

University of Twente, Enschede, NL | Westfälische Wilhelms-Universität, Münster, DE

BSc Public Governance across Borders

28th August 2017

Bachelor Thesis

Social Communication and Digital Privacy Concerns of Teenagers

Jeffrey Harrower

Bachelor Circle “Digital Privacy”

1st Supervisor: Dr. J. Svensson

2nd Supervisor: Dr. G. Jansen

ABSTRACT

Despite the growing popularity of Social Networking Sites, little is known about how online behavior, especially that of younger teenagers who are often described as the generation of 'digital natives', is influenced. Abuses and breaches related to digital privacy, such as cyber-bullying and the gathering of 'Big Data' are also becoming ever more prominent, raising concern. Using insights from the Theory of Planned Behavior by Fishbein and Ajzen, this paper thus tries to examine how social communication relates to digital privacy concerns and protective online behavior. Furthermore, the aim of this study is to provide insight into how teenage boys and girls differ when addressing the digital sphere. To do so, questionnaire-based survey data collected from two German secondary schools in 2017 (N=340) is analyzed.

Table of contents

1. Introduction.....	1
2. Theoretical Framework.....	3
2.1 Privacy Concerns.....	3
2.2 Social Communication.....	4
2.3 Online Behavior.....	5
2.4 Age and Gender.....	6
2.5 Theory of Planned Behavior.....	7
3. Methodology.....	8
3.1 Participants and Procedures.....	8
3.2 Measurements.....	9
3.3 Descriptive Statistics.....	11
3.3 Statistical Analysis.....	12
4. Results.....	12
4.1 Correlations.....	12
4.2 Regression Analysis.....	14
5. Conclusion.....	17
5.1 Discussion.....	17
5.2 Theoretical Implications.....	19
5.3 Practical Implications.....	20
5.4 Limitations.....	21
6. References.....	22
7. Appendix.....	24
7.1 Appendix A – Survey Items.....	24

1. INTRODUCTION

In this project we will study, whether the social communication of young adolescents has an effect on their attitudes and behaviour towards online privacy. Not only have Social Networking Sites (SNS) as well as information- and media sharing sites such as Facebook, Instagram and Twitter experienced a vast growth in users in recent years, with tremendously increasing quantities of personal data being stored, but the users of SNS have also become ever younger (Dingli and Seychell, 2015). Youn (2009) already states, that younger adolescents and teenagers are also concerned about their privacy. The generation of millennials and later is often being described as 'digital natives'. Dingli and Seychell (2015) define 'digital natives' as "today's young people who were born into the digital era and are growing up exposed to the continuous flow of digital information" (p. 9). As the potential threats towards digital privacy have also become ever more prominent and little is known about how SNS use the personal data provided – this has raised concern in the recent years about how online users can address their privacy in the digital sphere. Regarding younger users of SNS, another phenomena is the so-called cyber-bullying. The form of digital harassment, -humiliation and -stalking has increased within the last years (Patchin, 2016) and undermines the importance for privacy-related action especially for young people and pupils. Another phenomenon that has raised interest in the relationship between online self-disclosure and digital privacy concerns, is the so-called *privacy paradox*. It indicates that, "on the one hand, people tend to present themselves in online space by sharing their interests, likes, tastes, [...]. But on the other hand, they are wary of the potential social privacy threats [...] and have some degree of 'privacy concern'" (Dhir et al, 2017, p. 2). By also addressing the privacy paradox, this study hence contributes to the emerging literature.

There is not yet a substantial amount of research regarding privacy behaviours of young adults, taken into account that the subject is still relatively new. Yao et al (2007) for example examine, how "user concerns about online privacy differ for men and women" (p. 712). However, the focus of their study lies rather also psychological factors such as need for privacy or generalized self-efficacy as independent variables. The work by Davis and James (2013) examines "how [...] middle school students think about and manage privacy in new media environments" (p. 9) and gives qualitative results about the values of young adults. Most of the research conducted regarding the matter thus either focusses on older age-groups such as millennials (aged 18-24) and college students or seeks to examine psychological rather than sociological factors accounting for different online privacy behaviour. Though there are

existing studies in the field of gender-related privacy concerns, they are either relatively old regarding the exponential growth of the digital sphere in the past decade, or were conducted in the United States or Asia and therefore far abroad. Dhir et al (2017) further indicate, that “the prior social media literature has been criticized due to its overemphasis on United States (US) based study participants” (p. 2).

In this study we seek, however, to reveal what social conditions or social contexts, e.g. what experiences are being made online, whether there is parental-, teacher- or peer influence on online behaviour or whether the topic of privacy is being discussed more often, cause people to give up or protect digital privacy and whether there are differences to be observed regarding gender and age: The social communication about digital privacy thus is expected to influence digital privacy concerns and therefore the online behavior. Yao et al (2007) state, that women generally have more concern about privacy than men. Does this still account for privacy in the digital sphere? Does this still account for the younger generation, the so-called digital natives? Also, as that particular article is from 2009, do theories from vastly ten years ago still prove true in today’s society, which could find itself to be far more sophisticated due to recently experienced privacy breaches and scandals? But also focussing on the social context, especially social communication about digital privacy, questions arise, when wanting to explain differences in online privacy behaviour between boys and girls: Do girls have other experiences online than boys? Are they maybe being warned more often by important others (e.g. parents, teachers, peers..) or do they discuss the topic more often than boys? The study thus addresses the following explanatory research questions:

RQ1. *To what extent do differences in social communication about online privacy risks explain differences in digital privacy concerns and protective online behaviour of boys and girls of different ages?*

SubQ 1. *In what ways and to what extent do teenage boys and girls differ in social communication about online privacy risks?*

SubQ 2. *In what ways and to what extent do teenage boys and girls differ in digital privacy concerns?*

SubQ 3. *In what ways and to what extent do teenage boys and girls differ in protective online behaviour?*

SubQ 4. *To what extent do age, gender and social communication about online privacy risks explain differences in digital privacy concerns and protective online behaviour?*

As my colleague Mr. Vor dem Berge conducted similar research – examining whether technical proficiency of young adults has an impact on their concerns regarding privacy and their online behaviour – we have decided to merge our surveys into one, allowing us both a higher response. We have thus questioned over 340 pupils of German secondary schools and can therefore give insight into the matter from a European perspective, allowing international comparison regarding the societal circumstances related to the sphere of digital privacy and in that way, may help understanding the concerns of young adolescents – the new generation of digital natives – which may have differing motivations and conceptions, than students or adults.

We start with discussing the prior research related to digital privacy and online behaviour. Also, we discuss the Theory of Planned Behavior by Ajzen and Fishbein as one possible explanation for specific online behaviour. Then we present our methodology including the survey items and measurements as well as how the study was conducted. In the next section, we present the data on privacy concerns and social communication and how these affect the protective online privacy behaviour. We conclude by discussing comparisons between age and gender and discuss different theoretical and practical implications as well as some limitations to this study.

2. THEORETICAL FRAMEWORK

2.1 Privacy Concerns

Yao et al (2007) defined the concept of privacy before narrowing it down towards online privacy. They state, that there is “very little agreement on the definition of privacy” (p. 710) in the social and behavioural sciences due to the fact, that the term is used by scholars in different contexts with different meanings. However, it is concluded, that privacy deals with the control of personal information as “the right of the individual to decide what information about himself should be communicated to others and under what condition” (Yao et al, 2007, p. 710). The four factors of online privacy that are identified in their study are “unauthorized secondary use of personal information, improper access of digitally stored personal information, collection of personal information, and errors in collected personal information” (Yao et al, 2007, p. 711). To conclude towards the concerns about online privacy, Yao et al (2007) rely on studies indicating, that these “focus both on companies that seek to obtain and use personal information for marketing purposes as well as to more general entities such as spammers, hackers, viruses, and university/government monitoring” (p. 711). This could also

include the fear of one's webcam being hacked, as the widespread trend of covering up the laptops' webcam shows, after the US FBI director has warned to do so (Boult, 2016).

However, this study focuses on online privacy concerns of teenagers, which tend to share more information about themselves on Social Networking Sites (Madden et al, 2013). As Social Networking Sites, such as Facebook and Instagram, bear obvious benefits in terms of socializing and connecting with others to their users, the shortcomings and problems have also become more prominent. These rising privacy issues and concerns have led to the discussion about what one shall disclose about himself online and how the collected data online is being processed. Krasnova et al (2009) have identified in their study online social media specific privacy concerns. The most frequently mentioned concern was “General Accessibility” (p. 45), including unwanted access of the information provided through e.g. parents, teachers, fellow pupils, but also future employers. Further concerns mentioned are “Social Threats” (p. 46) which include forms of cyber-bullying and online harassment.

Especially when addressing privacy concerns of the youth, what appears prominent is the fear of paedophiles or other inappropriate audiences preying on the under-aged. To find out, whether such fears are still amongst the teenagers in this time – as recent media scares and enlightenment campaigns could have proven effective – is another aim of this study.

2.2 Social Communication

A previous study by Moscardelli and Divine (2007) has focussed on parental- and peer-influence as determinants of privacy concerns. The socialization agents used were about family-communication patterns and one's susceptibility towards peer-influence. One finding was, that socio-oriented family communication is not related to teens' privacy concerns, concluding, “that privacy concern is developed through communication with teens and not necessarily through rule setting” (p. 246).

We are interested in this study, whether social communication between teenagers and their peers in general can account for differences in their level of privacy concern and also their behaviour within Social Networking Sites. We conceptualize social communication as whether the teenagers do talk about topics related to digital privacy and how often they do so. We also take into account, whether they talk about it with teachers, friends or their parents. Talking about the possible privacy-related risks within SNS could lead to the spreading of such concerns and the creation of a privacy-related consciousness. We therefore hypothesize the following:

H1. When teenage boys and girls frequently address the topic, they show higher concerns for digital privacy.

2.3 Online Privacy Behaviour

Youn (2009) states, that “a positive relationship between the level of privacy concerns and protection behaviours has been consistently found in studies of adult consumers” (p. 399). Such coping strategies for when websites ask for sensitive personal information, which the user does not comfortable about, include fabricating false information, seeking guidance from peers or adults and refraining from certain websites/services. Another study by Moscardelli & Divine (2007) indicates the same relationship, “that increasing adolescents' concern for their online privacy leads to greater use of privacy-protecting behaviors” (p. 247). We expect that relationship to still prove itself true in today’s age, allowing us to hypothesize the following:

H2a. Teenage boys and girls, who are more concerned about digital privacy, are more likely to engage in privacy protection measures.

H2b. Teenage boys and girls, who frequently address the topic of digital privacy, are more likely to engage in privacy protection measures.

We think that examining the level of self-disclosure, that teenage boys and girls tend to have within Social Networking Sites is an essential measure for their privacy-related online behaviour. Do they have pictures of themselves, their address or maybe their phone number or other sensitive personal information on their online profiles? Krasnova et al (2009) indicate, that “detailed and updated profiles can be more attractive for bullies, who might eventually use this information to harass a victim” (p. 53). Therefore, we hypothesize the following:

H2c. Teenage boys and girls, who are more concerned about digital privacy, are less likely to provide sensitive personal information.

H2d. Teenage boys and girls, who frequently address the topic of digital privacy, are less likely to provide sensitive personal information.

Another important measure would be the privacy settings or the transparency within Social Networking Sites. As most sites, such as Facebook for example, allow the user to actively control the privacy settings in terms of what information shall be disclosed publicly or privately and how one can be *found* online. Profiles, where most of the sensitive personal

information is only visible to pre-selected friends would be less prone to abuse, such as bullying, and thus not visible to unwanted audiences. Measuring the actual settings for this study would prove itself not feasible. We can therefore only ask for how high or low the respondent perceives his own privacy settings. We hypothesize the following:

H2e. Teenage boys and girls, who are more concerned about digital privacy, show higher privacy settings in their SNS.

H2f. Teenage boys and girls, who frequently address the topic of digital privacy, show higher privacy settings in their SNS.

When computing a total measure of protective online privacy behaviour, including the three mentioned measures privacy protection, self-disclosure and perceived privacy settings, we can hypothesize the following:

H3a. Teenage boys and girls, who are more concerned about privacy, show a higher total protective online privacy behaviour.

H3b. Teenage boys and girls, who frequently address the topic of digital privacy, show a higher total protective online privacy behaviour.

2.4 Age and Gender

A previous study by Dhir et al (2017) indicates, that adolescents in general are less concerned than young adults. Similarly, Feng and Xie (2014) found that younger teenagers had lower privacy concerns and therefore showed a higher level of self-disclosure on the internet, compared to older adolescents. As both studies focussed however, on age groups older than in the current study, we can only assume a similar relationship when examining the concerns of middle-school-aged pupils.

Yao et al (2007) indicate, that women are generally more concerned about privacy than men. This could be due to the fact, that women are more prone to abuse, especially sexual abuse, harassment and stalking. Dhir et al (2017) in their study had similar findings, which suggested that male young adults “tend to self-disclose more and to have relatively lower privacy concerns compared to female young adults. Similarly, male adolescents are known to self-disclose more personal information online compared to their female counterparts” (p. 8).

We have not yet found substantial literature addressing age and gender differences in

social communication (about possible privacy risks), but as younger teenagers in nature are newer to the digital sphere, we can expect them to address the dangers and threats to privacy more often, especially with their parents and/or teachers. A previous study by Moscardelli and Divine (2007) indicates that “Conventional wisdom suggests that females are more communicative than males” (p. 246). Furthermore, as we also expect females to be more concerned than males, in turn, we also expect females to address the topic of digital privacy more frequently than males. Based on the prior literature and expectations, we propose the following hypotheses:

H4a. Older teenage boys and girls are more concerned about privacy, than younger teenagers.

H4b. Female teenagers are more concerned about privacy, than male teenagers.

H5a. Older teenage boys and girls address the topic of digital privacy less frequently, than younger teenagers.

H5b. Female teenagers address the topic of digital privacy more frequently, than male teenagers.

Figure 1 shows the proposed research model.

2.5 Theory of Planned Behavior

The Theory of Planned Behavior by Fishbein & Ajzen states, that it is the intention of a person, which predicts its behaviour. The determinants of the intention are, on the one hand, the behavioural beliefs and evaluations and on the other hand, the normative beliefs and motivation to comply. Together with the perceived behavioral control, the attitude towards the behaviour and the subjective norm determine the intention towards the behaviour. The theory further states, that people then show a specific behaviour, when they evaluate it as positive, and when they think, that their significant others would also evaluate it as positive (University of Twente, 2017).

The Theory of Planned Behavior can be applied to this study, as it seeks to explain specific behaviour. It can therefore be used as a possible explanation when wanting to predict the online privacy behaviour of teenage boys and girls. However, not all components were measured, hence, this study does not specifically test the theory. Yet, the core assumptions are reflected in the underlying mechanism that social communication as the subjective norm, and digital privacy concerns as the attitude towards the behavior together lead to the person's intention to perform specific protective online privacy behavior.

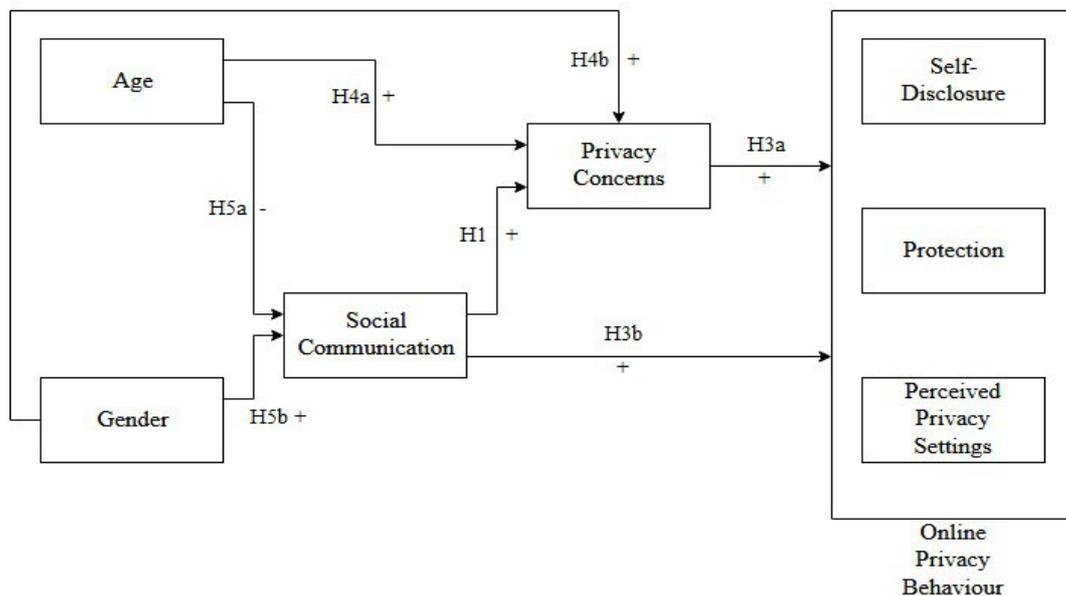


Figure 1 – Research Model

3. METHODOLOGY

3.1 Participants and Procedures

As my colleague Mr. Vor dem Berge conducted similar research, examining the effects of technical proficiency on privacy concerns and online behaviour with teenage boys and girls, we decided on similar measurements and thus merged our surveys into one. This allowed us a higher response rate, as well as the opportunity to conduct the research together and thus working more effectively.

Two German secondary schools participated. The German secondary school system consists of four types of schools. The *Gymnasium* offers the highest secondary education, solemnly allowing further admission at a university. The *Real-* and *Hauptschule* offer secondary education either qualifying for admission to the next higher level or vocational training. The fourth type is the so-called *Gesamtschule*. It combines all three tiers of education, with pupils of all levels being educated together until a certain year.

The first participating school for this study was a *Gymnasium* situated in a major city in the state of North-Rhine-Westphalia, home to many institutions of higher education. After given consent by the schools headmaster, the surveys were handed out by us in person. We

kept supervision about the process and informed teachers and pupils where needed. We tried to reach a sample of all classes and ages of the school. The graduating classes did not participate, as the study was conducted after their graduation ceremony. The second school that participated was a *Gesamtschule* in a major city in the German state of Lower-Saxony. Given consent for conducting the survey was more time consuming at that point, as education in Germany is regulated by the individual states. The state of Lower-Saxony, as opposed to North-Rhine-Westphalia, requests a written proposal to the state board of education for any types of research to be conducted at schools. After adoption, the conduction of the research proved similar as with the first school.

At first, 346 people participated in our survey. After straight lining and eliminating the biased responses a total of 334 valid responses were considered for our research. The final sample consisted of 53,5% females and 46,5% males, where the mean age of the sample was 14 years old, with ages 10 to 19 covered. The vast majority of the participants were educated at a *Gymnasium*, representing over 86,4% of the total sample, 8,3% were educated at a *Realschule* and only 5,3% at a *Hauptschule*. The mean internet usage per week was 16,7 hours. SPSS 22.0 was used for the analysis of the descriptive statistics.

3.2 Measurements

For this study a 5-point Likert scale is used for all measures except for the demographic measures, usage measures and the self-disclosure measures. Cronbach's Alpha was used to assess the reliability of the measures, more precisely the internal consistency of the items, whether they measure what they are supposed to. A high level for alpha indicates high reliability for the scale, although a low alpha might not automatically indicate the opposite. As very few measures are based upon previously validated studies, they could not be considered reliable prior to the conducting of the surveys. The concluding section of this thesis also delivers arguments for not wrongly labelling scales with a low alpha as untrustworthy.

3.2.1 Social Communication

The items measured for social communication (SC) were not adapted from previously validated studies. The social communication scale contains six items measured along a 5-point Likert-scale. The first three items ask for the frequency, with which the respondent addresses the topic of digital privacy and its dangers with parents, teachers or friends. The last three items address the importance of the topic with parents, teachers or friends. High scores for the first three items indicate that the respondent frequently addresses digital privacy with

his/her parents, teachers and peers, while high scores for the last three items indicate that the topic is important with his/her parents, teachers and peers. An example item could be SC6 “Cyber-bullying and other dangers in the internet are a big issue within my circle of friends.”, here a high score indicates, that threats to digital privacy are important to the respondent and his friends. The Cronbach's Alpha was 0,589.

3.2.2 Privacy Concerns

The items measured for privacy concerns (PC) were not adapted from previously validated studies. The privacy concerns scale contains six items measured along a 5-point Likert-scale. High scores for these six items indicates that the respondent shows high concerns towards the threats and dangers towards online privacy. For example, when a respondent indicates a high score for PC1 “How concerned are you, that unwanted audiences (teachers, parents, fellow students and potential future employers) can view content about you?” he or she is very concerned, that their personal content can be viewed by unwanted audiences. In our study, the Cronbach's Alpha was 0.891 indicating a good internal consistency.

3.2.3 Protective Online Privacy Behaviour

To measure protective online privacy behaviour, we split the construct into three variables; self-disclosure (SD), privacy protection (PP) and perceived privacy settings (PPS). Three items measured for privacy protection were adapted from the model Youn (2009) used in her study. The wording was modified for teenagers when necessary. Therefore, the privacy protection scale contains three items measured along a 5-point Likert-scale. High scores for each of the measures indicate that the respondent engages in privacy protecting behaviours, when dealing with privacy risks. An example of an item could be PP1 “I provide false information about myself”, a high score translates into the respondent frequently engaging in fabricating false information as a privacy-related risk-coping mechanism. In our study, the Cronbach's Alpha was 0.112.

For measuring self-disclosure, four items were adapted from Dwyer et al (2007). Two items were added by ourselves. Four items asked the respondent what type of personal information he or she publishes within Social Networking Sites (e.g. real name, address, photo), while the last two items asks, whether the respondent would chat and meet with strangers, whom they have met online. The scale was measured dichotomously with yes or no, this resulted in a score for each respondent from 1 till 6. In our study, the Cronbach's Alpha was 0.536.

For measuring privacy settings, we included one item asking respondents about the perceived level of their privacy settings within Social Networking Sites. The scale was along a 5-point Likert-scale. A high score would translate into the respondent perceiving his online privacy settings within SNS, e.g. Facebook, as high.

3.3 Descriptive Statistics

Table 1 shows the descriptive statistics of the sample in all five constructs, split up into male and female. Within this sample, there is a slight over-representation of women. Age is spread equally. The means for perceived settings are close to each other. However, one can note, that the means for concerns and disclosure differ from each other, stating that the female pupils were in general more concerned about their privacy and had less sensitive information about themselves disclosed on the internet, although they perceived their privacy settings at the same level that male pupils have, who in turn disclosed more sensitive information.

Table 1
Descriptive statistics of the sample

		N	Mean	Std. Deviation
Age	Male	157	14.54	1.99
	Female	178	14.27	2.06
	Total	335	14.40	2.03
Concerns	Male	155	2.67	1.05
	Female	182	3.23	1.20
	Total	337	2.95	1.13
Social Communication	Male	157	2.03	.64
	Female	182	2.30	.70
	Total	339	2.17	.67
Protection	Male	156	2.50	.60
	Female	178	2.80	.85
	Total	334	2.65	.73
Disclosure	Male	158	1.90	.79
	Female	182	.87	.56
	Total	340	1.39	.68
Perceived Settings	Male	152	3.32	1.10
	Female	176	3.38	1.10
	Total	328	3.35	1.10

3.4 Statistical Analysis

First, the frequencies for each items were calculated. A scale analysis delivered the measurement reliability levels for each item as indicated in 3.2 *Measurements*. The descriptive statistics including the mean and standard deviation were calculated for all five constructs in order to evaluate an even spreading across the sample.

Furthermore, a complete correlation table was conducted, in order to answer the sub-research questions 1 to 3. For the further analysis, we computed the three dimensions of online privacy behaviour into one measure, namely protective online privacy behaviour. This index now expresses the total extent of protective online privacy behaviour, giving each of the three concepts equal weight, ranging between zero and one. A high score on the index would translate into a high total online protective behaviour, meaning that the respondent does not disclose things he does not want others to abuse, lies about who he is and tends to perceive his privacy settings as high. For computing the index, first, the variable self-disclosure was recoded, so that all scores for 'no' translated into zero and all scores for 'yes' translated into one. The formula for the subsequent overall index was the following:

$$\text{Protective Online Privacy Behaviour} = (1 - \text{means}(\text{six items self-disclosure})/2 + \text{means}(\text{three items privacy protection})/5 + (\text{one item perceived privacy settings} - 1)/4)/3.$$

In order to answer the main research question and sub-question 4, as well as testing the hypotheses, a multiple regression analysis was conducted, to estimate the relationships among the variables. Regression analysis seeks to explain how the value of the dependent variable changes, when one of the independent does so. In our case, we can predict for example, how a change in protective online privacy behaviour is explained by changes in social communication. SPSS version 22 was used for all statistical analyses.

4. RESULTS

4.1 Correlations

We conducted a correlation analysis using *Pearson's r* to find out the strength of the relationships between all variables in the study. *Table 2* shows the full bivariate correlation table. Noteworthy correlations could be found between social communication and privacy concerns. There is a strong positive association between the two variables, $r = .354$ for males and $r = .257$ for females, both at $p = .000$. The relationship between privacy concerns and protection measures was significant for males with $r = .300$ and $p = .000$ and also for females, where the relationship was $r = .262$ and $p = .000$. Another noteworthy finding is, that privacy

concerns were significantly related to the level of self-disclosure only for males with $r = -.235$ and $p = .003$. For females, the correlation was not significant, with $r = -.035$ and $p = .635$. Furthermore, age was also significantly related to privacy concerns with $r = -.206$ and $p = .000$, social communication with $r = -.213$ and $p = .000$ and self-disclosure with $r = .309$ and $p = .000$.

Table 2 – Correlations

Gender			PC	SC	SD	PP	PPS	
Male	PC	Pearson's r	1	.354	-.235	.300	.073	
		Sig. (2-tailed)		.000*	.003*	.000*	.375	
		SC	Pearson's r		1	-.072	.255	.112
			Sig. (2-tailed)			.369	.001*	.171
			SD	Pearson's r			1	-.130
Sig. (2-tailed)						.105	.090	
PP	Pearson's r				1	.152		
Sig. (2-tailed)						.062		
PPS	Pearson's r						1	
Sig. (2-tailed)								
Female	PC	Pearson's r	1	.257	-.035	.262	.079	
		Sig. (2-tailed)		.000*	.635	.000*	.296	
		SC	Pearson's r		1	-.075	.398	.086
			Sig. (2-tailed)			.316	.000*	.257
			SD	Pearson's r			1	-.123
Sig. (2-tailed)						.102	.343	
PP	Pearson's r				1	.167		
Sig. (2-tailed)						.027**		
PPS	Pearson's r						1	
Sig. (2-tailed)								

		PC	SC	SD	PP	PPS
Age	Pearson's r	-.206	-.213	.309	-.050	.001
	Sig. (2-tailed)	.000*	.000*	.000*	.362	.987

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

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

To graphically show the strong positive correlation between the two variables social communication and privacy concerns for both genders together, we have produced a scatterplot diagram in SPSS version 22. Due to the large N, the mean privacy concerns were used. *Figure 2* shows the diagram: As the topic of digital privacy is discussed more often, the privacy related concerns increase.

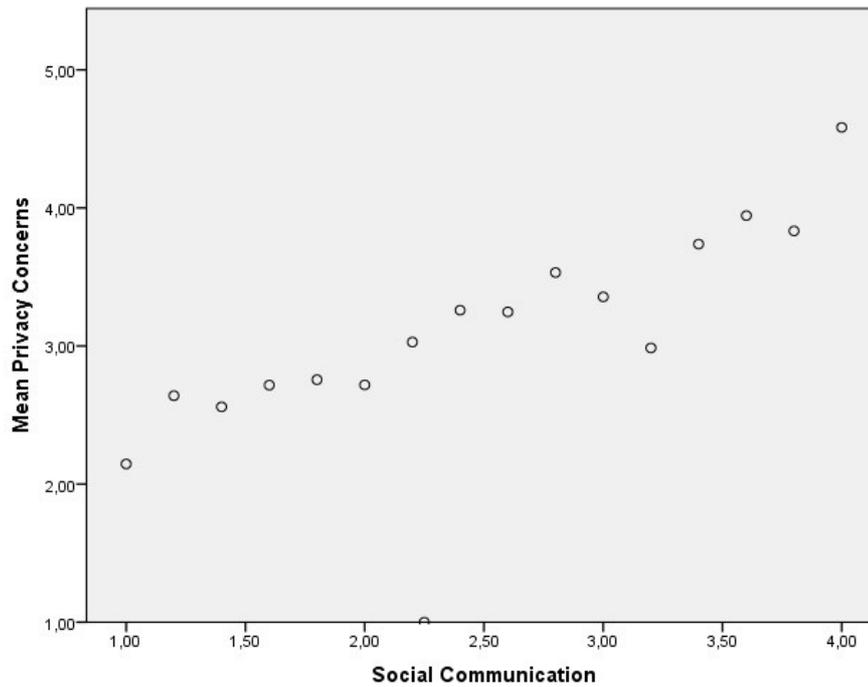


Figure 2 – Correlation Scatterplot – Social Communication vs. \bar{x} Privacy Concerns

4.2 Regression Analysis

4.2.1 Age/Gender vs. Social Communication

This section displays the results which answer the first research sub-question, namely in how far teenage girls and boys differ in the social communication about digital privacy risks. We conducted a regression analysis between age and gender, and social communication. As presented in the research model, age and gender are the dependent variables, while social communication is the independent variable. *Table 3* and *Table 4* show the results.

Table 3

Model Summary Regression Analysis – Age, Gender (IVs) vs. Social Communication (DV)

R	R Square	Adjusted R Square	Std. Error of the Estimate
.279	.078	.072	.655

Table 4

Coefficients Regression Analysis – Age, Gender (IVs) vs. Social Communication (DV)

	Standardized β	<i>t</i>	Sig.
(Constant)		9.55	.000
Gender	.180	3.406	.001
Age	-.200	-3.775	.000

From our analysis can be concluded that gender significantly predicts the social communication about digital privacy risks, $\beta = 0.180$, $t = 3.40$, $p < 0.001$, as does age, $\beta = -0.200$, $t = -3.775$, $p < 0.001$. Gender and age also explained a significant proportion of variance in social communication frequencies, $R^2 = 0.078$. Age and gender seem to account for 7,8% of the social communication variation. The coefficient for social communication is 0.180 for gender and -0.200 for age, so for every unit increase in gender (= females) and age, a 0.180 unit increase alternatively a -0.200 unit decrease in social communication is predicted, holding all other variables constant.

4.2.2 Gender/Age/Social Communication vs. Privacy Concerns

The research sub-questions 2 and 4 address how teenage boys and girls differ in privacy concerns and how age, gender and social communication impact these privacy concerns. In order to answer those questions and in line with our research model, we conducted a regression analysis with the variables gender, age and social communication as the dependent variable and the online privacy concerns as the independent variable. *Table 5* and *Table 6* show the results.

Table 5

Model Summary Regression Analysis – Gender, Age, Social Communication (IVs) vs. Privacy Concerns (DV)

R	R Square	Adjusted R Square	Std. Error of the Estimate
.400	.160	.153	1.063

Table 6

Coefficients Regression Analysis – Gender, Age, Social Communication (IVs) vs. Privacy Concerns (DV)

	Standardized β	t	Sig.
(Constant)		4.638	.000
Gender	.158	3.072	.002
Age	-.134	-2.584	.010
Social Communication	.284	5.400	.000

From the analysis can be concluded that all three dependent variables significantly predict online privacy concerns. Also, the interaction between age, gender and social communication explains a significant proportion of variance in digital privacy concerns, $R^2 = 0.16$. The dependent variables seem to account for 16% of the privacy concerns scores variation. The coefficient for gender is 0.158, $p < 0.001$, so for every unit increase in gender (=females), a

0.158 unit increase in privacy concerns is predicted. The coefficient for age is -0.134, $p < 0.005$, which translates into a -0.134 unit decrease in privacy concerns for every unit increase in age. Social communication had a coefficient of 0.284, $p < 0.001$, which translates into a 0.284 unit increase in privacy concerns for every unit increase in social communication. All effects are under the premise, that all other variables are held constant. Therefore can be concluded that age, gender and social communication all are significantly related to privacy concerns, with social communication having the strongest effect.

4.2.3 Social Communication/Privacy Concerns vs. Protective Online Privacy Behaviour

To answer the remaining parts of the main research and sub-questions, namely how social communication and digital privacy concerns relate to protective online privacy behaviour, we conducted a third regression analysis between social communication and privacy concerns as the independent variables and protective online privacy behaviour as the dependent. *Table 7* and *Table 8* indicate the results of the analysis.

Table 7

Model Summary Regression Analysis – Social Communication, Privacy Concerns (IVs) vs. Protective Online Privacy Behaviour (DV)

R	R Square	Adjusted R Square	Std. Error of the Estimate
.315	.099	.093	.11824

Table 8

Coefficients Regression Analysis – Social Communication, Privacy Concerns (IVs) vs. Protective Online Privacy Behaviour (DV)

	Standardized β	t	Sig.
(Constant)		20.971	.000
Social Communication	.215	3.853	.000
Privacy Concerns	.170	3.043	.003

From the analysis can be concluded, that both social communication, $\beta = 0.215$, $p < 0.001$, and privacy concerns, $\beta = 0.170$, $p < 0.005$, significantly predict the protective online privacy behaviour. With an $R^2 = 0.099$, the two dependent variables also explain a significant proportion of variance in protective online privacy behaviour scores. The R^2 value translates into 9,9% of the protective online behaviour variation, that social communication and privacy concerns account for. The coefficients translate into a 0.215 unit increase and a 0.170 unit increase of protective online privacy behaviour which is predicted per unit increase in either social communication or privacy concerns, with all other variables held constant.

5. CONCLUSION

5.1 Discussion

Table 9

Summary of hypotheses tests

Hypothesis	β	<i>p</i> -value	Support
H1. Social Communication → Privacy Concerns	.284	.000	Yes
H3a. (H2a, 2c, 2e) Privacy Concerns → Protective Online Privacy Behaviour	.170	.003	Yes
H3b. (H2b, 2d, 2f) Social Communication → Protective Online Privacy Behaviour	.215	.000	Yes
H4a. Age → Privacy Concerns	-.134	.010	No
H4b. Gender → Privacy Concerns	.158	.002	Yes
H5a. Age → Social Communication	-.200	.000	Yes
H5b. Gender → Social Communication	.180	.001	Yes

The objective of the study was to understand, in how far teenage boys and girls differ in communicating about the threats to digital privacy and how this is related to their subsequent digital privacy concerns and respectively their actual online privacy-related behaviour. These objectives were accomplished and all but one of the hypotheses were supported (see *Table 9*).

We predicted that frequently addressing topics related to digital privacy and the possible threats would lead to subsequent higher privacy concerns (H1). Most of all, because communicating about the threats and dangers of digital privacy could lead to the spreading of related concerns. Our hypothesis was confirmed, which is consistent with findings by studies who have linked “hearing about use or misuse of private information with increased levels of privacy concern” (Moscardelli & Divine, 2007, p. 246 ; Nowak & Phelps, 1992).

Regarding the protective online privacy behaviour, we predicted that both communicating about digital privacy as well as the subsequent privacy concerns influence the 'safe internet use' of teenage boys and girls (H3a, H3b). Consistent with findings from previous studies, which have linked privacy protection measures to privacy concerns for adult

consumers (Youn, 2009 ; Moscardelli & Divine, 2007) and stated, that a high level of online self-disclosure relates to privacy concerns in so far, as that detailed profiles are more prone to abuse (Krasnova et al, 2009), our hypothesis was confirmed. It appears that safe internet use, in terms of a low level of personal information self-disclosure and protectionist behaviour when tackling potential risks to privacy, is developed through communication about privacy risks and the subsequent privacy concerns.

The main aim of this study, which is also reflected in the four research sub-questions, was in how far boys and girls of different ages differ in their privacy concerns and their social communication about digital privacy. Based on prior literature concluding that adolescents were in general less concerned than young adults (Dhir et al, 2017 ; Feng et al, 2014), we predicted that privacy concerns should increase with age (H4a). The hypothesis was rejected. It appears that younger teenagers are more concerned, which could possibly be due to the fact, that they are newer to the digital sphere and are therefore less experienced with the risks and opportunities that SNS bear. Hypothesis 4b predicted that females are in general more concerned than males. The hypothesis was supported. These findings confirm similar results by Youn (2007) that links increased female concerns to females in nature being more prone to abuse, and Dhir et al (2017) that indicate males being less concerned while also having a higher level of self-disclosure. In our study, the mean disclosure for men was = 1.90 and for females = 0.87. Regarding age and social communication, we predicted, that younger teenagers should address topics of digital privacy more frequently than older ones (H5a). The hypothesis was not based upon previous literature, but one can assume that again, as younger teenagers are newer to the whole digital sphere and unknown to its dangers, that they therefore address digital privacy more often with their peers. H5b predicted, that females address the topic of digital privacy more often with their significant others. The hypothesis was supported and is in line with the results of Moscardelli & Divine (2007), who claim that females in general are more communicative than males.

Next to the research questions, which have been answered hypothesis by hypothesis, additional findings have been made with this study, some of which have been addressed in the introduction. The there mentioned 'privacy paradox', which has consistently been found in other studies (e.g. Dhir et al, 2017), states, that although internet users tend to disclose sensitive information about themselves, paradoxically they are aware about the possible risks and therefore have some degree of digital privacy concern. In this study, 34,7% of respondents that would chat with strangers are on the other hand *moderately to extremely concerned* about adults, that pretend to be someone else (e.g. of younger age) online. Such

finding supports the privacy paradox and shows, that the phenomena can also be observed in European middle-schools.

Also, as already mentioned under *3.3 Descriptive Statistics*, the means for concerns and disclosure differ significantly for males and females, indicating that females are in general more concerned about their privacy and have less sensitive information about themselves disclosed on the internet, while they perceive their privacy settings at the same level as males do, who in general disclose more information about themselves. This indicates a distorted image of how pupils perceive their privacy settings.

Another finding that has been made is the fear, that strangers can watch one through his webcam, being the most frequent mentioned concern, with 39,8% of the respondents being *extremely concerned* about the possibility. This finding differs somewhat from the expectation of *unwanted audiences* being able to view and post content to harm another as being the most frequent concern indicated by Krasnova et al (2009). Also, the previous identified concern about possible e-marketers using personal data for advertising in the study of Yao et al (2007) has not proved itself convincing in the course this study. Respondents' concern varied from 24% being *moderately concerned* and also 22,3% being *not at all concerned*.

5.2 Theoretical Implications

The present study has different theoretical implications for scholars. The current study findings contribute significantly to the interdisciplinary literature on social media and psychology. Also, the present findings complement the available findings from largely US scholars in US populations with insights from the European Union, particularly Germany. Similarly, the study results contribute to the erratic literature on age-gender differences in human-computer-interaction and fosters a deeper understanding of the interaction between social communication, privacy concerns and social media behaviour of the generation titled 'digital natives', as most previous studies have focussed on older age groups.

The study could be further improved in terms of reliability, by using a bigger sample in a different population. An interesting finding from this research is the mean for both male and female respondents for perceived privacy settings is ranging at *moderate*, while females tend to be more concerned (mean of 3.23). This indicates a somewhat distorted image of how privacy settings are perceived. A study on the relationship between privacy concerns, perceived privacy settings and the actual height of such settings could be an interesting topic for future research. Also, in line with the topic of the bachelor circle, future research could include other social conditions, which may cause certain categories of people to either give up

or protect their privacy. This study tried to include the three tiers of the German school system as the variable *educational level*, however, the data collection proved itself too complicated for the extent of this thesis.

This study used core assumptions of the Theory of Planned Behavior by Ajzen and Fishbein in its research model, which proved significant in predicting the protective online behavior. However, important variables of the theory were excluded, such as the normative beliefs and the control beliefs and perceived behavioral control, which further determine the intention towards specific behavior (Ajzen, 1991). Future research could investigate the determinants for privacy related online behavior by using the variables from this study and including the above mentioned from the Theory of Planned Behavior. As my colleague Mr. Vor dem Berge (2017) examined the impact of (perceived) technical proficiency on privacy concerns and online behavior, technical proficiency could be understood as the perceived behavioral control. Future studies could combine the measures from this study and from Vor dem Berge (2017) in order to test the Theory of Planned Behavior.

5.3 Practical Implications

As this study examined the privacy concerns, social communication and online privacy behavior of middle-school pupils in Germany, the practical implications that ensue address educators and policy makers whom focus on that age group. Especially in the light of rising problems such as cyber-bullying and online abuse, this study gives important insights, from which practitioners can start acting. This study has indicated, that communicating about possible threats to digital privacy can foster privacy related concerns and in that way lead to safer online behavior in terms of lower self-disclosure of personal information, a higher protective behavior and higher privacy settings. However, online privacy related education and the possibility to talk about digital privacy with teachers was mentioned the least frequent pattern in this study, with 62,8% of respondents *never* talking about digital privacy and its dangers with their teachers. Also, 61,4% *strongly disagreed* to *disagreed*, that they learn about digital privacy in the school and can address the topic with their teachers. Policy professionals focussing on education, as well as headmasters and teachers can use the insights from this study in order to amplify the importance of digital privacy at the stage of secondary education. A German example of how such actions could look like are the *Medienscouts*. It is a project financed by the State Institute for Media in North-Rhine-Westphalia and focuses on peer-to-peer imparting of media related competences (Landesanstalt für Medien Nordrhein-Westfalen, 2017). Pupils are educated regarding the risks and chances of social media and

privacy in the digital sphere and in turn, educate their fellows and peers. In line with the findings from this research, such projects could lead to the spreading of a privacy-related consciousness and thus safer internet use, minimizing the prominent abuses such as cyber-bullying and digital harassment. In line with the theory by Ajzen and Fishbein and from a theoretical stance, such educational projects would strengthen the normative beliefs that support the persuasive goal and also create a new subjective norm (Communication Institute for Online Scholarship, n.d.).

5.4 Limitations

A number of limitations persist within our research. Firstly, the reliance on self-reported data posed a major threat to our validity. This was amplified by the young ages of the participants. While conducting the survey it was clear, that some respondents did not take to study very serious and may have biased the responses. Also, some participants were very young and to some extent did not understand the questions, some simply did not use the internet. The study could be improved by using a bigger sample size, thus making the results more robust, as the respondents came from our social environment. The consistency of the sample proved as equally distributed in our study with age and gender spread equally. Furthermore, there is some amount of unexplained variance in the research model of this study, which is why future studies should take into consideration more variables that might influence privacy concerns and online behavior. The survey items to some extent reflected inaccurate measures and can be improved. Especially in terms of the Theory of Planned Behavior, the normative beliefs have to be addressed. Adding to that, the results from the reliability analysis were poor in our study. The Cronbach's alpha was acceptable for only the variable privacy concerns. However, one can argue, that the items in this study that were used for social communication and for protection behaviour were measured rather on an index than a scale. Computing a Cronbach's alpha for an index, which simply accumulates scores assigned to individual items (Crossman, 2017) would not prove appropriate.

6. REFERENCES

- Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*. 50(2), 179-211.
- Boult, A. (2016, September 16). Put Tape over your Webcam, FBI Director warns. Retrieved from: <https://telegraph.co.uk/technology/2016/09/15/put-tape-over-your-webcam-fbidirector-warns/>
- Communication Institute for Online Scholarship (n.d.). Theory of Reasoned Action. Retrieved from: http://www.cios.org/encyclopedia/persuasion/Gtheory_1reasoned.htm
- Crossman, A. (2017, April 19). The Differences Between Indexes and Scales. Retrieved from: <https://www.thoughtco.com/indexes-and-scales-3026544>
- Davis, K., & James, C. (2013). Tweens' conceptions of privacy online: implications for educators. *Learning, Media and Technology*. 38(1), 4-25.
- Dhir, A., Torsheim, T., Pallesen, S. & Adreassen, S. (2017). Do Online Privacy Concerns Predict Selfie Behaviour among Adolescents, Young Adults and Adults? *Frontiers in Psychology*. (8), 815.
- Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviours. *European Journal of Social Psychology*. (45), 285-297.
- Dingli, A., & Seychell, D. (2015). The new digital natives : Cutting the chord. *Heidelberg: Springer*
- Dwyer, C., Hiltz, S. R. & Passerini, K. (2007). Trust and privacy concern within social networking sites. *AMCIS 2007 Proceedings*. (p. Paper 339).
- Feng, Y., & Xie, W. (2014). Teens' concern for privacy when using social networking sites: an analysis of socialization agents and relationships with privacy protecting behaviors. *Comput. Hum. Behav.* 33, 153–162.
- Krasnova, H., Günther, O., Spiekermann, S. & Koroleva, K. (2009). Privacy concerns and identity in online social networks. *Identity in the Information Society*. (2), 39-63.
- Landesanstalt für Medien Nordrhein-Westfalen (2017). Medienscouts NRW. Retrieved from: <http://www.lfm-nrw.de/foerderung/medienkompetenz/projekte-materialien/medienubergreifend/medienscouts-nrw.html>
- Madden, M., Lenhart, A., Cortesi, S., Gasser, U., Duggan, M., Smith, A. & Beaton, M. (2013). Teens, Social Media, and Privacy. *Pew Research Center*.

- Moscardelli, D. M. & 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) 232–252.
- Nowak, G. J. & Phelps, J. (1992). Understanding privacy concerns. An assessment of consumers' information-related knowledge and beliefs. *Journal of Direct Marketing*. (6), 28-39.
- Patchin, J. (2016, November 26). Summary of Cyberbullying Reserch (2004-2016). Retrieved from: <https://cyberbullying.org/summary-of-our-cyberbullying-research>
- Read, P., S-O'Brien, L., Woolcott, J., & Shah, C. (2011). Understanding privacy behaviors of millennials within social networking sites. *Proceedings of the American Society for Information Science and Technology*. 48(1), 1-10.
- Tjiptono, F., Arli, D. & Viviea (2016). Gender and digital privacy: examining determinants of attitude toward digital piracy among youths in an emerging market. *International Journal of Consumer Studies*. 40, 168–178.
- University of Twente (2017, February 27). Theory of Planned Behavior/ Reasoned Action. Retrieved from: [https://utwente.nl/en/bms/communication-theories/sorted-by-cluster/Health Communication/theory_planned_behavior/](https://utwente.nl/en/bms/communication-theories/sorted-by-cluster/Health%20Communication/theory_planned_behavior/)
- Yao, M. Z., Rice, R. E., & Wallis, K. (2007). Predicting user concerns about online privacy. *Journal of the American Society for Information Science and Technology*. 58(5), 710-722.
- Youn, S. (2008). Parental Influence and Teens' Attitude toward Online Privacy Protection. *Journal of Consumer Affairs*. 42(3), 362-388.
- 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. APPENDIX

7.1 Survey items (translated from German; language adjusted for younger audience)

Demographics

GEN: I am a...

- Boy
- Girl

AGE: I am ... years old

EDU: Currently I'm visiting...

- Hauptschule
- Realschule
- Gymnasium

Usage

USE: Per week I spend ca. ... hours on Instagram, YouTube, Facebook, Snapchat, etc.

Social Communication

SC1: How often do you talk about privacy in the internet and the possible threats with your parents?

SC2: How often do you talk about privacy in the internet and the possible threats with your friends?

SC3: How often do you talk about privacy in the internet and the possible threats with your teachers?

SC4: My parents tell me, how to behave online.

SC5: Cyber-bullying and other threats in the internet are a big topic in my circle of friends.

SC6: In the school we can learn and talk about digital privacy.

Privacy Concerns

PC1: How concerned are you, that unwanted persons can view online content about you (e.g. teachers, parents, fellow pupils, possible future employers)?

PC2: How concerned are you, that pictures of you are published without your permission?

PC3: How concerned are you, that you are being humiliated online (cyber-bullying)?

PC4: How concerned are you, that your personal data is being used for advertising?

PC5: How concerned are you, that strangers can watch you through your webcam?

PC6: How concerned are you, that adults pretend to be someone else (e.g. of your age)?

Self-Disclosure

SD1: Would you publish a picture of yourself? (Dwyer, 2007)

SD2: Would you publish your private phone number? (Dwyer, 2007)

SD3: Would you publish your private address (including email)? (Dwyer, 2007)

SD4: Would you publish your real name? (Dwyer, 2007)

SD5: Would you chat with strangers?

SD6: Would you meet up with someone, you met online?

Privacy Protection

PP1: When a website or service (whatsapp, snapchat, instagram, google, etc.) asks too personal information, then I provide false information. (Modified from Youn, 2009)

PP2: When a website or service (whatsapp, snapchat, instagram, google, etc.) asks too personal information, then ask friends/parents/teachers for help. (Modified from Youn, 2009)

PP3: When a website or service (whatsapp, snapchat, instagram, google, etc.) asks too personal information, then I search for alternative sites, that don't ask for such information. (Modified from Youn, 2009)

Perceived Privacy Settings

PS1: I think that my privacy settings on the internet are generally...

- low
- rather low
- medium
- rather high
- high