Security and Privacy Perceptions of Millennials (18-24) and Non-Millennials (36-50) on Facebook

Stanislav van den Braber
University of Twente
P.O. Box 217, 7500AE Enschede
The Netherlands

ABSTRACT
Being socially active online is something most Millennials find themselves doing as they move towards adulthood. The non-Millennials today adapt more and more to this trend of being socially active online. The rising amount of data generated from social media´s, also labelled as big data, could result in new issues regarding privacy and security. The potential privacy and security risks of social networking sites (SNS) are often underestimated. Not a lot is understood of the privacy and security perceptions on Facebook in particular. This paper tries to examine whether there is a significant difference in perception between members of the 'net-generation' and non-members. Furthermore, the aim is to provide insight into the relationship between the privacy/security perceptions of the two age groups and their social media behavior. This study examines security, trust and privacy concerns with regard to Facebook. To do so, we conducted a survey-based study, in which we questioned two specific age groups.

Supervisors: I. Singaram & DR. A. H. van Reekum

Keywords
perceived privacy, perceived security, millennials, Facebook, social media behavior, social networking sites (SNS)

7th IBA Bachelor Thesis Conference, July 1st, 2016, Enschede, The Netherlands.

1. INTRODUCTION

Online Social Networking Sites (SNS), such as MySpace, Facebook, and Twitter, have experienced exponential growth in membership in recent years.[1] In April 2016, the website of Facebook was visited approximately 139 million times in the United States, and listed as number 3 of most visited sites in the US.[2] These numbers illustrate the rising popularity of Facebook as a SNS. The amount of time people spend on interacting with social networking sites nowadays is enormous. Now more and more people are connected by SNS, their drawbacks are receiving more attention as well. The quantities of personal information revealed on the internet are increasing tremendously. While users want to communicate and present themselves to others online, many are becoming increasingly vigilant with regard to the information they disclose.[3]

For the end-users, privacy and security issues have emerged in the environment of SNS. A security issue occurs when a hacker gains unauthorized access to a site's protected coding or written language.[4] Privacy issues, those involving unwarranted access of private information, do not necessarily involve security breaches. Information disclosure is a vital part of the identity of Facebook. On Facebook users reveal their personal information, post their experiences, share news, and post photos. For business purposes it is not strange that Facebook will use this information to remain sustainable towards the future. User-provided content is an important determinant of Facebook's commercial success.[5] Due to the media, people became aware of the privacy threats users face with Facebook. Together with the rising popularity of Facebook in particular, the privacy concerns will get more and more attention in the upcoming years. On the other hand, Facebook recently provided privacy settings for the end-users. Nevertheless, SNS and its technologies are relatively new, and it is not surprising that people have difficulties with managing their privacy settings correctly. If the privacy settings are experienced as too difficult and the end-user is aware of privacy and security concerns regarding Facebook, the end-user will probably interact and share less on Facebook.

However, despite the importance of the developments for the SNS' business and public value, researchers know little about the privacy concerns of end-users and how those concerns impact users' self-representation and self-disclosure strategies.[6] Therefore, in this study we would like to investigate whether perceived privacy and security of a Facebook user has influence on its online social behavior. Furthermore, the second aim of this study is to investigate whether there are differences in perception between members of the net-generation (18-24) and non-members (35-50). In this study, members of the net-generation are also referred to as millennials.[7] Since the millennials grew up within the digital environment of today, the perceptions of millennials regarding privacy and security could differ from the non-millennials, who had to adapt in a later stage of their lives to the digital world. The non-millennials could be more cautious towards sharing personal information on Facebook, because the online technologies are new for them and perhaps they do not know the specific consequences of their actions online. When exploring the relationship between perceived privacy and security, and the differences in perception of the two age groups, the paper addresses the following research questions:

RQ: What effect has age on privacy and security perceptions in Facebook, and how do these perceptions affect their online behavior on Facebook?

SubQ: To what extent do millennials (18-24) and non-millennials (35-50) have different perceptions on privacy and security?

We start with discussing the prior research on privacy and security concerns in the SNS environment, and prior research regarding social media behavior. Then, we present our methodology, including a description of the survey we conducted and explaining the measured items. In the next section, we present the data on the privacy and security perceptions, and how these perceptions influence the users' social media behavior. We conclude by discussing comparisons on privacy and security perceptions between millennials and non-millennials. In addition, the discussion continues with the relationship between perceptions and behavior on Facebook. Based on our results, we suggest that online businesses should be careful with the perceptions of their customers, since these are essential for the company's survival in the digital world. Furthermore, the age differences are not that important, since nearly everyone is attached to their privacy and security online regardless of their age.

2. THEORETICAL FRAMEWORK

2.1 Perceived Privacy in SNS

Facebook and other SNS sites offer a large amount benefits to the end-users. However, due to its immense popularity, the shortcomings of Facebook have come to light. One of the shortcomings that has come to light is the concern of end-users regarding privacy. These rising privacy concerns have started to compel users to reconsider their approach to self-disclosure on SNS sites.

Krasnova et al. (2009) identified in her study several categories of privacy concerns related to the end-users.[8] The most frequently mentioned concern, was that unwanted audiences view their shared content, where unwanted audiences included future employees, supervisors, family members, peers and subordinates. Organizational threats related to the collection and use of the big data by the SNS and third parties is one of the privacy concerns. Furthermore, concerns regarding social threats are mentioned, including people who post content to harm another individual on purpose. These are all privacy concerns Facebook users are facing today.

Christofides et al. (2012) addresses the gap, since Facebook and other social networking sites are environments where high levels of self-disclosure are normalized, it will be important to learn about privacy knowledge and behavior over time and across various age groups.[9] The interesting issue is whether age has an influence on privacy perceptions. On the one hand, we have the millennials who grew up within the 'net-generation', on the other hand, there are the non-millennials who had to adapt in a later stage of their lives to the internet technologies. Would they have different privacy perceptions due to their age? Privacy for

[1] (Barker, 2009)
[2] (Quantcast, 2016)
[3] (Krasnova, Günther, Spiekermann, & Koroleva, 2009)
[4] (Shin, 2010)
[5] (Krasnova, Günther, Spiekermann, & Koroleva, 2009)
[6] (Krasnova, Günther, Spiekermann, & Koroleva, 2009)
[7] (Palfrey & Gasser, 2008)
[8] (Krasnova, Günther, Spiekermann, & Koroleva, 2009)
[9] (Christofides, Muise, & Desmarais, 2012)

teenagers is very important and they especially have privacy concerns about parents viewing their intimate life details.[10] Nevertheless, non-millennials could have similar concerns with regard to family members, employers, friends, etc. Both age groups have unwanted audiences, but different groups of people. Chung et al. (2010) found out in their study that younger and older adults were not different in their degrees of concern about privacy issues within online communities.[11] It may not be the case that the millennials do not value privacy, but the concept has evolved to reflect generational differences.[12] Millennials do not have to be careless in protecting their personal information online, this could be our way of conventional thinking. Based on these findings from previous studies, we hypothesize the following:

H1. Millennials and non-millennials do not have different privacy perceptions on Facebook.

Furthermore, another aim in this study is to investigate whether privacy and security perceptions affect behavior on Facebook. Tufekci conducted research on the relationship between a users' privacy concerns and their information disclosure on a SNS.[13] Eventually, the author found no relationship between the two. Even users who indicated to have many privacy concerns, revealed large amounts of personal information on their SNS profile. Nevertheless, behavior on Facebook is not only measured in terms of self-disclosure. There are more factors that play a role in determining someone's behavior on Facebook.

2.2 Perceived Security in SNS

Perceived privacy and security are often confused. Much of the current debate over privacy involves a subset of privacy in general, namely data privacy. As a result, many discussions over data privacy raise the issue of security, which often means information security.[14] To clarify, we defined privacy and security issues earlier.

Companies managing the social networking sites are engaged in lots of interactions, but less focused on privacy and security and more focused on marketing purposes.[15] This is a common opinion which is probably widely shared by a lot of users. Therefore, social networking sites have been criticized because users lack trust in the site's security.[16] Nevertheless, protecting the privacy of the users is important for SNS providers to increase information security and prevent privacy invasion, and therefore to retain customers.[17]

The two opinions develop in a debate on to what degree the SNS providers are protecting the users' privacy and security. However, it can be said that individuals' perceptions of security can differ from real security levels. This feeling of security is largely determined by the feeling of control a user has in a social networking site.[18] The difference between perceived control and actual control is important to note, since perceived control has a direct impact on behavior and the feeling of security is determined the feeling of control. Prior studies have shown that perceived control affects human behavior more than actual control.[19] Furthermore, little research has examined age differences in the users' perceptions of security issues. However, similar to perceived privacy we can say that millennials are not careless in protecting their personal information, and therefore we hypothesize the following:

H2. Millennials and non-millennials do not have different security perceptions on Facebook.

2.3 Social Media Behavior

Based on the model of (Shin, 2010) we decided to include the constructs trust and attitude in our research model to measure behavior on Facebook. A person's performance of a specified behavior is determined by his or her behavioral intention to perform the behavior, and behavioral intention is jointly determined by the person's attitudes and subjective norms.[20] The constructs attitude and trust are therefore confirmed to be

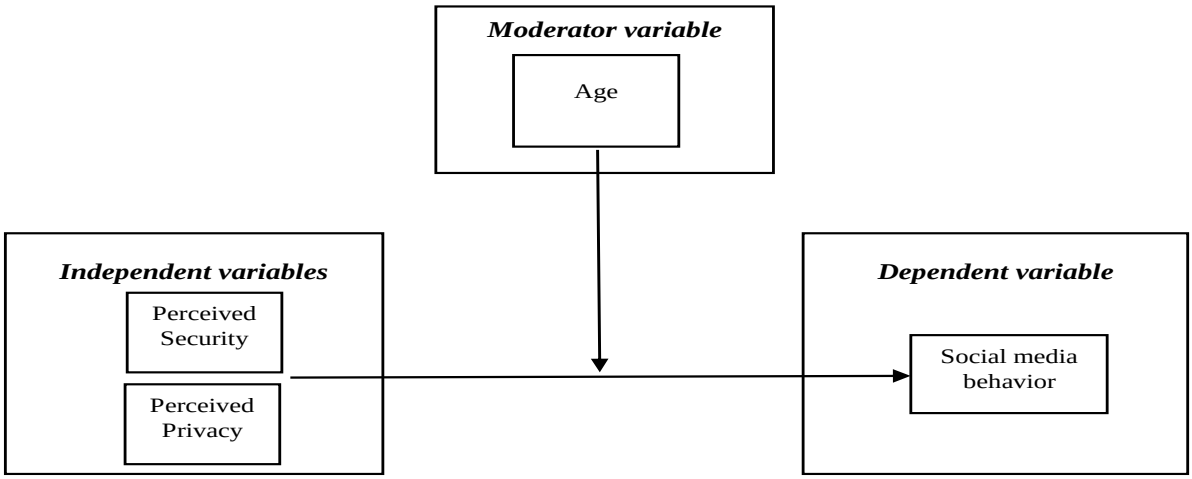

Figure 1 - Research Model

[10] (Livingstone, 2008)
[11] (Chung, Park, Wang, Fulk, & Mclaughlin, 2010)
[12] (Raynes-Goldie, 2010)
[13] (Tufekci, 2008)
[14] (Shin, 2010)
[15] (Lawler, Molluzzo, & Doshi, 2012)
[16] (Dwyer, Hiltz, & Passerini, 2007)
[17] (Hajli & Lin, 2014)
[18] (Kim & Shin, 2008)
[19] (Skinner, 1996)
[20] (Ajzen & Fishbein, 1980)

important measures for a person's behavior. In addition, we included a third construct self-disclosure, which measures the extent to which people reveal personal information on their Facebook page.

Together with the rising popularity of the internet technologies, *trust* becomes a vital part for online businesses. Trust has taken a central role in the SNS business. The higher the customers' trust in the web, the less effort customers will exert to scrutinize details of the site to assess its authenticity of services.[21] In a case where trust is perceived as high, the person would reveal more private information on the SNS, because it reduces the risks involved.[22] That makes trust a precondition for self-disclosure. Previous research on trust and behavior indicates that trust plays an important role in determining a person's actual behavior.[23] High perceived privacy and security would logically link to high trust, and therefore we hypothesize the following:

H3. Perceived privacy and security positively affects users' trust in Facebook.

Attitude towards a behavior is defined as an individual's positive or negative feeling about performing the target behavior.[24] A higher perception of information control generates a more positive attitude towards the SNS, as SNS user will be less worried about data collection when they share their personal information on the SNS.[25] Translating this to Facebook and our study, when a person has high privacy/security perceptions it automatically results in positive attitude towards Facebook. Since the relationship between attitude and perceptions is not that complicated, we hypothesized the following:

H4. Perceived privacy and security positively affects users' attitude towards Facebook.

In our opinion, *self-disclosure* is an essential measure for behavior on Facebook. Self-disclosure measures the extent to which a person reveals personal information on Facebook. As identified earlier by Krasnova et al., perceived privacy risk has been a critical barrier for users to disclose personal information on SNS.[26] The users' personal information can be easily collected, distributed, and used without consents. It makes therefore sense high privacy and security risks will impact their willingness to share private information on Facebook. This makes us hypothesize the following:

H5. Perceived privacy and security positively affects users' willingness to disclose personal information on Facebook.

In our research model, the variable age is the moderator between perceptions and behavior. Eventually, we want to know whether age has an impact in that certain relationship. Haji and Lin (2014) examined information sharing behavior on SNS, and applied age as a control variable, they found out that their results were robust after controlling for age, computer experience, and experience for using SNS.[27] None of these variables impacts SNS continuance intention to share information. Therefore, we hypothesized the following:

H6. The interaction between age and perceptions has no impact on the behavior constructs; trust, attitude and self-disclosure.

3. METHODOLGY

3.1 Participants and Procedures

To improve our initial survey, a small pre-test was conducted. We asked some relatives to enroll in the survey on multiple devices. After they completed the survey, we asked the respondents if they have encountered any difficulties. Feedback from the respondents was used to create the final questionnaire. In the final survey, respondents were asked to rate each statement on a 7-point Likert scale, where one meant *strongly disagree* and, four meant *neutral*, and seven meant *strongly agree*. At first, 349 people participated in our survey. After straight lining and eliminating the biased responses a total of 337 responses were considered usable for our research. In addition, regarding the subgroups, 165 millennials (18-24) and 51 non-millennials (36-50) responded sincerely. The final sample for the data analysis consisted of 58.5% females and 41.5% males, where the mean age of the sample was 33 years old. The vast majority of the participants are Dutch, representing over 85% of the total sample. The level of education among the respondents ranges from high school to advanced graduate work. 97% of all participants said that they check Facebook at least once a day. SPSS 22.0 is used for the analysis of a descriptive statistics.

3.2 Measurements

For this study a 7-point Likert scale is used for all measures except for the demographic measures, usage measures and the self-disclosure measures, At the end of the survey an open optional question is included for the participant to note his/her negative experiences with Facebook. Most of the measures are based upon previously validated studies and are therefore considered reliable.

3.2.1 Perceived Privacy

The items measured for perceived privacy were adapted from the model (Shin, 2010) used in his study.[28] The perceived privacy scale contains four items measured along a 7-point Likert-scale. High scores for these four items indicates that the respondent perceives Facebook as a privacy protecting platform. For example, when a respondent indicates a high score for the item PP3 "I am not concerned that the information I submitted on Facebook could be misused" he or she is not concerned that Facebook will misuse the information provided. In the original study, the Cronbach's Alpha was 0.8872.

[21] (Shin, 2010)
[22] (Metzger, 2004)
[23] (Shin, 2010)
[24] (Ajzen & Fishbein, 1980)
[25] (Hajli & Lin, 2014)
[26] (Krasnova, Günther, Spiekermann, & Koroleva, 2009)
[27] (Hajli & Lin, 2014)
[28] (Shin, 2010)

3.2.2 Perceived Security

The items measured for perceived security were adapted from the model (Yenisey et al., 2005) used in their study.[29] The perceived security scale contains five items measured along a 7-point Likert-scale. High scores for the first two items indicate that the respondent perceived Facebook as a security protecting platform. High scores for the last three items indicate that the respondent perceives Facebook not as a security protecting platform. For analysis later on in SPSS we will shift the values from the last three items in order to make a consistent score. An example item could be PS2 "I am confident that the private information I provide with Facebook will be secured.", here a high score indicates that the respondent feels secure with Facebook. In the original study, the Cronbach's Alpha was 0.9311.

3.2.3 Behavior on Facebook

To measure behavior on Facebook we split the construct into three variables; attitude, trust and self-disclosure. Three items measured for a*ttitude* were adapted from the model (Shin, 2010) used in his study.[30] One item to measure attitude was added by ourselves. Therefore, the attitude scale contains four items measured along a 7-point Likert-scale. High scores for the first three items indicate that the respondent has a positive attitude towards Facebook. A high score for the last item indicate that the respondent has a negative attitude towards Facebook. Later on in the data analysis with SPSS, we shift the values from the last item in order to make the score consistent. An example of an item could be AT3 "Facebook has become part of my daily routine", where a high score translates into a positive attitude towards Facebook. In the original study, the Cronbach's Alpha was 0.8289, where in our study the Cronbach's Alpha was 0.589.

Three items measured for *trust* were adapted from the model (Fogel & Nehmad, 2009) used in their study.[31] One item to measure trust was added ourselves. Therefore, the trust scale contains four items measured along a 7-point Likert-scale. High scores for these four items indicate that the respondent sees Facebook as a trustworthy platform. For example the item TR3 "Facebook can be relied on to keep its promises", a high score translates into high trust in Facebook. In the original study, the Cronbach's Alpha was 0.8873, where in our study it was 0.524.

The item measured for *self-disclosure* was adapted from (Dwyer et al., 2007) in their study on trust and privacy concerns in social networking sites.[32] The item asked the respondent what types of personal information they disclose on their own Facebook profile (e.g. real name, hometown, phone number, relationship status, etc.). The item consisted of 11 options and this resulted in a score for every respondent from 1 till 11.

3.3 Statistical Analysis

The descriptive statistics were calculated for all 5 constructs including the mean and standard deviation given for both age groups. Next, an ANOVA test was conducted comparing the means of the millennials to non-millennials regarding privacy and security perceptions. The ANOVA test is used to analyze the differences among group means, and its procedures like variation among and between groups. Therefore, in our sample we compare two age groups and the ANOVA is suitable, since it provides us a statistical test of whether or not the means are equal. In addition, an ANOVA test was performed comparing the means of millennials to non-millennials for the control variables; gender, nationality, education and the dependent variables; trust, attitude, and self-disclosure. First, we performed an ANOVA for the control variables to see whether the genders, nationalities and levels of education are spread equally among the two age groups. In the case where they are spread equally, we can say that we have more representative samples comparing to each other, and therefore a more robust analysis. Second, we performed the ANOVA for the dependent variables of the study as well to find out if there are some noteworthy results between the age groups. Furthermore, a complete correlation table was conducted for both continuous and ordinal variables. For the continuous variables Pearson's correlation was used, and for the ordinal variables Spearman's Rho. In order to answer the second part of the research question on how the perceptions influence the online behavior, we conducted several regression analyses. Regression analysis estimates the relationships among variables. Moreover, regression analysis explains how the value of the dependent variable changes when one of the independent variables varies. In our case, we can predict how one unit of the behavior variables is explained by the changes in the perception variables. Therefore, we can properly estimate the relationship between the privacy and security perceptions and the behavior variables. Lastly, to measure the impact of age as a moderator in the relationship between perceptions and behavior, we created a new variable; age multiplied by perception score. With this variable we conducted a new regression analysis between this variable and the dependent behavior variables. With the results from this analysis we can see what the impact is of age in this relationship. SPSS version 22 was used for all statistical analyses.

4. RESULTS

4.1 Descriptive Statistics

Table 1 shows the descriptive statistics of the millennials (18-24) and non-millennials (36-50) in all five constructs. Within this sample there is a slight overrepresentation of women, where women represented 2/3 of the sample against 1/3 men. The means for the first three constructs perceived privacy, security and attitude are close to each other. However, one can note that the means for trust and self-disclosure are quite far from each other. Furthermore, a striking finding here is that the standard deviation for self-disclosure is large, on the other hand, one has to take into account that the scores for self-disclosure range till eleven.

[29] (Yenisey et al., 2005)
[30] (Shin, 2010)
[31] (Fogel & Nehmad, 2009)
[32] (Dwyer, Hiltz, & Passerini, 2007)

Table 1

Descriptive statistics of the sample, with the millennials as a randomized sample

		N	Mean	Std. Deviation
Perceived Privacy	Millennials	51	3,48	,87
	Non-Millennials	51	3,19	,96
	Total	102	3,33	,92
Perceived Security	Millennials	51	4,44	,92
	Non-Millennials	51	4,18	,87
	Total	102	4,31	,90
Attitude	Millennials	51	4,99	,79
	Non-Millennials	51	4,92	1,17
	Total	102	4,95	,99
Trust	Millennials	51	4,23	,95
	Non-Millennials	51	3,5	1,16
	Total	102	3,87	1,11
Self-Disclosure	Millennials	51	6,27	2,16
	Non-Millennials	51	4,90	1,93
	Total	102	5,59	2,15

4.2 Comparisons Millennials vs. Non-Millennials (ANOVA)

One aim of this study was to find out if age has an effect on privacy and security perceptions. In other words, whether there are differences in privacy and security perceptions between millennials (18-24) and non-millennials (36-50). We approached this by conducting an ANOVA test comparing the means of both age groups. *Table 2* shows the results from the different ANOVA analyses. Furthermore, we conducted several ANOVA tests for the control and dependent variables as well.

4.2.1 Control Variables (Model 1)

Model 1 takes into account the comparisons for the control variables education, gender, and nationality between millennials and non-millennials. For *education* applies the higher the score, the more educated the respondent is. One would expect a significant difference between millennials and non-millennials in terms of education. However, the ANOVA result shows that there is just no significant difference. For *gender* we measure if there is a significant difference between the spread of men and women over the two age groups. The millennials group consists of 25 men and 26 women, on the other hand the non-millennials group consists of 9 men and 42 women. From the analysis we can conclude that there is a difference between the two age groups with a corresponding p-value of 0.001. This indicates that there is an unequal spread of men and women over the two age groups. Lastly, for *nationality* there were three options, namely 1 for Dutch, a 2 for German, and a 3 for other nationality. Therefore, for nationality we measure if there is a significant difference between the spread of different nationalities over the two age groups. The millennials group consists of 47 Dutchmen, 1 German, and 1 other nationality. The non-millennials group consists of 42 Dutchmen, 2 Germans, and 7 other nationalities. From the ANOVA can be concluded that the spread over the two age groups is roughly equal.

Table 2

Analysis of Variances (ANOVA) results – comparing the means of millennials to non-millennials

	Model 1 (F-value (Sig.))	**Model 2 (F-value (Sig.))**	**Model 3 (F-value (Sig.))**
Control variables			
Education	3.66(0.06)	3.66(0.06)	3.66 (0.06)
Gender	12.45(0.00)*	12.45(0.00)*	12.45(0.00)*
Nationality	2.15 (0.15)	2.15 (0.15)	2.15 (0.15)
Independent variables			
Privacy Perceptions		2.54 (0.11)	2.54 (0.11)
Security Perceptions		2.12 (0.15)	2.12 (0.15)
Dependent variables			
Attitude			0.10 (0.75)
Trust			11.98(0.00)*
Self-Disclosure			11.42(0.00)*

4.2.2 Independent Variables (Model 2)

In this section we test our earlier stated hypotheses regarding the effect of age on privacy and security perceptions. *Table 2* shows the results of the comparisons for privacy and security perceptions between millennials and non-millennials. We stated earlier in our hypotheses that we expect age to have no effect on privacy and security perceptions. For *privacy perceptions*, millennials have a slightly greater mean (3.48) than the non-millennials (3.19). Both scores are below the neutral score of 4, which indicates that both age groups tend to have low/moderate privacy perceptions on Facebook. However, from the ANOVA test we can conclude that there is no significant difference between the means of the millennials (3.48) and the non-millennials (3.19). The F-statistic (2.535) is large, the corresponding p-value is large as well (0.114), and higher than the alpha (0.05). There is not a significant effect of age on privacy perceptions at the $P<.05$ level for the three conditions [$[F\ 1,100] = 2.535$, $P = 0.114$]. This indicates that millennials and non-millennials perceive Facebook at the same level regarding privacy protection. For *security perceptions*, millennials again have a slightly greater mean (4.44) than the non-millennials (4.18). Both scores are a little above neutral, which indicates that both age groups tend to have a moderate feeling towards Facebook and security. From the ANOVA test we can conclude that there is no significant difference between the means of the millennials (4.44) and the non-millennials (4.18). The F-statistic (2.12) is small and the corresponding p-value is large (0.148), and higher than the alpha (0.05). There was not a significant effect of age on security perceptions at the $P<.05$ level for the three conditions [$[F1,100] = 2.12$, $P = 0.148$]. This indicates that millennials and non-millennials perceive Facebook at the same level regarding security.

4.2.3 Dependent Variables (Model 3)

Model 3 analyzes the comparisons for the dependent variables trust, attitude and self-disclosure between millennials and non-millennials. *Table 2* shows that we found significant differences between the age groups for the variables *trust* and *self-disclosure*. First, for trust, millennials have a significantly greater mean (4.23) than the non-millennials do (3.5). Both scores are around the neutral score of 4. This indicates that the respondents have a moderate trust with regard to Facebook. The F-statistic (11.979) is large and the corresponding p-value is small (0.001), and lower than the alpha (0.05). Therefore, there is a significant effect of age on trust at the P<.05 level for the three conditions [[F1,100] = 11.979, P = 0.001]. Furthermore, for the variable self-disclosure, millennials have a significantly greater mean (6.27) than the non-millennials (4.9). This result shows that millennials are likely to reveal more personal information on their Facebook page than non-millennials. The F-statistic (11.42) is large and the corresponding p-value is small (0.001), and lower than the alpha (0.05). Therefore, there is a significant effect of age on self-disclosure at the P<.05 level for the three conditions [[F1,100] = 11.42, P = 0.001]. For the variable a*ttitude*, we did not find a significant relationship.

4.3 Correlations

We conducted a correlation analysis to find out the strength of the relationships between all variables in the study. In *Appendix A* one can find the correlation table for the continuous variables in the study. In *Appendix B* one can find the correlation table for the ordinal variables. The most noteworthy result is the significant association between perceived privacy and security. There is a strong positive association between the two variables, r = 0.225 and p = 0.023. This indicates that the strength of the relationship is strong. Since these two variables are both independent, to avoid multicollinearity problems later on in the regression analysis, we decided to create a new variable which takes into account both perception scores. Furthermore, another interesting result is the fact that all variables have a significant correlation with trust except for self-disclosure. The ordinal variables are analyzed with the Spearman's Rho function. Here, gender and nationality are positively correlated.

4.4 Regression Analysis

4.4.1 Privacy/Security Perceptions vs. Facebook Behavior

This section displays the results which answer part of the research question, namely to find out if these privacy and security perceptions affect Facebook behavior. We conducted a regression analysis between privacy and security perceptions, now merged into one variable due to multicollinearity problems, and trust, attitude and self-disclosure, which represent Facebook behavior. As presented in our research model, privacy and security perceptions is the independent variable, and the remaining three are the dependent variables.

Table 3

Model summary Regression Analysis – Perceptions vs. Behavior

Dependent variable	R	R Square	Adjusted R Square	Std. Error of the Estimate
Trust	,37[a]	,14	,13	1,04
Attitude	,18[a]	,03	,02	,99
Self-Disclosure	,02[a]	,000	-,01	2,16

a. Predictors: (Constant), Perceived Privacy + Security

Table 4

Coefficients Regression Analysis – Perceptions vs. Behavior

		Unstan. B	t	Sig.
Trust	(Constant)	1,68	2,98	,00
	PP + PS	,57	3,95	,00*
Attitude	(Constant)	4,0	7,49	,00
	PP + PS	,25	1,83	,07
Self-Disclosure	(Constant)	5,38	4,59	,00
	PP + PS	,06	,18	,86

From our analysis can be concluded that privacy and security perceptions significantly predicts trust scores, $\beta = 0.573$, $t(101) = 3.95$, $p < 0.001$. Privacy and security perceptions also explained a significant proportion of variance and in trust scores, $R^2 = 0.135$, $F(1,101) = 15.6$, $p < 0.001$. The privacy and security perceptions seems to account for 13.5% of the trust scores variation. The coefficient for the trust score is 0.573, so for every unit increase in trust score, a 0.573 unit increase in privacy and security perceptions is predicted, holding all the other variables constant. The other two variables, attitude and self-disclosure, are not significantly related to perceptions according to our analysis. Therefore, perceptions predicts one out of the total three behavior variables.

4.4.2 The Interaction of Age on Perceptions and Behavior

The last part of the research question was how age has an impact on perceptions, and therefore how age has an impact on Facebook behavior. In order to find out what the interaction of age is in our research model, we created a new variable in SPSS where we multiplied the merged perception score by the age of the respondent. With this variable, we conducted a regression analysis with the other Facebook behavior variables; trust, attitude and self-disclosure.

Table 5

Model Summary Regression Analysis – Perceptions multiplied by age vs. Behavior variables

Dependent variable	R	R Square	Adjusted R Square	Std. Error of the Estimate
Trust	,11[a]	,01	,00	1,11
Attitude	,10[a]	,01	,00	1,00
Self-Disclosure	,28[a]	,08	,07	2,08

a. Predictors: (Constant), Perceived Privacy and Security * Age

Table 6

Coefficients Regression Analysis – Perceptions multiplied by age vs. Behavior variables

		Unstand. B	t	Sig.
Trust	(Constant)	4,16	14,35	,00
	PPS*Age	-,00	-1,10	,27
Attitude	(Constant)	4,71	18,12	,00
	PPS*Age	,00	1,02	,31
Self-Disclosure	(Constant)	7,07	13,06	,00
	PPS*Age	-,01	-2,96	,01*

From the analysis can be concluded that the interaction between age and perceptions significantly predicts self-disclosure scores, β = -0.012, $t(101)$ = -2.955, $p < 0.005$. The interaction between age and perceptions explains a significant proportion of variance and in self-disclosure scores, R^2 = 0.08, $F(1,101)$ = 8.73, $p <$ 0.005. The interaction between age and perceptions seems to account for 28.3% of the self-disclosure scores variation. The coefficient for self-disclosure is -0.002, so for every unit increase in self-disclosure scores, a 0.002 unit decrease in the interaction between age and perceptions is predicted, holding the other variables constant. Therefore can be concluded that age has a significant role as a moderator in the relationship between perceptions and self-disclosure. The other two variables, trust and attitude, are not significantly related to the interaction between age and perceptions.

5. CONCLUSION

5.1 Discussion

Table 7

Summary of hypothesis tests

Hypothesis	*t(F)*-Value	*p*-Value	Support
H1. PP millennials = PP non-millennials	2.535	0.114	Yes
H2. SP millennials = SP non-millennials	2.124	0.148	Yes
H3. Perceptions → Trust	3.95	0.0001	Yes
H4. Perceptions → Attitude	1.826	0.071	No
H5. Perceptions → Self-Disclosure	0.182	0.856	No
H6A. Interaction Age & Perceptions → Trust	-1.1	0.274	No
H6B. Interaction Age & Perceptions → Attitude	1.016	0.312	No
H6C. Interaction Age & Perceptions → Self-Disclosure	-2.955	0.004	Yes

The objective of the study was to understand the privacy and security perceptions of millennials and non-millennials, and how these perceptions impact behavior on Facebook. Not to forget the moderating effect of age on the influence of perceptions on behavior. Both objectives are accomplished and half of the hypotheses are supported.

We predicted that millennials and non-millennials would not differ in terms of their privacy perceptions. Most of all, because the concept of privacy has evolved and therefore it reflects generational differences. From our analysis can be concluded that no difference was found between millennials and non-millennials regarding privacy perceptions on Facebook, which is consistent with Raynes-Goldie (2010)[33], who suggested that millennials are not more careless than non-millennials with regard to protecting their personal information in online environments. In addition, that we found no age-related differences in perceptions is in line with Chung et al. (2010) who similarly found no age-related differences in perceived privacy protection in the context of online community participation and therefore similarly with our study younger and older adults were not different in their degrees of concern about privacy issues.[34] Furthermore, as identified by Krasnova et al. (2009) a major privacy concern for end-users in social media is the organizational threat of data collection by the SNS provider and third parties.[35] In the present study, we found a similar results, where most of the respondents were unaware of the specific parties collecting the data (mean of 1.9). These results confirm that a lot of Facebook users are unaware of the current big data

[33] (Raynes-Goldie, 2010)

[34] (Chung, Park, Wang, Fulk, & Mclaughlin, 2010)

[35] (Krasnova, Günther, Spiekermann, & Koroleva, 2009)

gathering by several parties, which results in concerns regarding their privacy. We might be seeing this result due to the novelty of the technology. Facebook is rather new for a lot of people and are therefore unaware of its consequences. When the users would be aware, it could change their perceptions on privacy and security. Malhotra et al. (2004) found similar results where internet privacy concerns were highly correlated with perceived awareness.[36] This indicates that when a Facebook user would be aware of the data collection procedure, it could result in more privacy concerns.

For security perceptions of Facebook users, we predicted no differences between the age groups. We made this prediction based on the same argumentation of Raynes-Goldie (2010)[37], saying that the concept of privacy and security has evolved over time and therefore reflects generational differences. Therefore, the results are consistent with the hypothesis, since no differences in security perceptions are found between millennials and non-millennials. This indicates that despite the generational differences, all the respondents feel rather similar about the security of Facebook. Both age groups feel neutral about the security of Facebook. However, the respondents strongly felt to seek control over their personal information by adjusting the privacy settings (mean of 5.5). This result is in line with (Kim & Shin, 2008) who suggest that perceived security is largely determined by the users' perceived control over their personal information. In addition, as Hajli and Lin (2014) described that SNS users are in great need of control over their personal information, and this need of control determines how we evaluate the security of a SNS.[38] Facebook users use the privacy settings and the group feature to control their personal information, these two features could mean that the users perceive Facebook as more secure.

The results show that privacy and security perceptions have a significant impact on the users' trust in Facebook. When a Facebook user perceives the privacy and security of the platform as low, a logical consequence is that the user perceives the platform as less trustworthy. The perceptions predict a large part of the trust scores. Shin (2010) suggests that trust plays an important role in determining someone's actual behavior.[39] Furthermore, Christofides et al. (2012) found out that the participants in their study have become less trusting as a result of their experiences, where the experiences can be related to privacy and security issues.[40] The fact that we found a similar relationship between perceptions and trust as a behavior construct is therefore consistent with previous research. If a person perceives Facebook as careless regarding privacy and security, than these perceptions will reflect on their trust in Facebook. In addition, the findings of Shin (2010) support this result, where trust related significantly to perceptions of security, and a mediating effect of perceived privacy on trust through perceived security was found.[41] Especially, in the digital world of today trust is essential for the survival online businesses, where trust is the most important factor in the use or acceptance of consumer product websites.[42] However, the for the other two behavior variables, attitude and self-disclosure, was no significant relationship found. This implies that for one of the three behavior variables a link found with privacy and security perceptions. Therefore, can be said that within our study privacy and security perceptions had little impact on the online behavior of a Facebook user.

Lastly, we investigated the impact of age as a moderator in relationship between privacy/security perceptions and Facebook behavior. The results show that there was a significant impact of age as moderator in the relationship between perceptions and self-disclosure. This result implies that millennials and non-millennials are distinctive in their relationships between perceptions and self-disclosure. We might be seeing this results due to the fact that young adults (millennials) are more active on social networking sites and therefore disclose more personal information. The results from the ANOVA test showed similar results, where millennials and non-millennials were significantly different in the amount of personal information they disclosed on their Facebook. However, no moderating role of age was found in the relationship between perceptions and trust/attitude. The role of age as a moderator in the relationship between perceptions and Facebook behavior is therefore limited. Previous research from Haji and Lin (2014) showed that their results on information sharing behavior were robust after controlled for age as a control variable.[43] Furthermore, the results from (Chung et al., 2010) support these findings, since no moderating role of age was found for behavioral intention to participate in online communities.[44]

5.2 Theoretical Implications

5.2.1 Privacy Perceptions

The study could be further improved by using a bigger sample in another population in order to make the results more reliable. An interesting finding from this research is that the mean for both age groups is little below neutral, this indicates there is a small tendency from the respondents towards perceiving Facebook as not securing privacy issues. In addition, the respondents from both age groups showed that they are not fully aware of all the parties who collect the information from Facebook (mean of 1.9). When the participants would be aware of the data collection of Facebook and third parties, the participants could tend to perceive the privacy on Facebook even lower. A study on the relationship between awareness of data collection and privacy/security perceptions could be an interesting topic for future research. Furthermore, another suggestion could be to conduct the study on multiple platforms (e.g. MySpace, Twitter, and LinkedIn).

5.2.2 Security Perceptions

The mean for both age groups is a little above neutral. Furthermore, a noteworthy result is that both age groups extensively use the group feature in Facebook (mean of 4.72). For future studies, an interesting idea could be to investigate the motivations for the use of the Facebook group feature. Moreover, perhaps a more interesting finding is that most of the respondents tend to adjust their privacy settings in order to make their posts and information visible to a specific group of people (mean of 5.49). A study concerning the awareness of Facebook's privacy settings and the relationship to the usage of these settings would

[36] (Malhotra, Kim, & Agarwal, 2004)
[37] (Raynes-Goldie, 2010)
[38] (Hajli & Lin, 2014)
[39] (Shin, 2010)
[40] (Christofides, Muise, & Desmarais, 2012)
[41] (Shin, 2010)
[42] (Lankton & McKnight, 2011)
[43] (Hajli & Lin, 2014)
[44] (Chung, Park, Wang, Fulk, & Mclaughlin, 2010)

be interesting, since not all the Facebook users nowadays are aware of its settings.

5.2.3 Facebook Behavior

The other variables attitude and self-disclosure had no significant relationship to privacy and security perceptions. We would suggest to improve the study by using a bigger sample size in order to make the results more robust. Furthermore, a future study about the relationship between privacy/security perceptions and trust on social media's is suggested. This study should be performed on multiple platforms (Twitter, MySpace, and LinkedIn) to see whether the results are the similar for different platforms. Our results displayed a significant impact of age as a moderator in the relationship between perceptions and self-disclosure. However, these results were contradicting with prior research, therefore a further study on age as a moderator in this research model would be an interesting topic.

5.3 Practical Implications

5.3.1 Privacy Perceptions

Insights into privacy perceptions regarding Facebook is of interest for every business active on Facebook. First of all, for Facebook itself it is important to acknowledge that not much people are aware of its privacy settings. Perhaps people want to adjust their settings, but they are not aware. As we found no significant differences in privacy perceptions among millennials and non-millennials, Facebook could target their privacy strategies on both age groups in the same way. Furthermore, most respondents indicated that they are not aware of the information collected. Governmental institutions could start awareness campaigns regarding disclosure of personal information online. Social network participation actually reinforces face-to-face relationships rather than replacing those (O'Brien et al., 2011).[45] The popularity of social networking will rise even more, and therefore the public opinion on privacy and security too. With the knowledge of privacy perceptions among Facebook users, companies online could broaden their perspective online presentation of the company.

5.3.2 Security Perceptions

The most striking finding regarding security perceptions was that a lot of respondents indicated that they adjust their privacy settings to make their posts and information visible to specific group of people. The result indicates that people tend to protect their personal information. Companies who collect and analyze big data should be careful in their strategies, since people nowadays tend to have negative feelings towards the use of their personal information by third parties. Several lawsuits have been filed against Facebook, because Facebook shares its members' personal information for commercial purposes. All social media's should be careful in their strategies, since privacy and security online is a sensitive issue nowadays. Moreover, businesses active on Facebook could address security issues on their page. For example, convincing the customer that the transaction process is robust against breaches, and in case that something happens they will get the amount returned.

5.3.3 Facebook Behavior

Privacy and security perceptions seems to account for 13.5% of the variation in the trust scores. This means indicates that privacy and security perceptions link to trust. Trust is a very sensitive topic and vital for a business like Facebook. Therefore, social networking sites should be mindful in their privacy and security strategies, since it will have an effect on the end-users' behavior. Furthermore, gender appears to have an effect on attitude, which is logically since men and women behave differently. Lastly, we found out that age is a moderator in the relationship between perceptions and self-disclosure. For further research on the topic of self-disclosure on social networking sites, researchers should take age into consideration.

5.4 Limitations

A number of limitations persist within our research. Firstly, the respondents might not represent the whole population since the respondents come from our social environment. Most of the participants were Dutch and German. On the other hand, our study takes into consideration different ages and therefore can be said that our sample provide a comprehensive picture of the SNS community with regard to age. Secondly, the study could be improved by using a bigger sample size. By doing so, as the sample size increases the results eventually get more robust and remarkable patterns can be picked out. Thirdly, the research model is composed of too many similar and overlapping constructs, which are correlated with each other. This problem was also encountered by Shin (2010) in his study, he notes that therefore the findings may be a result of inaccurate measures. Fourthly, the results from the reliability analysis were poor in our study. The Cronbach's alpha was acceptable for only the variables trust and attitude. However, we followed the procedure as proposed by Shin (2010) in his study. His results were considered reliable, since the Cronbach's alpha always was on an acceptable level. But also due to time constraints within our bachelor thesis we accepted the poor reliability results.

[45] (O'Brien, Read, Woolcott, & Shah, 2011)

6. REFERENCES

Ajzen, I., & Fishbein, M. (1980). *Understanding Attitudes and Predicting Social Behavior.* New York: Prentice Hall.

Barker, V. (2009). Older Adolescents' Motivations for Social Network Site Use. *CyberPsychology & Behavior*, 209-213.

Christofides, E., Muise, A., & Desmarais, S. (2012). Risky Disclosures on Facebook: The effect of having a bad experience on online behavior. *Journal of Adolescent Research*, 1-18.

Chung, J. E., Park, N., Wang, H., Fulk, J., & Mclaughlin, M. (2010). Age differences in perceptions of online community participation among non-users. *Computer in Human Behavior*, 74-84.

Dwyer, C., Hiltz, S. R., & Passerini, K. (2007). Trust and privacy concern within social networking sites:. *AMCIS 2007 Proceedings*, (p. Paper 339).

Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior*, 153-160.

Hajli, N., & Lin, X. (2014). Exploring the Security of Information Sharing on Social Networking Sites. *Journal of Business Ethics*.

Kim, W.-Y., & Shin, D.-H. (2008). Applying the Technology Acceptance Model and Flow Theory to Cyworld User Behavior. *CyberPsychology & Behavior*, 378-382.

Krasnova, H., Günther, O., Spiekermann, S., & Koroleva, K. (2009). Privacy concerns and identity in online social networks. *Identity in the Information Society*, 39-63.

Lankton, N., & McKnight, H. (2011). What Does it Mean to Trust Facebook? Examining Technology and Interpersonal Trust Beliefs. *Advances in Information Systems*, 32-54.

Lawler, J., Molluzzo, J., & Doshi, V. (2012). An Expanded Study of Net Generation Perceptions on Privacy and Security on Social Networking Sites (SNS). *Information Systems Eduction Journal*, 21-36.

Livingstone, S. (2008). Taking risky opportunities in youthful content creation. *New Media & Society* , 393-411.

Malhotra, N., Kim, S., & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC). *Information Systems Research*, 336-355.

Metzger, M. (2004). Privacy, Trust, and Disclosure: Exploring Barriers to Electronic Commerce. *Journal of Computer-Mediated Communication*.

O'Brien, L., Read, P., Woolcott, J., & Shah, C. (2011). Understanding Privacy Behaviors of Millennials within Social Networking Sites. *ASIST*.

Palfrey, J., & Gasser, U. (2008). *Understanding the first generation of digital natives.* New York: Basic Books.

Quantcast. (2016, Mei 3). *Quantcast.* Retrieved from Quantcast: https://www.quantcast.com/top-sites/US

Raynes-Goldie, K. (2010). Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. *First Monday*.

Shin, D.-H. (2010). The effects of trust, security and privacy in social networking. *Interacting with Computers*, 428-438.

Skinner, E. (1996). A guide to constructs of control. *Journal of Personality and Social Psychology*, 549-570.

Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social networking sites. *Bulletin of Science Technology Society* , 20-36.

Yenisey, M., Ozok, A., & Salvendy, G. (2005, July). Perceived security determinants in e-commerce among Turkish university students. *Behaviour & Information Technology*, pp. 259-274.

7. APPENDICES

7.1 Appendix A – Correlations Table continuous variables (Pearson's correlation)

Correlations

		Perceived Privacy	Perceived Security	Attitude	Trust	Self-Disclosure	AGE_1_TEXT	EDU
Perceived Privacy	Pearson Correlation	1	,225*	,109	,312**	,058	-,146	-,077
	Sig. (2-tailed)		,023	,276	,001	,563	,142	,442
	N	102	102	102	102	102	102	102
Perceived Security	Pearson Correlation	,225*	1	,173	,262**	-,031	-,133	-,078
	Sig. (2-tailed)	,023		,082	,008	,761	,184	,437
	N	102	102	102	102	102	102	102
Attitude	Pearson Correlation	,109	,173	1	,426**	,111	,013	-,087
	Sig. (2-tailed)	,276	,082		,000	,268	,898	,382
	N	102	102	102	102	102	102	102
Trust	Pearson Correlation	,312**	,262**	,426**	1	,129	-,303**	-,259**
	Sig. (2-tailed)	,001	,008	,000		,198	,002	,009
	N	102	102	102	102	102	102	102
Self-Disclosure	Pearson Correlation	,058	-,031	,111	,129	1	-,344**	-,242*
	Sig. (2-tailed)	,563	,761	,268	,198		,000	,014
	N	102	102	102	102	102	102	102
Age in text	Pearson Correlation	-,146	-,133	,013	-,303**	-,344**	1	,177
	Sig. (2-tailed)	,142	,184	,898	,002	,000		,076
	N	102	102	102	102	102	102	102
Education	Pearson Correlation	-,077	-,078	-,087	-,259**	-,242*	,177	1
	Sig. (2-tailed)	,442	,437	,382	,009	,014	,076	
	N	102	102	102	102	102	102	102

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

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

7.2 Appendix B – Correlations Table ordinal variables (Spearman's Rho)

Correlations

			Gender	Nationality
Spearman's rho	Gender	Correlation Coefficient	1,000	,206*
		Sig. (2-tailed)	.	,038
		N	102	102
	Nationality	Correlation Coefficient	,206*	1,000
		Sig. (2-tailed)	,038	.
		N	102	102

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

7.3 Appendix C – Survey items

Demographics
NAT: What's your nationality?

- Dutch
- German
- Other:

AGE: What's your age?

GEN: What's your gender?

- Male
- Female

EDU: What's your highest level of completed education:

- Did Not Complete High School
- High School
- Trade/technical/ vocational training
- Some College
- Bachelor's Degree
- Master's Degree
- Advanced Graduate work or Ph.D.

Perceived privacy
PP1: I am confident that I know all the parties who collect the information I provide during the use of Facebook
PP2: I am aware of the exact nature of information that will be collected during the use of Facebook
PP3: I am not concerned that the information I submitted on Facebook could be misused
PP4: I believe there is an effective mechanism to address any violation of the information I provide to Facebook

Perceived security
PS1: I believe the information I provide with Facebook will not be manipulated by inappropriate parties
PS2: I am confident that the private information I provide with Facebook will be secured. (Yenisey et al. (2005))
PS3: I believe inappropriate parties may deliberately view the information I provide with Facebook (Yenisey et al. (2005)
PS4: I adjust my privacy settings on Facebook in order to make my posts visible to a specific group of people.
PS5: I make use of the private groups feature of Facebook

Usage
USE: How often do you come into contact with Facebook?

- Less than once a week (1)
- Once a week (2)
- At least once a day (3)
- 11-20 times a day (4)
- More than 20 times a day (5)

TIM: About how much time do you spend on Facebook a week?

- 0-5 hours (1)
- 5-10 hours (2)
- 10-15 hours (3)
- 15-20 hours (4)
- 20+ hours (5)

DEV: On which devices do you use Facebook? You can give multiple answers.

- Desktop computer
- Laptop
- Smartphone
- Tablet
- Other

Self-disclosure

ADD: Please indicate what information you include on your Facebook profile (also when it is not shown to other users). You can give multiple answers. (Dwyer, 2007)

- Photograph of yourself
- Real name
- Hometown
- Email address
- Cell phone number
- Relationship status
- Sexual orientation
- Work
- Religion
- Political preference
- Education

Trust

TR1: Facebook is a trustworthy social network
TR2: I can count on Facebook to protect my privacy
TR3: Facebook can be relied on to keep its promises
TR4: I never read privacy policies on Facebook

Attitude

AT1: I would have positive feelings towards Facebook in general
AT2: The thought of using Facebook is appealing to me
AT3: Facebook has become part of my daily routine.
AT4: The fact that my posts on social media may be viewed by other individuals in my social environment influences my social media behavior