Security and privacy perceptions of millennials vs non-millennials in digital environments

Author: Deirdre Kuperus
University of Twente
P.O. Box 217, 7500AE Enschede
The Netherlands

This research investigates the effect of privacy and security perception of internet users on online search behavior. It aims to increase the understanding on differences between millennials and non-millennials in this effect. Privacy perception is measured by awareness and trust, while security perception is determined by trust and practice, all measured by items in an online survey. The results of this survey indicate a significant correlation between privacy and online search behavior, but between security and online search behavior it does not show a significant effect. A univariate analysis of variance showed a significant difference between millennials and non-millennials regarding privacy, but not in the case of security perception. The lack of significance for security is possibly caused by the fact that awareness of lack of privacy does not necessarily correspond in practice to protect privacy.

Supervisors: Raja Singaram
Dr. Rik van Reekum

Keywords
Online search behavior, privacy perception, security perception, millennials

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

1. INTRODUCTION

In recent years the usage of internet technologies has expanded and for most people the internet is a very present factor in everyday life. The data collection of users of these technologies has also experienced a rapid development, marking the rise of Big Data. This Big Data retrieved from internet activities contains a large amount of personal information and presents many marketing opportunities. However, the data collection also has downsides. According to the book *Big Data, A Revolution That Will Transform How We Live, Work and Think* 'datafication risks arise when crossing the lines of consumer analysis to invasion of privacy' (Mayer-schonberger & Cukier, 2013). The privacy issue gains importance as the presence of internet in our life increases and the application options for Big Data grow. According to Mekovic (2011) a significant number of customers is only willing to use web sites in the case they believe this web site will ensure and protect their privacy. Privacy perception is thus an important aspect of marketing.

Besides protection of their privacy, users of the internet want to be secure against online threats, they wish for their safety to be secured. Benassi (1999) and Zucker (1986) agree that trust is the most precious asset any business has. According to their findings, customers have to believe that their privacy and security is guaranteed before they are willing to do business with a firm or make use of their services. According to Hoffman, Novak and Peralta (1999), this trust is more important than ever in 'the new era of the Internet and the World Wide Web'. This implies that in e-commerce privacy and security perception play an important role in the success of a company, but does this also apply for online searching, before any business is done?

Of all the possible online activities a large amount can be described as online search behavior. Online search behavior concerns the internet activities related to gathering information. Online search behavior is not a new concept, but since it is evolving in a fast rate research tends to become outdated and incomplete rapidly. Therefore, explorative research on the current situation can always be regarded as relevant. Also, in previous research on online search behavior there have barely been quantitative results on its relationship with privacy and security perception. This makes the exploration of the possible effect of privacy and security perception of internet users on online search behavior attractive. According to Tene (2007), the privacy of users is threatened by search engines using and abusing their users information. Search engines record your keywords and share this with the websites visited, often combined with information making it possible to identify you (Weinberg, 2016). Most internet users do not seem to realize that they are themselves a precious information source for the search engine that records all of their requests. Another possibility is that these users choose to ignore this fact. Are internet users aware of their lack of privacy online? In what way can online search behavior be affected by the variables privacy perception and security perception? In Figure 1 the model of this question is displayed.

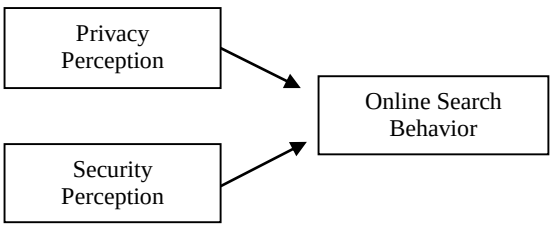

Figure 1

Although this would already prove an interesting research, there is another variable which can be added. A side of this issue which has not been researched extensively is the difference in age groups regarding privacy and security perception on online search behavior. The existing literature mostly describes online privacy and security perception without considering the possible effect of age. Especially within the field of search behavior, a possible correlation between privacy, security and age has not been investigated thoroughly.

Relevant age groups for comparison are millennials and non-millennials. Is there a difference in privacy and security perception and its effect on search behavior for those growing up in an online world? One would expect the source of any differences to be the generation gap and the infused technological influence the millennials are experiencing (Taylor, 2012).

Any results on the difference between age groups regarding online privacy perception could prove to be a useful marketing tool. It could be possible to develop recommendations for businesses on how to deal with different age groups regarding privacy perception on online search behavior.

Incorporating the factor age in the research results in the model displayed in Figure 2.

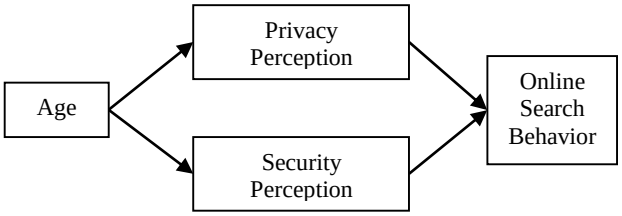

Figure 2

Considering the possible practical advantages of increased knowledge on the effect of age on the subjects previously mentioned, the central research question in this paper will be:

'What is the effect of age on privacy and security perception and how does that affect online search behavior?'

Based on this research question two hypotheses are formed:

Hypothesis 1: privacy and security perception have a significant positive effect on online search behavior

Hypothesis 2: there is a significant difference between millennials and non-millennials in this effect

This paper will contribute to existing literature by increasing the understanding on the differences in age groups regarding privacy and security perception of online search behavior. The objective of the research is to narrow the existing research gap in this area. It would be interesting to look at the differences between age groups and the outcomes of the research could draw a different angle on the current knowledge of privacy perception between age groups and its effect on online search behavior.

2. THEORETICAL FRAMEWORK

In order to provide a reasonable understanding of the research the key concepts are important. The concepts millennials and non-millennials, privacy perception, security perception and online search behavior are elaborated on below.

2.1 Millennials & non-millennials

This research aims to understand the difference in privacy perception of two age groups, defined as millennials and non-millennials. Howe and Strauss (1991) identify millennials as the generation born between 1982 and 2000. "Our generation is […] about technology, discovery" says Mikah Giffin (Howe &

Strauss, 2000). The millennials were born into a digital world infused with unlimited information and technologies, unlike the generation before them (Taylor, 2012). Due to an upbringing within this technological, online world, the online search behavior as well as the privacy and security perception of the millennials might be different from older age categories. Within this paper, millennials are defined as individuals within the age group 18 to 24 years old in May 2016. Non-millennials are essentially all falling out of this group, but in this research the other age group focused on will be individuals in the age 36 to 50 in May 2016. This group shall be referred to as the non-millennials.

2.2 Privacy and security perception

2.2.1. Privacy perception

Privacy perception in this research refers to the manner in which the groups perceive their online privacy to be. Dritsas (2005) explores different kinds of privacy and how privacy of users can be protected in digital environments. It reviews different perspectives on the matter and tries to understand trends.
Privacy is often defined in four ways: territorial privacy, bodily privacy, informational privacy and communicational privacy (Dritsas, 2005). For online privacy regarding search behavior mainly informational privacy is important. This includes 'the awareness and control of whether and how personal data can be gathered, stored, processed and communicated' (Dritsas, 2005).

Castañeda & Montoro (2007) provide a similar definition. Online privacy can be defined as Internet users' concern regarding their control over collection of information during online activity and control over the usage of this information. Privacy perception measures the way internet users perceive this privacy to be.

Combining these definitions, privacy perception in digital environments refers to the awareness of collection of personal data during online activity and usage of this information. There is, however, another factor influencing privacy perception. According to Cullen et al. (2000) 'virtually all determination of authenticity or integrity in the digital environment ultimately depends on trust'. Besides the awareness of privacy issues, the attitude towards these issues plays a relevant role. The trust online users have towards online businesses, search engines, social media etc. affects their perception of privacy. Figure 3 displays how both awareness and trust build up privacy perception. It is based on the literary sources mentioned above.

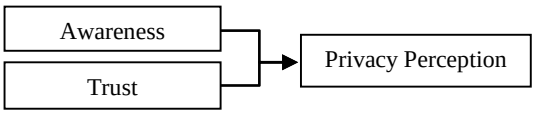

Figure 3

2.2.2. Security perception

The Oxford English Dictionary defines security as: 'The state of being free from danger or threat' (Oed, 2016).
The basic concept of web security is assessed by Garfinkel et al. (1997). The paper examines the different issues present regarding risks for online users. The privacy of users is not the only thing at stake on the world wide web. The property of individuals and companies can be threatened when hackers or other third parties are able to obtain credit card numbers and other sensitive financial information. The prospect of possessing such sensitive information make web servers an attractive target for hackers and other attackers (Garfinkel, 1997). Where online privacy concerns the collection and usage of personal data, online security is about safety; being secure from possible online threats. It is concerned with the protection of personal data from unwanted intruders.
From the perspective of online users, it concerns the trust the users have in the safety of the world wide web, and the practices the users undertake to ensure their protection.
The practice of the user reflects the perception of security the user has. The extent to which a user engages in action to ensure its online safety is a determinant of its perceived security.
Similar to privacy perception, trust plays a relevant role in establishing security perception. The attitude towards online safety is a part of security perception, besides the practices an online user commits to in order to ensure its security. According to Mayer, Davis and Schoorman (1995), users will engage in risk taking 'if the level of trust surpasses the threshold of perceived risk'. The level of trust is thus, according to their findings, important in determining perceived risk and security. Figure 4 displays the combining of practice and trust to form the variable security perception.

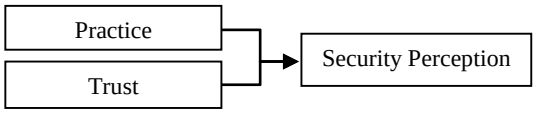

Figure 4

2.3 Online search behavior

The term online search behavior can be applied broadly, including e-commerce and basically most websites where information is present, but will be limited to search engines in this research. There are three major search engines without a limiting geographical scope and operating in multiple languages, namely Google, Bing and Yahoo. Besides these major engines, there are several less known engines operative. However, the overwhelming majority of searching is done via the three major search engines (Comscorecom, 2016).

2.3.1 Privacy and security within online search behavior

There is controversy on the respect search engines have for the privacy of its users. Tene (2007) believes the privacy of users to be threatened by search engines using and abusing their users information and investigates the privacy problems and mentions solutions. It is common knowledge that the major search engines are tracking the search history of individual users and building profiles based on this data. Different search results and advertisements are presented based upon these profiles, Google even mentions it on their own help page (Google, 2016).
For those uncomfortable with being tracked there are alternative search engines, such as DuckDuckGo, StartPage and Ixquick (Weinberg, 2016). Where DuckDuckGo is a regular search engine, StartPage and Ixquick are metasearch engines, 'using another search engine's data to produce their own results from the internet' (Glover et al., 1999). Their information comes from Google, but Google is not able to track individual searchers. Although this would be a suitable option for those concerned about their privacy, the existence of these alternative options is not widely known. It is also possible for users to search in incognito or private mode, which disables websites to save cookies onto your device. Every website is still, however, able to recognize your IP address.
In the field of security search engines have a better reputation. In general, the tracking of search history and profiling of this data does not pose immediate threats to the user. Search engines also take effort to ensure security of users, for example by 'blocking searchers from sites with deceptive download buttons' (Schwartz, 2016). Most of the negative associations with being tracked are about privacy rather than security.

It is, however, the case that personal data is collected which could do damage in case this information is misused. Servers and websites can be vulnerable for attacks by hackers and leaks of personal information are not uncommon (Calo, N, 2014).

3. METHODOLOGY

3.1 Procedure

Quantitative research was used to collect data. Through qualtrics.com an online questionnaire was created, which link was sent via email, Facebook and WhatsApp to possible respondents. The respondents were provided with a short text, explaining the aim of the research and assured of the anonymity of the participants. Contribution to the research was voluntary, allowing participants to decline answering the questionnaire or not to finish it. The survey was only conducted at a single point in time, making it a cross-sectional study.

The survey contained items set up in the form of a Likert scale to find quantifiable results on privacy perception and online search behavior. The Likert scale consisted of seven options on a differing scale of, for example, 'strongly disagree – strongly agree' and 'never – always'. The Likert scale attempts "to improve the levels of measurement […] through the use of standardized response categories in survey questionnaires, to determine the relative intensity of different items" (Babbie, 2010). In order to ensure a reliable and valid outcome a minimum of 50 respondents per age category was required.

Although this research only compares one age class of millennials (18-24) with another age class of non-millennials (36-49), the respondents of the survey were divided into four categories. There were two millennial age categories: '18-24' and '25-35', and two non-millennial age classes: '36-49' and '50 and older'.

The survey consisted of statements concerning their online search behavior, the level of perceived privacy within digital environments, level of privacy concerns and if the users take action regarding protecting their privacy.

3.2 Population and sample

The total amount of respondents is 439. The sample was divided in four groups, all requiring a minimal amount of fifty respondents (N=50). There was a significantly higher response in the lower age categories, especially in the group of 18-24 containing 205 respondents. The other millennial age group (25-35) had a total amount of 83 respondents. The two non-millennial age groups both had 70 respondents, meeting the requirement of N=50 per age group.

The deletion of respondents with missing information, however, resulted in a final sample of 258 respondents. The large difference between the total amount of respondents and the final sample can partly be explained by a rather high dropout rate, of 39,18%, or 172 respondents. Only 267 of the respondents managed to complete the survey, making just 60,82 percent of the responses valid.

In the final sample the first group of millennials (18-24) contained 125 respondents. The second group, consisting of respondents aged 25 to 35, had a final sample of 51 respondents. The two non-millennial age classes (36-49 and 50 up) both contained 41 respondents.

This resulted in a millennial sample of 125 respondents and 41 respondents of non-millennials. In the final sample the requirement of N=50 was unfortunately not met, which should be taken into account analyzing the results. Also, the sample size is unequal; the millennial age class contains three times as much respondents as the non-millennials.

The response rate was challenging to be measured since the survey was distributed in various ways. The response rate via Facebook sharing was incredibly low, if all individuals who could have seen it are taken into account. In this research there was no time to develop a suitable formula to calculate the response rate via continuous Facebook sharing. The respondents contacted personally mostly filled in the survey, but via Facebook sharing the response rate was extremely low.

3.3 Measures

In this research privacy and security perception are chosen as the independent variables and their effect on the dependent variable search behavior is tested. Thus, search behavior depends on the perception of privacy and security. There are three control variables, namely occupation, education and nationality.

The questionnaire followed the framework of Yang et al. (2004), consisting of three sets of measures. The research of Yang et al. aimed to analyze the different stages in the product/service purchasing cycle, including information search online. The first set covered general information, including demographic variables. The second set: 'perceptions of overall online service quality and individual quality dimensions' was replaced by privacy and security perception. The last set, 'computer and internet usage information' was applied to online search behavior (Yang et al., 2004).

3.3.1 Independent variables

The combination of the two figures mentioned in the theoretical framework 4 leads to the model displayed in Figure 5. This figure displays the factors measured in the survey and how they are divided between privacy and security perception. The measurement of trust is used for both independent variables.

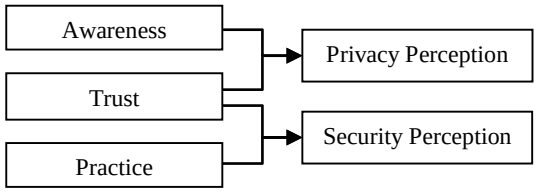

Figure 5

Privacy and security perception were measured in the survey by 16 items. Two of these items are not included in the calculations, since they could not be measured on an ordinal scale. All items are included in the Appendix.

Privacy perception was measured by five items (three statements and two questions), concerning the collection and use of personal data. The response to these statements and questions resulted in a value of one to seven on an ordinal scale. Four of the items measured awareness and one measured trust. The five items were pooled into a single variable: privacy.

Security perception was measured by nine items, all included in the calculations. These items consist of six questions and three statements. Like Privacy and Search Behavior, the response to these items resulted in a value of one to seven on an ordinal scale. Seven items measured practice and two of the items measured trust. The items measuring practice and those measuring trust were also pooled into a single variable: security.

3.3.2 Dependent variable

The dependent variable search behavior was measured in the survey by eight questions. These questions cover different aspects of online search behavior, namely frequency of use, engine preference, purpose of use and efficacy. Eventually five of the eight questions were omitted. It was decided these questions did not measure the preferred dimensions of search

behavior. In order to develop a consistent variable, the items and response option needed to be aligned. Only three of the questions were used, concerning usage and efficacy. These questions can be found in the appendix.

The response to the questions resulted in a value of one to seven, on an ordinal scale. The higher the value of the respondent, the more frequently the respondent makes use of the internet and the more effective the user is in finding its way on the web.

3.3.3 Control variables

The variables nationality, occupation and education were considered likely to have a certain effect on search behavior and therefore chosen as control variables. Their correlation with the dependent and independent variables was tested. The univariate analysis of variance also includes these control variables.

3.4 Reliability

The internal consistency of the independent and dependent variables was tested by Cronbach's Alpha, with table 1 presenting the results. The test for security produced a value of α=0.631. This makes the internal consistency acceptable. The Cronbach's Alpha for privacy resulted in α=0.421. This value is too low to be regarded reliable. The outcomes of the calculations involving this variable should be looked at with caution, since the variable privacy is not internally consistent. The dependent variable search behavior had a value of α=0.603. This value is also higher than α=.6 and can be regarded as acceptable (Cronbach, 1951).

Table 1: Reliability by Cronbach's Alpha

Variables	N	Cronbach's Alpha
Security	286	0.631
Privacy	286	0.421
Search Behavior	286	0.603

The quantitative data retrieved from the survey was analyzed using the statistical program IBM SPSS Statistics, in order to compare the groups among each other. The data analysis includes descriptive statistics such as the mean, the standard deviation the and minimum and maximum. A correlation table is included to examine significant correlations among the independent, dependent and control variables. A univariate analysis of variance was used with the aim to show the amount of variability in the age classes and to determine whether the variability is greater between these age groups than within the groups (Gravetter & Wallnau, 2010).

For all analyses a criterion level of α=.05 is chosen to evaluate significance.

4. RESULTS

4.1 Descriptive statistics

The most important descriptive statistics can be found in Table 1. There was one extreme outlier in age, i.e. a respondent with the age of 200. This respondent was removed from the data set. Also, respondents below the age of 18 were removed, since this was the minimal age required. After this process, along with the deletion of respondents with missing information, a final sample of 286 respondents remained (N=286).

The mean age is 32.54, with a minimum of 18 and a maximum of 80 years of age. The standard deviation is 14.069 years. For the remaining variables the lowest response option is 1 and the highest is 7. The independent variable security has a mean of 3.66. The responses range from 2 to 7. The standard deviation for security is 0.778. The independent variable privacy has a mean of 5.28. The minimum for privacy is 3 and it has a maximum of 7 (the highest possibility). The higher this number is, the less privacy the respondent perceives, since the respondent is aware of the fact that data is collected and further shared. The mean is almost two points higher than security, proving it to be more significant for the respondents or this study. The standard deviation for privacy is 0.740. Lastly, the variable search behavior has a mean of 5.71 with a standard deviation of 0.824. The responses range from a minimum of 2 to the maximum of 7. The higher this response, the more frequently the respondent makes use of search engines and the more effective the user is in finding its way on the web.

Table 2: Descriptives of the variables

Variables	N	Minimum	Maximum	Mean	Standard Deviation
Age	286	18	80	32.54	14.069
Security	286	2	7	3.66	.778
Privacy	286	3	7	5.28	.740
SearchBehavior	286	2	7	5.71	.824

4.2 Correlations

In Table 1 the correlations between security, privacy, search behavior and the control variables are displayed. The control variables have categorical values. Since the survey consisted of items set up in the form of a Likert scale with seven options, the independent and dependent variables have ordinal results. Due to these categorical variables the statistical test Spearman is used.

Table 3: Correlations among all variables

Variables	1	2	3	4	5	6
1.Security		.453	.179	.020	.000	.159
2.Privacy			.007	.249	.001	.619
3.SearchBehavior				.054	.906	.796
4.Nationality					.057	.001
5.Occupation						.000
6.Education						

The Spearman correlation revealed no significant correlation between the independent variable privacy and the dependent variable search behavior. Table 1 does show a significant positive correlation between the independent variable privacy and the dependent variable search behavior ($\rho = .168$; n=286; $p < .01$). This means that those respondents scoring high on privacy are more likely to be frequent and effective users of search engines. These correlations are also displayed in Figure 3.

The correlation between privacy and the control variable occupation is significant ($\rho = -.202$; n=286; $p < .01$). The independent variable security correlates significantly with the control variables nationality ($\rho = .144$; n=286; $p < .05$) and occupation ($\rho = .268$; n=286; $p < .01$). Between the control variables nationality and education there is also a significant correlation ($\rho = .205$; n=286; $p < .01$). The correlation between

occupation and education is also significant (ρ = .270; n=286; p < .01).

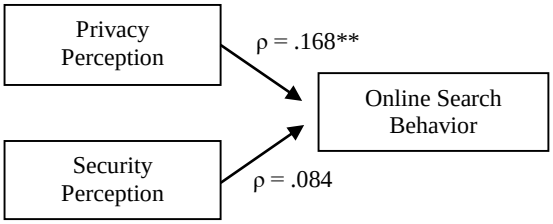

Figure 6

Figure 6 describes the correlations between privacy perception and online search behavior and security perception and online search behavior. Between security perception and online search behavior there is an insignificant positive relation. This means that the engagement of the user in security practices to protect its own data do not have a significant effect on the frequency of the use of search engines and the effectiveness of the user in finding its way on the web.

The correlation between privacy perception and online search behavior is significant at the α=.01 level. Those who perceive to have little privacy and a high awareness of the collection and usage of their personal data seem to be more active and more effective searchers on the internet.

4.3 Univariate analysis of variance

In Table 3 the results of the univariate analysis of variance are displayed with descriptive information of the different age groups. The first column describes the mean and number of respondents of the millennials. The second column explains the same for the non-millennial age category. In the last column the results of the test are displayed.

Table 4: Results univariate analysis of variance

	18-24 Mean (SD) N = 125	**36-49** Mean (SD) N = 41	**F(df), *p* value**
Independent variables			
Privacy	5.47 (0.68)	5.06 (0.82)	F(1,166) = 4.125, *p*= .044
Security	3.44 (0.68)	3.78 (0.82)	F(1,166) = 0.127, *p*= .722
Control variables			
Occupation	1.17 (0.64)	3.34 (1.15)	F(1,166) = 1.141, *p*= .287
Education	3.50 (1.48)	4.49 (1.33)	F(1,166) = 0.774, *p*= .380

The test does not reveal a significant difference between the age groups regarding security perception. There is, however, a significant difference between the groups regarding privacy perception (F = 4.125; n=166; p < .05). This means that the effect of privacy on search behavior is significantly different for millennials and non-millennials. The control variables occupation and education were also tested, and the values of *p* = .287 and *p* = .380 show no significant difference between the age groups.

Figure 7 shows the initial model mentioned in the introduction, with the outcomes of the tests included. The two tests produce different kinds of results, so the numbers noted are not on the same scale.

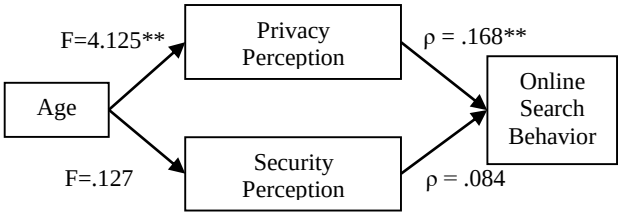

Figure 7

As indicated by the asterisks, age has a significant effect on privacy perception at the α=.01 level. This effect was shown by the univariate analysis of variance. The results of this research indicate that there is a difference between millennials and non-millennials regarding privacy perception. The Spearman correlation test showed a significant positive correlation between privacy perception and online search behavior. This correlation indicates that those who are aware of their (lack of) privacy are more active and effective searchers on the internet.

The figure does not show any significant effects in the area of security perception. Millennials and non-millennials do not differ significantly from one another and the effect of security perception on online search behavior is insignificant.

5. DISCUSSION

The purpose of this research was to increase the understanding on the differences between millennials and non-millennials regarding privacy perception of search behavior within digital environments. It was investigated whether there was an effect of age on privacy perception and how this might affect online search behavior: *'What is the effect of age on privacy and security perception and how does that affect online search behavior?'* A questionnaire was conducted to collect data of different age groups on privacy and security perception as well as online search behavior.

Firstly, based on the theories of Mekovic (2011) and Hoffman, Novak and Peralta (1999), a significant positive correlation was expected between the independent variables privacy and security perception and the dependent variable online search behavior. This would mean that those who perceive to have little privacy and a high awareness of the collection and usage of their personal data are more active and more effective searchers on the internet. Furthermore, the online users that score high on security perception, actively protecting their security, have a higher frequency and efficacy in online searching. The first hypothesis was formulated as the following:

Hypothesis 1: privacy and security perception have a significant positive effect on online search behavior

Between privacy perception and online search behavior there is indeed a significant positive effect. The correlation indicates that those who are aware of their (lack of) privacy are more active and effective searchers on the internet. This is in accordance with the first hypothesis. Between security perception and online search behavior, however, no significant effect was found. So according to the results of this research hypothesis 1 is partially accepted.

An explanation for the lack of significant effect between security perception and online search behavior could be that although internet users are aware of online threats they do not have a high interest for their safety. This was also suggested by the analysis of the open questions present at the end of the survey. Nowadays most websites claim they have to use cookies in order to provide proper service for internet users. Perhaps online users simply

believe that the end (the full internet experience) justifies the means (loss of privacy and security).

Secondly it was hypothesized that there would be a significant difference between millennials and non-millennials in this effect, formulated as the following:

Hypothesis 2: there is a significant difference between millennials and non-millennials in this effect

The results of the univariate analysis of variance show that there is indeed a significant difference regarding privacy perception. Millennials and non-millennials perceive privacy in different manners. The infused technological influence the millennials are experiencing is expected to be a source for this difference (Taylor, 2012). Where the non-millennials adopted the use of search engines into their lives once they were adults, the millennials enjoyed an upbringing within a technological, online world. This difference in acquaintance with online search engines and privacy is expected to be an important factor in differences between the age classes.

For the variable security perception, however, the difference is insignificant. Thus, hypothesis 2 is also partially accepted.

The insignificant difference between millennials and non-millennials regarding security was not expected. According to this research there is not a large difference between the practices online users have to ensure their digital security and their trust towards other players in this area of security. Since the difference in awareness between the age groups is significant, it is hypothesized that the awareness of lack of privacy might not be enough to change the practices of online users.

6. LIMITATIONS & FURTHER RESEARCH

6.1 Limitations

An important limitation of this research is the small sample size. The older age categories did not meet the minimal requirement of N=50 after the deletion of respondents with missing information and respondents which did not meet the age criteria. The final sample is large enough to get valid results, but not large enough to be able to generalize the results to the whole population.

Also, the Cronbach's Alpha for privacy of α=.421 was too low to be regarded reliable. Therefore, the outcomes of the calculations are questionable, since the variable is not internally consistent.

Lastly, trust beliefs could have been excluded in the pooling of the independent variables security and privacy, or could have been measured differently. The inclusion of these two items in the measurement of privacy and security makes the interpretation of these variables unnecessarily vague. Excluding these items results in a measurement of awareness for privacy and practice for security, making the outcomes of the survey clearer. The scale on which the responses of the items were measured was different for both trust and awareness and trust and practice. This results in values for privacy and security which are difficult to interpret.

6.2 Recommendations for further research

A larger sample will be required to draw generalizable conclusions. It would be preferable to have similar sizes for the age groups compared.

Furthermore, a recommendation for further research is the development of a framework or formula to measure response rate via Facebook sharing. When a questionnaire is posted on the wall of one person the response rate can be calculated by the amount of friends of that person, but this does not take into account that many friends might not have seen it. Also, once the questionnaire is shared further it becomes challenging.

Also, as mentioned in the limitations, the measurement of trust beliefs was not ideal. In further research trust could be measured separately or measured by different items.

Lastly, the outcomes of this research indicate a difference between awareness of collection and usage of personal data and practice to protect the online user for this collection and usage. Although many respondents were aware of their lack of online privacy, few took any measures to protect their personal data. A possibly interesting research would be to look at the difference between awareness and practice. To what extent are online users aware of their level of privacy and security? Does this awareness correspond in different practices regarding protection of privacy and security? What is the motivation of online users to protect or choose not to protect their data, even when they are aware of ways to do this? These are all relevant questions which could be answered by future research.

7. REFERENCES

Babbie, E. (2010). *The practice of social research.* Belmont: Wadsworth.

Benassi, P. (1999). TRUSTe: an online privacy seal program. *Communications of the ACM*, 42(2), 56-59.

Calo, N. (Producer). (2014). *Hacking and Cybersecurity Threats.* [Television programme]. Washington: Washington Journal

Castañeda, J.A & Montoro, F.J. (2007). The effect of Internet general privacy concern on customer behavior. *Electronic Commerce Research*, 7(2), 117-141.

Comscorecom. (2016). *ComScore, Inc*. Retrieved 6 June, 2016, from http://www.comscore.com/Insights/Press-Releases/2012/11/comScore-Releases-October-2012-US-Search-Engine-Rankings?cs_edgescape_cc=NL

Cronbach, L.J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika*, 16(3), 297-334.

Cullen, C.T et al. (2000). *Authenticity in a Digital Environment*. Washington, DC: Council on Library and Information Resources.

Dritsas, S. (2005). Protecting privacy and anonymity in pervasive computing: trends and perspectives. *Elsevier*, 23(12), .

Garfinkel, S & Spafford, E. (1997). *Web Security & Commerce.* Sebastopol: O'Reilly.

Garfinkel, S & Spafford, E. (2002). *Web Security, Privacy, and Commerce, second edition.* Sebastopol: O'Reilly.

Glover et al. (1999). Architecture of a Metasearch Engine that Supports User Information Needs. *Proceedings of the Eighth International Conference on Information Knowledge Management, (CIKM-99)*, 210-216.

Google. (2016). *About Google ads*. Retrieved 11 June, 2016, from https://support.google.com/ads/answer/1634057?hl=en

Gravetter, F.J & Wallnau, L.B. (2010). *Statistics for the Behavioral Sciences*. (9th ed.). California: Wadsworth.

Hoffman, D.L, Novak, T.P & Peralta, M.A. (1999). Building Consumer Trust Online. *Communications of the ACM*, 42(4), 80-85.

Howe, N. & Strauss, W. (1991). *Generations: The History of America's Future, 1584 to 2069.* New York : NY: William Morrow and Company.

Howe, N & Strauss, W. (2000). *Millennials rising: the next great generation* . New York : Vintage books.

Mayer-schonberger, V & Cukier, K. (2013). *Big Data: A Revolution That Will Transform How We Live, Work and Think*. Canada: Eamon Dolan/Houghton Mifflin Harcourt.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review*,20, 709–734.

Mekovic, R. (2011). Factors That Influence Internet Users' Privacy Perception . In Vrcek, N (Ed), *ITI 2011 33rd Int Conf on Information Technology Interfaces* (pp.). Cavtat: .

Oed. (2016). *Oxforddictionariescom*. Retrieved 2 June, 2016, from http://www.oxforddictionaries.com/definition/english/security

Schwartz, B. (2016, 12 April). Google now blocks searchers from sites with deceptive download buttons. [Weblog]. Retrieved 30 May 2016, from http://searchengineland.com/google-now-blocks-searchers-sites-deceptive-download-buttons-247114

Taylor, A. (2012). *A study of the information search behaviour of the millennial generation.* New Jersey: College of Business Administration, Rider University.

Tene, O. (2007). *WHAT GOOGLE KNOWS: PRIVACY AND INTERNET SEARCH ENGINES.* Forthcoming: Utah Law Review.

Weinberg, G. (2016). *DuckDuckGo*. Retrieved 1 June, 2016, from https://duckduckgo.com/privacy

Yang, Z., Jun, M., & Peterson, R. T. (2004). Measuring customer perceived online service quality. *International Journal of Operations & Production Management*, 24 (11), 1149 - 1174.

Zucker, L.G. (1986). Production of trust: Institutional sources of economic structure, 1840–1920. *Research in Organizational Behavior*, 8(2), 53-111.

8. APPENDIX

8.1 Questions used to determine search behavior

The items in italics were omitted from the calculations.

1. How often do you use online search engines?
2. *Which search engine do you use most often?*
3. *With which goal do you use search engines?*
4. *Do you usually know the address (URL) of the website you visit in advance? (Instead of going through search engines to find your way on the web)*
5. Can you always find the information you need, while using search engines on the internet?
6. *How often do you use the search suggestions (autocomplete) on e.g. Google?*
7. *How often do you choose the advertised options on search engines?*
8. Do you consider yourself to be skilled in finding what you need on the internet?

8.2 Questions used to determine privacy perception

The items in italics were omitted from the calculations.

1. I am aware that my private/search data can be given/sold to 3rd parties by online search engines.
2. I am aware that advertising is based on my prior searches.
3. Have you, personally, ever noticed advertisements online that are directly related to things you have recently searched for or sites you have recently visited?
4. If a search engine kept track of what you search for, and then used that information to personalize your future search results, how would you feel about that?
5. *Do you take any measures in order to protect your private data while searching online?*
6. In general, I trust mainstream online search engines.
7. Please share any security or privacy incidents while searching online that concern you. (Please answer in 3-5 sentences)

8.3 Questions used to determine security perception

1. Would you refuse to give information to an online search engine, if you think it is too personal or not necessary for the search process?
2. Privacy policies/terms and conditions on online search engines are easily accessible and understandable.
3. Do you read privacy policies of online search engines?
4. Would you refuse using a certain online search engine because of privacy policies?
5. Do you read terms and conditions of online search engines before you agree to them?
6. Would you refuse using a certain online search engine because of terms and conditions?
7. I believe that my personal information is protected while searching online.
8. Are you aware of the ways internet users can limit how much personal information websites collect about you?
9. I expect mainstream online search engines to fulfill basic digital security protection(s).