be tested in terms of their internal consistency. All items that asked for the information the participant is willing to share and if they would interact with strangers via the Internet or in real life had a rather low internal consistency with Cronbach's Alpha = .523. A score above = .7 can be considered as reliable (Spiliotopoulou, 2009) which is why my model for online behaviour measurement is at least questionable and has to be improved for further research. The same accounts for the second set of questions that was used to evaluate the participant's behaviour. The internal consistency was not satisfying, with Cronbach's Alpha for positive affect = 0.112. Due to the low score I ignored the second set of questions in my analysis and used the first subscales only albeit the score is not satisfying as well.

## Part 4. Analysis

The following part of my paper is the analysis representing the core of my research. In the analysis I test whether my hypotheses are valid and if there is a causal relationship between the different variables. In case there are causal effects I will furthermore analyse if these correlations are positive or negative, strong or weak and whether they are significant. In order to do that a multivariate regression based upon my data set will be conducted.

### 4.1 Descriptive Analysis

*Table 1* shows the descriptive data of the population. I sub-classified all variables by gender in order to figure out significant gender-based differences straight away. The first thing that we can see is that boys and girls do not differ in terms of their time spent online per week. The standard deviation is rather high for both. Outliers could explain this. And indeed there were a few participants who indicated that they use the Internet for more than 100 hours per week which influenced the mean value strongly. In terms of technical proficiency *Table 1* shows that boys scored slightly higher with a mean score of 4.01 versus 3.30 for female participants. Resulting from that, I can state that boys are more proficient than girls. To test this hypothesis (*H2*) I will further analyse a potential causation between gender and technical proficiency in the regression analysis. As already mentioned above the participants could score between 6 and 12 with regard to their online privacy behaviour which is defined by what sort of private information they hand out to strangers and what kind of actions (*meet with strangers they met online*, etc.) they are willing to perform. In the descriptive analysis we can witness that girls tend to behave more carefully (Mean = 10.03) than boys (Mean = 9.57). However, both dissemble most of their private content towards third persons. When it comes to *general privacy settings on the Internet* there are no significant differences (Male = 3.32, Female = 3.38). The mean can be settled somewhere between “I think that my privacy settings on the Internet are

in general *moderate*” and “[...] *rather high*”. Nonetheless, the participants tend to have moderate privacy settings on their SNS accounts or profiles.

		<b>N</b>	<b>Mean</b>	<b>Std. Deviation</b>
Internet Usage	Male	152	17.094	18.01
	Female	178	16.5	17.01
Technical Prof.	Male	158	4.01	0.916
	Female	182	3.30	0.943
Online Privacy Concerns	Male	155	2.688	1.04
	Female	182	3.22	1.190
Online Behaviour	Male	154	9.57	1.41
	Female	177	10.03	1.25
General Online Privacy Settings	Male	152	3.32	1.101
	Female	178	3.38	1.099
Age	Male	157	14.54	1.992
	Female	178	14.27	2.063

Table 1: Descriptive Statistics

The total number of participants ranges between 330 (*Internet Usage*) and 340 (*Technical Proficiency*). This range can be explained by the omittance of questions or invalidity of answers (For more detailed information about the population see *Part 3.1*).

## 4.2 Correlations

This subsection will focus on outcomes of the correlation analysis. Even though the results of this analysis do not explore the relations within the whole model there might be some significant connections between several variables. The causal diagram as a whole will be estimated on the basis of my multivariate regression analysis in Part 4.3. In order to find out whether there are significant strong associations a correlation analyses based on Pearson’s-R has been

conducted. In addition to that the significance of these (potential) relations was estimated with a 2-tailed-test in SPSS.

The most significant connection can be drawn between *age* and *technical proficiency*. With  $r = 0.401$  and  $p = 0.000$  one can state a strong positive correlation between these two variables. Hence, it can be assumed that the older someone becomes the more technical competencies he or she develops. The influence of gender on technical proficiency and online behaviour was part of my research questions and thus hypotheses as well. The output of the correlation analysis has shown that there is a significant strong correlation between *gender* and *technical proficiency* like there is one between *age* and this variable too. A Pearson's-R score of  $-0.355$  and  $p = 0.000$  indicates that gender has a strong and significant influence on technical skills of young people. The negative *p-score* implies that there is a negative connection between gender and proficiency or, in other words, girls seem to be less proficient in terms of digital skills than boys. Another noteworthy relation was found between the technical skills and the online privacy behaviour of the participants.  $P = -0.286$  illustrates that technical competencies influence online privacy behaviour in a negative way which signifies that participants with more knowledge or competencies tend to behave less careful when it comes to their online privacy. In general I can say that all outcomes have been significant after having conducted a 2-tailed-test within SPSS. An overview of all outcomes can be found in the appendices.

#### **4.3 Path Diagram based on the regression model**

Using the causal diagram (see *Figure 1*) as a starting point the following path diagram is constructed on the basis of the regression analysis. The arrow, for which the regression analysis did not show a significant result, has been excluded from the model.

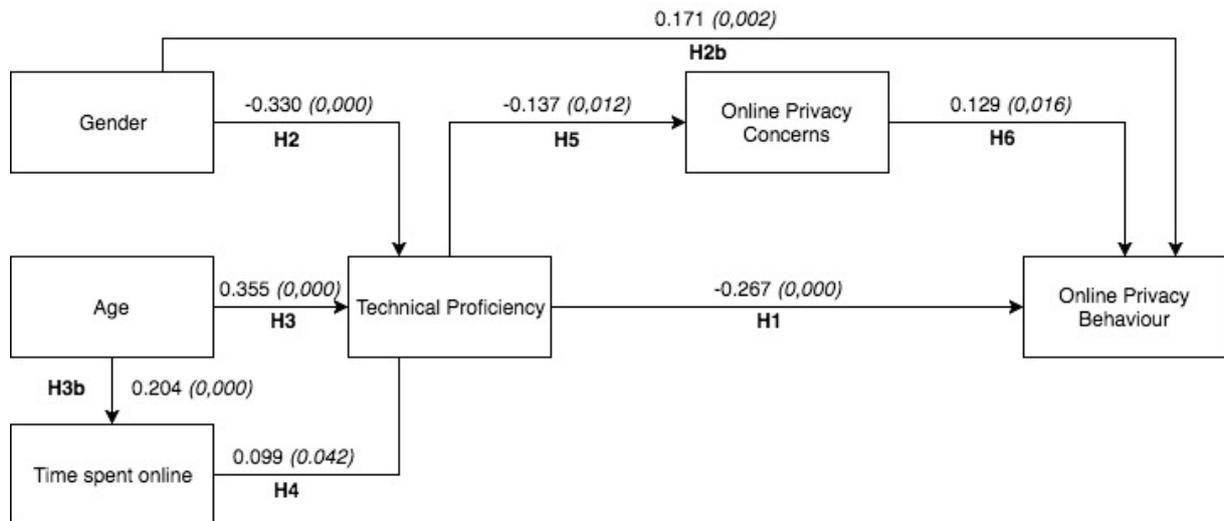


Figure 2: Causal Diagram based on the multivariate regression analysis

#### 4.4 Analysis of the Hypotheses

This part will focus on the analysis of the hypotheses in order of their respective relevance for the main- and sub-research question(s). The path diagram above depicts the findings to answer the questions formulated in the introduction. The first and main research question of this paper enquires the potential effect of IT-related technical skills of young people on their online privacy behaviour which will be answered with hypotheses 1 and 4. Hypothesis 4 depicts a reverse conclusion since it assumes a connection between behavioural trait and technical proficiency.

The second research question deals with potential effects of online privacy concerns on the online behaviour of young people in Germany. To answer this question hypothesis 6 is of special interest. Furthermore hypothesis 5 will be applied to classify the variable of privacy concerns into the study's model. Regarding the two sub-research questions which mainly include demographic variables (age, gender), H2 to H3b will be made use of in order to find an answer.

##### 4.4.1 Analysis of the main Research Question

The main goal of this paper was to answer the question to what extent technical competencies have an influence on the online privacy behaviour of people in Germany. By finding an answer to this question one can arrive at new

approaches concerning educational strategies in schools and homes. The scientific literature as discussed in Part 2 has not sufficiently agreed on a potential association between these factors yet. boyd (2014), for instance, found a paradox between the actual knowledge of young teenagers and their online privacy behaviour. In order to resolve this paradox hypothesis 1 has been set and was then analysed within a multiple regression analysis:

H1: The more technically proficient someone is the less carefully he/she behaves whilst using the Internet.

The outputs of the regression analysis which was conducted via SPSS v22.0.0 support these findings. With a coefficient of -0.267 a relatively strong negative correlation between technical competencies (measured with the items PTP3.1 to PTP3.5 - see 7.2 Appendix B) and online privacy behaviour can be assumed. In other words a technical pro does not necessarily behave carefully on the Internet, just because he/she knows how to protect against potential threats. The *p*-value being smaller than 0.001 delivers a significant result. Hence hypothesis 1 will not be rejected. The findings furthermore contradict the ones of previous studies. Park (2013), in her study, assumed that users with a high level of knowledge are more likely to exercise information control than those with a low level of knowledge (p. 219). The numbers of this analysis indicate the opposite.

**H4: The more time someone spends online the more technically proficient he/she is.**

In terms of what determines technical proficiency one can exclude the factor of time spent online as the results of the regression analysis show. Despite the fact that there is a rather weak association between the duration someone spends online and the technical skills actually assumed by hypothesis 4 one must respect the high *p*-value of 0.042. This indicates a low significance of the findings. Thus hypothesis 4 has to be rejected due to its low significance.

However, the first hypothesis delivers enough information to answer the main research question of this paper. One can state that in fact technical proficiency has an influence on the privacy behaviour of young people in Germany. From these findings the question to what extent this is the case might arise. The sub-research questions as well as the discussion within the conclusion part of this paper might provide answers for that.

#### **4.4.2 Analysis Sub-Research Question No. 1**

The first sub-research question deals with the influence of online privacy concerns on the online behaviour of young people in Germany. In other words; does someone who is aware of potential threats of the Internet, behave different from someone who does not know anything about these issues? Hypothesis 6 depicts the main guidepost and predicts that privacy concerns influence the privacy behaviour in a positive way because people will not disclose as many information as unconcerned people in the same age group. Hence, concerned people's behaviour is considered to be more conscious.

#### **H6: The more concerned someone is in terms of privacy the more carefully he/she behaves online.**

With a coefficient of 0.129 the hypothesis can be seen as supported and thus will not be rejected. The correlation shows a positive effect of concerns on the level of self-disclosure which defines the online behaviour. People who are aware of different types of threats on the Internet are, because of that, more concerned and thus tend to disclose less information compared to the group of people who are not anxious about these very issues. They furthermore tend to refuse to meet or even chat with strangers which can be considered as careful behaviour too. Since the *p*-value of this correlation (0.016) is way higher than the values of other correlations within this analysis, one can consider this correlation as less significant. By applying a significance level of 0.05 (5%), this hypothesis can still be contemplated as significant. This result supports the assumptions and outcomes of other studies too. Buchanan (2007) found a significant correlation

between his Privacy Concern scale and the General Caution scale as well. Albeit the fact that he conducted a linear regression analysis only, a score of  $r = 0.333$  and  $p < 0.005$  (p. 161) goes along with the findings of the present study.

**H5: The more technically proficient someone is the less concerned he/she is in terms of privacy**

To answer the question, in what way privacy concerns influence the online behaviour of young Germans in a proper way, it is essential to estimate potential determinants of privacy concerns. One of them could be technical proficiency, as it is assumed in hypothesis H5. After the multiple regression analysis has been conducted, this statement can be supported. The beta score (-0.137) indicates a negative effect of technical proficiency on the concerns of young people. Because of that, one can say that IT-familiar people are less anxious with regard to threats the Internet might entail. In addition to the existence of a connection between these variables the outcome furthermore showed that significance is given ( $p$ -value = 0.012), when a 5%-level is applied.

Considering the two hypotheses which are related to the first sub-research question as supported, one can say that online privacy concerns have a positive influence on the privacy behaviour of the participants who participated in this study. Technical proficient teenagers, however, are not as concerned as technical less competent fellow men and thus behave less careful. All in all this answer supports the model that has been built by answering the main research question (connected to H1 & H4). Moreover it strengthens the role of the online privacy concern variable as a mediating variable between technical proficiency and online privacy behaviour. Further reasons for that could be explored within the conclusion part of this thesis.

**4.4.3 Analysis Sub-Research Question No. 2**

This section will focus on gender-related differences in terms of technical proficiency and online behaviour. The topic has been explored in a vast number of surveys, previous to this one. Intra-personal sources can be predictors for privacy

concerns (Youn, 2009) and hence the online behaviour as well. So, in order to answer the second sub-research question hypothesis 2b will be adducted.

**H2b: Girls behave more careful when it comes to online privacy.**

It assumes that girls tend to be more cautious when they communicate online and implies on the other hand that boys often show a more parlous behaviour. Moscardelli and Divine (2007) state that girls have a greater fear or awareness of danger and of being the victims of potential aggression and crime. The outcome of their analysis indicated a positive correlation between gender and concerns ( $\beta = 0.097$ ). Since the connection between the scale of concerns and the privacy behaviour has been confirmed above, a similar result can be expected for the present study.

Indeed, the results of the analysis indicate a positive association between gender and online privacy behaviour. A  $\beta$ -score of 0.171 supports hypothesis H2b which is why it will not be rejected. It is furthermore significant as its  $p$ -value is low (0.002). The  $\beta$ -score shows evidence that girls tend to disclose less critical information than boys. H2b is also supported by the findings presented in *Table 1*, where girls scored slightly higher with regard to the security of their general online privacy settings.

To answer the research question in its entirety, one has to include the technical proficient variable as well. Therefore, as elucidated in the theory part, it is assumed that boys hold more technical skills than girls and accordingly behave less careful. This has already been confirmed by analysing the main research question (see Part 4.4.1).

**H2: In digital affairs boys are technically more proficient than girls.**

Like most of the previous hypotheses, this hypothesis is supported by the outcomes of the regression analysis as well. A  $\beta$ -score of -0.330 indicates a strong negative correlation between gender and technical proficiency. In addition to that the findings are significant as the  $p$ -value is 0.000. H2 will not be rejected. The

outcomes of this analysis go along with previous studies too. Park (2013), for instance, found a significant negative correlation between gender and technical skills. Her  $\beta$ -score was somewhat lower (-0.14) but still directed towards the same type of association. Like in Park's study, this paper had a high value (2) for girls and a low value (1) for boys.

To sum up the analysis and answer the second sub-research question of this paper, one can say that both, the level of technical proficiency and the online behaviour (with regard to the level of self-disclosure), differ between boys and girls. While girls tend to behave more careful on the Internet, boys have more technical skills that could help them to protect themselves. Both hypotheses tested within this section were supported by the results of the regression analysis and are in line with previous scientific studies on this topic.

#### **4.4.4 Analysis Sub-Research Question No. 3**

The aim of the third sub-research question was to explore the influence of the age factor on the variables of technical proficiency and online privacy behaviour. A vast majority of scientists agree on the assumption that age leads to more technical skills or literacy. Livingstone et al. (2013) found an increase in digital skills related to the average age of the participants of the study. According to the literature review, hypothesis 3 was set out to answer the question which is targeted in this section.

#### **H3: The older someone is the more technically proficient he/she is.**

Like Livingstone and her colleagues, this present study supports the assumption that older individuals on average have more knowledge related to digital security protection than the investigational group of younger people. The  $\beta$ -score confirms this hypothesis.  $\beta = 0.355$  can be interpreted as a strong connection and in combination with the high significance ( $p$ -value = 0.000) H3 will not be rejected. However it contradicts towards the findings of Park (2013) and Moscardelli and Divine (2007), who found negative or even no significant correlations between the variables that were subject in this hypothesis. The

contradictoriness between the findings of the present study and the two mentioned above might be resolved in the later discussion.

Even though H3 has proven to be true it is necessary to involve another test in order to answer the concluding sub-research question. Albeit the fact that hypothesis 3b does not directly assume changes in online privacy behaviour due to the factor of age, it still predicts an effect on the behaviour in general which, in the end, might allow inferences on the privacy behaviour as well.

### **H3b: The older someone is, the more time he/she spends online.**

In fact, age has an influence on the time teenagers spend online weekly. Interpreting the outcome's numbers allows the conclusion that older teens tend to use the Internet more frequently than younger participants. The  $\beta$ -score (= 0.204) as well as the  $p$ -value (0.000) implies this hypothesis to be true and support it. It is thus not rejected.

To answer the question whether and in what way age has an influence on the two variables mentioned, one can state: Yes, age has an influence. The process of maturing goes along with digital education, regardless of gender or education in terms of school. However the question partly remains unanswered since the second hypothesis which was adducted to answer the second part of the question failed in providing target-oriented answers. This depicts a limitation and has to be discussed in the correspondent section (Part 5.1).

Nevertheless, the analysis of the third sub-research question concludes the analysis part. Fortunately almost every hypothesis that was drawn from the theory part of this paper could be supported by the outcomes of the multiple regression analysis. Most of the findings indicated strong and always significant connections between the relevant variables. The main research question (To what extent does technical proficiency of young people (ages 10-19) in Germany have an influence on their online privacy behaviour?) can be answered by adducting hypotheses 1 and 4. Further backgrounds and potential implementations for educators in Germany will be highlighted in the conclusion section. *Table 2* recapitulates the outcome of the regression analyses together with the results of the tested

significance. One can conclude that 7 out of 8 hypotheses are supported by these very results. The reasons for the failure of hypothesis 4 will be illuminated in the following section.

Hypothesis	$\beta$	<i>p</i> -Value	Supported?
H1: Tech. Prof. → Online Privacy Behaviour	-0.267	0.000	Yes
H2: Gender → Tech. Prof.	-0.330	0.000	Yes
H2b: Gender → Online Privacy Behaviour	0.171	0.002	Yes
H3: Age → Tech. Prof.	0.355	0.000	Yes
H3b: Age → Internet Usage	0.204	0.000	Yes
H4: Internet Usage → Tech. Prof.	0.099	0.042	No
H5: Tech. Prof. → Online Privacy Concerns	-0.137	0.012	Yes
H6: Online Privacy Concerns → Online Privacy Behaviour	0.129	0.016	Yes

Table 2: Hypotheses Support Overview

## Part 5. Conclusions and Discussion

The objective of the study was to understand and estimate potential determinants for the online privacy behaviour of young people in Germany. As a result of the literature review several assumptions concerning what the determinants could be and in what way they influence the digital privacy behaviour crystallised. The literature review itself was complex, due to the massive amount of studies about various definitions, variables and models. Even within the time of working on this thesis, new theories were developed. E.g. Chen et al. (2017), who used three new theories, parallel to the protection motivation theory, to explain scam victimization and online privacy concerns. However, with the gathered data and the analysis which was conducted to provide the reader with answers, this paper could deliver a new perspective on the debate, which has recently heated up due to numerous hacker attacks or, for instance, the *NSA-spying-scandal*.

The analysis of this paper explored the technical competencies of young people in Germany as a predictor for their online privacy behaviour. Hence, it contradicts the findings of many studies and also the general perception of the society. Park (2013), for example, found a positive correlation between technical competencies and privacy securing behaviour. In this study, there was a negative correlation and accordingly technically proficient participants scored lower in terms of privacy behaviour. This could have multiple reasons:

1. As Bartsch and Dienlin (2016) stated in their article, that people with more privacy literacy (which is according to their definition similar to the definition of technical proficiency used in this paper) feel safer and more self confident while using SNSs. According to them, technical proficient users are in general less concerned. This has been underlined by the present study as well.
2. Another reason for this finding that furthermore goes along with the previous point, is delivered by Livingstone, Haddon, Görzig, and Ólafsson (2011). In their report they argue that children who are more digitally

literate are less jeopardised of being harmed when using SNSs. They have the competencies to defend against threats like, for instance, being cyber bullied by classmates. Hence, they are less concerned and because of that, less careful when it comes to their privacy.

3. Thirdly, this correlation could have occurred due to limitations related to the questionnaire that will be targeted in the next section. Yet, one can remark that the questionnaire asked for the 'know-how' of the participants concerning privacy-securing-related skills, but missed out on asking if and how they actually use these mechanisms, applications and whatsoever. Even though the survey requests the general privacy settings, the appliance of the applications was not assessed. As mentioned above, this has to be further discussed in the limitation section below.

Furthermore the study indicated that the variable of online privacy concerns is a mediating factor between technical proficiency and online privacy behaviour. As the results of the analysis show, it is affected by technical proficiency and positively correlates with the level of self-disclosure (equal to online privacy behaviour). These findings highlight the importance of general awareness concerning online privacy threats and the concerns that might arise from these.

The analysis of the hypotheses turned out to be quite surprising, since almost every hypothesis was supported by outcomes of the multiple regression analysis. Except for hypothesis H4 all other hypotheses of this survey were confirmed to be true.

But why are the results like that? One explanation for the missing correlation could be an issue or deficits within the questionnaire. There was no item asking for the participant's actual type of activity when he or she uses the Internet. There was an item which assessed the time the participant spends on his favourite websites or SNSs per week. Unfortunately there was no item measuring the frequency in which the participant deals with privacy related topics while he or she uses the Internet.

All in all the findings of this study strengthen the important role of technical proficiency among young adolescents. For the future it is important to raise the awareness and skills towards online privacy threats, though.

Without any doubt the present age features great potentials which could lead us into a brighter, digitalized future. As this study has shown, almost every participant of this study uses the Internet on a daily basis. With a potential common ubiquitous strategy for guiding young people towards a more conscientious behaviour, they could deal with threats in a far better way and will have better experiences and results out of their Internet communication.

### **5.1 Limitations**

Throughout the work on this paper, numerous limitations occurred. A lot of them are related to the process of data gathering. Due to the fact, that the used concepts were applied in the questionnaire mostly for the first time, there reliability (Cronbach's Alpha) was not always given. Because of that, some items had to be excluded from the analysis which impeded an in-depth assessment of the participant's skills, concerns and behaviour.

Talking about difficulties in this assessment one can assert that in fact it is much more complex than initially anticipated to really assess the actual digital skills of young people within a paper-based questionnaire. The items were somewhat measuring the 'perceived' technical proficiency of the participants. On the other hand an online test within an online questionnaire would be biased and might have excluded those who do not have an Internet access.

A bias was existent anyway, owing to the fact that the study included German secondary schools in the western part of Germany only. Regarding the short time span in which the study was conducted it was almost impossible to include more than these two schools. For future research work it would be important to use more complex models in order to better assess technical proficiency. Furthermore more participants should be included into the study population to reach a higher level of representation.

### **5.2 Policy and Strategy Recommendations**

Regarding potential policy implications for educators, no matter if theoretical or practical, it might be interesting to conduct an international comparison since Germany is the only country that was explored in the present study. Maybe German teachers can use foreign educational policies as a pattern for their own concepts. The study has shown that often technical proficiency is existing but the awareness towards online privacy issues has to be increased. Since school are the place where young people spend a bulk of their time, it seems to be likely to target these issues within the educational facilities. Even though, IT-related subjects are part of the German core curriculum the present study revealed that technically competent teens care less about their privacy than non-technical proficient teens. Therefore this paper recommends guidelines for teachers including the aspects of skills and awareness. These guidelines could also highlight the importance of conscientious digital privacy behaviour. By repeating these ‘digital privacy instruction’- days (one possible name) on a yearly or even monthly (due to the fast changing privacy policies of SNSs) basis for each class level, these instructions could be adapted to the age dimension and counter potential age-based differences among the secondary-school-aged adolescents.

Furthermore, this paper recommends establishing an independent, open-source information pool for up to date recommended digital privacy settings and behaviour for widespread SNS as well as for other mayor Internet communications hubs, Internet buying portals etc. By doing this, a superior ‘Department for Digital affairs’ could assure that teachers, regardless of their own technical knowledge, provide important information to their young students. This could additionally alleviate the work of the teachers, since an external governmental institution provides the teaching material. This institution could work EU-wide in order to develop a EU guideline for teaching children in digital affairs.

The findings of the study uncovered a lack of information in terms of privacy threats. Hence, it is to state that the existing policies are not sufficient with respect to their quantity and/or quality.

## 5. Literature

- Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509-514.
- Appari, A., & Johnson, M. E. (2010). Information security and privacy in healthcare: current state of research. *International journal of Internet and enterprise management*, *6*(4), 279-314.
- Bartsch, M., & Dienlin, T. (2016). Control your Facebook: An analysis of online privacy literacy. *Computers in Human Behavior*, *56*, 147-154.
- Baruh, L. (2017). Online privacy concerns and privacy management: A meta-Analytical review. *Journal of Communication*, *67*(1), 26-53. doi: 10.1111/jcom.12276
- boyd, d. (2014). *It's complicated : the social lives of networked teens*. New Haven: Yale University Press.
- Buchanan, T., Paine, C., Joinson, A. N., Reips, U. D. (2007). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology*, *58*(2), 157-165. doi: 10.1002/asi.20459
- Chen, H., Beaudoin, C., & Hong, T. (2017). Securing online privacy: An empirical test on internet scam victimization, online privacy concerns, and privacy protection behaviors. *Computers in Human Behavior*, *70*, 291-302. doi: 10.1016/j.chb.2017.01.003
- DeVries, W. T. (2003). Protecting Privacy in the Digital Age. *Berkeley technology law journal*, *18*(1), 283-311.
- Dommeyer, C., & Gross, B. (2003). What consumers know and what they do: An investigation of consumer knowledge, awareness, and use of privacy protection strategies. *Journal of Interactive Marketing*, *17*(2), 34-51. doi: 10.1002/dir.10053
- Dwyer, C., Hiltz, S., & Passerini, K. (2007). Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. *AMCIS 2007 proceedings*, 339.
- Fishbein, M., & Ajzen, I. (2011). *Predicting and changing behavior: The reasoned action approach*. New York: Taylor & Francis.
- Frees, B., & Koch, W. (2015). Internetnutzung: Frequenz und Vielfalt nehmen in allen Altersgruppen zu [Internet use: Frequency and variety increase for all age groups]. *Media Perspektive*, *9*, 366-377.
- Helsper, E., & Eynon, R. (2010). Digital natives: Where is the evidence? *British Educational Research Journal*, *36*(3), 503-520. doi: 10.1080/01411920902989227
- Krasnova, H., Günther, O., Spiekermann, S., & Koroleva, K. (2009). Privacy concerns and identity in online social networks. *Identity in the Information Society*, 39-63.
- Livingstone, S. (2008). Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression. *New media & society*, *10*(3), 393-411.

- Livingstone, S., Haddon, L., Görzig, A., & Ólafsson, K. (2011). Risks and safety on the internet: the perspective of European children: full findings and policy implications from the EU Kids Online survey of 9-16 year olds and their parents in 25 countries.
- Livingstone, S., Ólafsson, K., & Staksrud, E. (2013). Risky social networking practices among “underage” users: lessons for evidence-based policy. *Journal of Computer-Mediated Communication*, 18(3), 303-320.
- Moscardelli, D., & Divine, R. (2007). Adolescents' concern for privacy when using the internet: An empirical analysis of predictors and relationships with privacy-Protecting behaviors. *Family and Consumer Sciences Research Journal*, 35(3), 232-252. doi: doi:10.1177/1077727X06296622
- Newman, A. L. (2015). What the "right to be forgotten" means for privacy in a digital age. *Science*, 347(6221), 507-508. doi: 10.1126/science.aaa4603
- Park, Y. J. (2013). Digital Literacy and Privacy Behavior Online. *Communication Research*, 40(2), 215-236. doi: 10.1177/0093650211418338
- Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The journal of psychology*, 91(1), 93-114.
- Sheehan, K. (2002). Toward a typology of internet users and online privacy concerns. *The Information Society*, 18(1), 21-32. doi: doi:10.1080/01972240252818207
- Spiliotopoulou, G. (2009). Feature article: Reliability reconsidered: Cronbach's alpha and paediatric assessment in occupational therapy. *Australian Occupational Therapy Journal*, 56(3), 150-155.
- Stein, L., & Sinha, N. (2002). *New Global Media and Communication Policy: the Role of the State in Twenty-First Century*. London: Sage.
- Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., & Lind, F. (2015). *Do people know about privacy and data protection strategies? Towards the “Online Privacy Literacy Scale”(OPLIS)*. Springer Netherlands.
- van den Braber, S. (2016). *Security and privacy perceptions of millennials (18-24) and non-millennials (36-50) on Facebook*. (Bachelor), University of Twente, Enschede, The Netherlands.
- Vodanovich, S., Kathy Ning Shen, and David Sundaram. (2015). Social competence of digital natives: Impact of Social Networking Sites (SNS) use. *University of Wollongong in Dubai - Papers*, 1.
- Warren, S., & Brandeis, L. (1890). The Right to Privacy. *Harvard Law Review*, 4(5), 193-220. doi: doi:10.2307/1321160
- Ybarra, M. (2012). Defining and measuring cyberbullying within the larger context of bullying victimization. *Journal of Adolescent Health*, 51(1), 53-58. doi: doi:10.1016/j.jadohealth.2011.12.031
- Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *Journal of Consumer affairs*, 43(3), 389-418.

## 7. Appendices

### 7.1 Appendix A - Correlation Table

Correlation Table (Pearson's Correlation), with significance and total number of cases

		Gender	Age	Internet usage/week	Technical Proficiency	Online Privacy Concerns	Online Behaviour
Gender	Pearson-R	1	-0.67	-0.17	-0.355	0.233	0.171
	Sig. (2-tailed)		0.222	0.761	0.000	0.000	0.002
	N	340	335	330	340	337	331
Age	Pearson-R	-0.67	1	0.204	0.401	-0.206	-0.309
	Sig. (2-tailed)	0.222		0.000	0.000	0.000	0.000
	N	335		325	335	332	326
Internet usage/week	Pearson-R	-0.17	0.204	1	0.177	0.031	-0.137
	Sig. (2-tailed)	0.761	0.000		0.001	0.579	0.014
	N	330	325		330	327	321
Technical Proficiency	Pearson-R	-0.355	0.401	0.177	1	-0.137	-0.286
	Sig. (2-tailed)	0.000	0.000	0.001		0.012	0.000
	N	340	335	330		337	331
Online Privacy Concerns	Pearson-R	0.233	-0.20	0.031	-0.137	1	0.167
	Sig. (2-tailed)	0.000	0.000	0.579	0.012		0.002
	N	337	332	327	337		330
Online Behaviour	Pearson-R	0.171	-0.30	-0.137	-0.286	0.167	1
	Sig. (2-tailed)	0.002	0.000	0.014	0.000	0.002	
	N	331	326	321	331	330	

## 7.2 Appendix B - Survey Items

### Demographics

Gender:

- Male (1)
- Female (2)

Age: How old are you? (in years)

Education: Currently I am attending ...

- Hauptschule
- Realschule
- Gymnasium

### Internet usage

Time spent on SNS:

- Per week usage in hours

Most used SNS:

- Facebook (1)
- Instagram (2)
- Snapchat (3)
- AskFM (4)
- YouTube (5)

### Perceived Technical Proficiency

PTP1.1: If I want to change the privacy settings on this SNS I ask my parents.

PTP1.2: If I want to change the privacy settings on this SNS I ask my friends.

PTP1.3: If I want to change the privacy settings on this SNS I browse the Internet.

PTP1.4: If I want to change the privacy settings on this SNS I do that on my own.

PTP2: I think that I know how to browse the Internet anonymously.

PTP3.1: I know how to delete my browser's history.

PTP3.2: I know how to use an AdBlocker.

PTP3.3: I know how to block other persons on SNSs.

PTP3.4: I know how to delete Cookies.

PTP3.5: I know how to use Anti-Virus-programmes.

### **Online Privacy Concerns**

OPC1: How concerned are you that unwanted persons can see your online postings (teachers, parents, classmates, potential future employers)?

OPC2: How concerned are you that pictures of you are published without your permission?

OPC3: How concerned are you that you are exposed on the Internet (Cyber-Mobbing)?

OPC4: How concerned are you that your data is used for advertisements?

OPC5: How concerned are you that strangers watch you through your webcam?

OPC6: How concerned are you that strangers pretend to be of the same age as you?

### **Online Privacy Behaviour**

OPB1.1: Would you publish a profile picture of yourself online?

OPB1.2: Would you publish your phone number?

OPB1.3: Would you publish your private address (also E-mail)?

OPB1.4: Would you publish your real name?

OPB1.5: Would you chat with strangers?

OPB1.6: Would you meet with someone you met on the Internet?

OPB2.1: If a website or SNS asks me for too private information I will give false information.

OPB2.2: If a website or SNS asks me for too private information I will ask my friends/parents/teachers for advice.

OPB2.3: If a website or SNS asks me for too private information I will search for other websites or SNSs which do not ask for these information.

OPB3: I think that my privacy settings on the Internet are in general ...

- Low (1)
- Rather low (2)
- Moderate (3)
- Rather high (4)
- High (5)

## **8. Honesty Declaration**

Hereby, I declare that I have composed the presented paper independently on my own and without any other resources than the ones indicated. All thoughts taken directly or indirectly from external sources are properly denoted as such.

This paper has neither been previously submitted to another authority nor has it been published yet.

Münster, 7th of August, 2017

A handwritten signature in blue ink, appearing to read 'M. Vor dem Berge'.

Moritz Vor dem Berge (s1741594)