Willingness to pay for privacy on Facebook

Do people want to pay in order to guarantee their privacy on Facebook and how could this willingness to pay be manipulated?

Thesis supervisor:	Yu Gao
Name:	Rebecca Hoogendam
Student number:	346973
E-mail:	rebeccahoogendam@hotmail.com
Study:	Economie en Bedrijfseconomie

ERASMUS UNIVERSITY ROTTERDAM – BACHELOR THESIS

Table of Contents

1. Introduction

1.1 Internet, social media and Facebook

The introduction of Internet has led to a world that is more connected than ever before. Although three billion people probably will be connected in 2015 worldwide, still 60% of the global population has never connected to Internet (internet.org, 2014).
One of the many Internet-based applications that have emerged during the years is social media. These applications allow participants to create, exchange and share information, pictures and videos and have discussions, either on virtual communities or on networks. Figures from 2010 show that 22% of time online is spent on social media-related activities (The Nielsen Company, 2010). There are multiple social media websites nowadays. Besides Facebook, the most well-known are Twitter and LinkedIn. These networking platforms have all become very popular. This study will focus on Facebook.
The Facebook website (www.facebook.com) was launched in the United States early 2004 by Mark Zuckerberg, initially for the students of Harvard University. The site got a massive expansion, first nationally and later globally. At the end of 2014 Facebook had 1.39 billion users (Facebook Inc., 2015). To participate in the Facebook community one has to create a user profile that also contains personal information. Facebook tries to create a welcoming and safe environment, so that people can share and connect with their family and friends. People share so many things on Facebook; they enjoy updating their daily lives, from messages about their babies to pictures of their weddings and from music they listen to the location they have just arrived at on their vacations. There are not only individuals on Facebook, but also a lot of businesses for brand awareness and multiple other marketing reasons. Facebook went public in May 2012 and is listed on the NASDAQ (NRC.nl, 2012).

1.2 Facebook under scrutiny

Facebook is collecting many data of and information about their users. Much information is publicly available under the default settings of a Facebook account. Due to criticism, the networking site has tried several times to create a safer environment (BBC, 2012). Nowadays, the way social networks collect people's private information and make profits out of this is examined critically. The subject gets a lot of media attention and scientists are engaged in research on the right to privacy (Krishnamurthy & Willis, 2009).

1.3 Research question and scientific relevance

In a world that becomes more digital, how would it be possible to guarantee that companies and public institutions properly deal with our personal details? Do we have any privacy, in a time of digital media? There are for example already some applications available, like 'Keeper' and 'mSecure Password Manager', that ensure that passwords are saved and managed. Some people choose for non-free applications, because they are convinced that their private information is better protected in paid than in free applications.

A lot of research has been done on the topic of online privacy. In the past has been examined how digital privacy could be protected: is industry self-regulation sufficient or is legislation needed (Culnan, 2000). Legal and ethical issues concerning consumer online privacy have also been subject to scientific discussion (Caudill & Murphy, 2000). With regard to the willingness to pay for privacy on Internet, there has been done a field experiment in 2012 (Beresford, Kübler, & Preibusch, 2012) in which two web shops were compared. This experiment showed that customers paid more attention to the price of a product than to their privacy.

Yet it has never been investigated if people are willing to pay in order to protect their privacy on social media. Therefore, the main objective of this paper is to look at the willingness to pay for privacy on these online platforms. It is also very interesting to see if one's willingness to pay could be manipulated by the so-called framing technique. The manipulation aspect has also never been covered in previous research. In order to grant clarity about this central discussion point, a survey has been created to answer the following research question:

Are people willing to pay in order to guarantee their privacy on Facebook and could this willingness to pay be manipulated?

1.4 Valuing privacy

The question arises: is it actually possible to value privacy? In certain circumstances it is definitely possible to calculate the costs for privacy, e.g. the price differences between first- and second-class traveling in public transport. For online privacy however, there is no economic market. Since privacy is one of the human rights, it is obliged to protect personal details online. Both revealed preference methods and stated preference methods offer a solution for valuing digital privacy (Atkinson & Mourato, 2008). The former methods apply empirical data from associated markets to estimate the value of non-tradable goods. The latter methods require surveys in which respondents are asked to value such a good based on a described hypothetical market where the good in question can be traded. One of these methods is the Contingent Valuation (CV) method. Respondents are asked to express their maximum willingness to pay (or minimum willingness to except/compensation). In this paper, there will be looked with help from a questionnaire, how much one is relatively willing to pay for the protection of privacy on Facebook. In addition, the survey will investigate if the valuation of privacy could be manipulated.

1.5 Economic and social relevance

From an economic point of view, companies should really know how customers/users think about privacy. Especially the current attention for the protection of privacy on Internet should make companies like Facebook curious about the way their (potential) users are thinking about this subject. News about hacking government sites and personality theft could scare off (potential) users. Probably, paying a financial fee would increase the amount of users, because people might feel more secure about their privacy concerns. Also other social media could perhaps benefit from this investigation to attract more members.

Society could benefit from this research in case Facebook (and eventually some other networking sites) would apply the results that are in favor of the majority of the population. It is definitely important that companies listen to the audience, the more because social media – and Facebook in particular - are well and truly a phenomenon of the contemporary world.

1.6 Structure

In order to answer the research question, this paper is structured as follows: section 2 will demonstrate some definitions and theories about privacy in general, with special focus on the privacy paradox. Facebook as a company will be further analyzed, including its Data Policy and there will be provided more information about the privacy settings. Then section 3 tells more about research that has been done before, especially aimed at the online privacy experience in the Netherlands and how Dutch people deal with privacy on Facebook. This paper is a complement to the latter research. In section 4, the Methodology part, the experimental design will be discussed. There will be explained how the questionnaire is constructed. Section 5 shows the results of the investigation through a description of the statistics followed up by some testing statistics, where the significant outcomes will come up for discussion. The next section, section 6, will give a critical review: the limitations and options for further research will be mentioned. Finally, the conclusion in section 7 will obviously sum up the conclusions of this research.

2. Theoretical Framework

2.1 The right to privacy

There should be defined what is exactly meant by privacy. It should be noted that there is no consensus about a strict definition in the literature, because it has various meanings in different disciplines. One could think of a political, a juridical, a psychological or a philosophy context. An often seen definition is either the state in which one is not observed or disturbed by other people or the state of being free from public attention (Oxford Dictionairies, 2015). The damaged freedom could have been caused by the government, a corporation or on the individual level, for example between colleagues or in family relations. Scientific literature is definitely more precise in terms of definitions. Privacy could either be a psychological state, in the sense of ''being-apart-from-others'' or the ''right to be let alone'' (physically). From a more political perspective, it can be formulated as ''security against intrusion by government''. It could also be a form of having control over our own personal information, so having the right to keep information confidential (non-physically) (Parker, 1974). In this paper, the latter definition will be leading because of the digital context. The book Privacy and Freedom has gone beyond this and told us more about the benefits. According to this book, privacy enhances personal autonomy in society and can be defined as ''people's ability to control the terms under which their personal information is acquired and used'' (Westin, 1968). Personal information is information that can lead to identification of an individual. But how could privacy be explained in the context of social media? There is a negative relation between privacy and the online media: the more activity on social media, the more chance that one loses grip on privacy. Sharing too many data could be bad for your reputation. Above that, there is a clear risk of identity theft by cyber criminals in general. According to the 2013 Identity Fraud Report, there were 12.6 million victims of identity fraud in the United States in 2012 (Ozawa & Barlow, 2013). This means that there was one victim every three seconds in that year.

2.2 The privacy paradox

The privacy paradox is a key concept when it comes to the discussion about privacy rights (Barnes, 2006). The fundamental paradox shows that everyone emphasizes the importance of privacy, but in fact everyone shares personal details if it is required, and even on a voluntary basis. Practically, it is a contradiction in terminus between actual behavior and thoughts about the subject. This contrast does not only make sense for Social Media, but also for web shops for example. Trend Micro, a Dutch innovating company that strives to a world where digital information can be exchanged securely, investigated that about 62% of the Dutch social media users doesn't know how to limit the content they are updating on social media (Trend Micro, 2013). This could probably partially explain the paradox.

2.3 Facebook's Data Policy

Facebook offers a wide spectrum of different brands, services (like the Mobile app) and products. There are communication services (like Facebook Messenger) and advertising platforms. These services are covered by their Data Policy (Facebook Inc., 2015). But what kind of information does Facebook collect? There are eight categories of data collection in their Privacy Policy, depending on which services you use. Every single category will be summarized shortly to give an initial impression.

1. Things you do and information you provide

Facebook collects information that you provide when you use their services. This could be for example signing up for an account, communicating with others, sharing pictures or leaving a comment. Besides, Facebook collects where and when a file was created. Furthermore, Facebook knows what types of content you view and the frequency and duration of your activities.

2. Things that others do and information they provide

This category is almost similar to the first category. Facebook collects information that other people provide when they make use of their services. Included is also information about you, like when they are sharing a picture of you or sending a message to you.

3. Your networks and connections

Facebook collects data about people you are connected to. This means that the company has insight in how you are interacting and with whom you keep in touch. Facebook also collects information you provide if you upload this information from a device.

4. Information about payments

The fourth category contains the collection of data with regard to using Facebook's services for purchases and financial transactions. This could be donating for charity, purchasing something in a game or just buying something on their website. Apart from payment information, such as your credit card number, Facebook also collects other account and authentication data, like contact information.

5. Device information

Facebook collects information from and about the devices that one uses to install or to have access to their services, for example your mobile phone, computer or tablet. This goes along with very many data, like the hardware version, software names and software types, the strength of your battery, the strength of your signal and the operating system you are using. Also device location information is owned by Facebook, since they have insight in the Global Positioning System (GPS), Bluetooth and Wi-Fi signals. These positioning systems are developed to provide precise positional data. Finally, connection information, including browser type, language, time zone, mobile phone number and the name of your mobile operator are covered by category 5.

6. Information from websites and apps that use Facebook's services

When you visit a third-party website or apps that use Facebook's services, Facebook is able to collect information regarding these visits. Websites and apps could make use of Facebook's services by offering the so-called Like-button or a Facebook Log-In possibility. Facebook knows how one uses their services on those websites and apps.

7. Information from third-party partners

Facebook receives information about your experience or interactions with Facebook's third-party partners, when Facebook and the partners offer you services together.

8. Information from Facebook companies

Facebook gets information from companies that are owned or operated by Facebook (e.g. Facebook Payments Inc., Instagram LLC, Atlas, Onavo, Parse, Whatsapp Inc.), in accordance with their terms and conditions. Each company treats the individual's information differently. The aim of the cooperation between Facebook companies and Facebook is to support and develop their activities and optimize their services.

2.4 Service development

Facebook collects all kind of information to create a customized experience. In the commercial branch, the increased need to collect consumer data is on the one hand driven by competitive forces facing marketers and on the other hand it is due to consumers' desire for individualized attention and personalized communication. Facebook is not only a concept of commerce, but they are also offering special services. The data collection is therefore not especially meant to increase purchases. Instead, there are four goals that have priority, in which the Facebook users should occupy center stage. Actually, everything is focused on optimizing their services (Facebook Inc., 2015).

First of all, it is about providing, developing an improving their services. This means that Facebook is personalizing content and providing shortcuts or suggestions in terms of friend-suggestions or location-suggestions. Facebook is also trying to help you to check-in at for example local events or to tell your friends that you are nearby with the help of collected location information. Research and development aims to improve their services. Secondly, Facebook uses their data in order to communicate with you. They attach great importance to marketing and therefore they need a lot of communication with people that make use of their services. Above that, they want to interact with their users about their constantly changing terms and conditions. Furthermore, Facebook strives to match the

right adds to the right persons which results in making sure that everyone only sees the relevant adds.
Finally, the information is used for safety reasons. Facebook verifies accounts and activity to guarantee the safety and security of the users.

2.5 Sharing information: publicly versus privately

Facebook gives the option to choose the audience who can see what you share when you post something on your own profile. You can make your post either publicly available, just available for friends, members of a group or a customized group of individuals. The so-called ''only me'' option, makes it possible that the information is only available for your own eyes. Information is publicly available when you share it with a public audience – this could be on your own page, but also on a public forum or Facebook Page. In short, public information is available to everyone, including anyone who is off the service. As an individual user, you don't have influence on the availability of the accounts of other users. The person who owns the page decides for whom its posts are available, in other words; the audience. Leaving a comment on someone's publicly available posts or liking this kind of posts results in the fact that your comments or likes are visible for everyone.
Also apps, websites and third-party cooperations that use Facebook's services have insight in your information. For example, it is the case, when you are playing a game with your Facebook friends, that the game developer has insight in your activities in the game. Or, when you are using a third-party service, the third-party partner can look at your public profile. It is now possible for them to see your name, age, nationality, friend list, pictures, posts and other kind of data. The same policy holds for Facebook companies. Advertising partners only receive information from Facebook that not personally identifies you. They could tell them how their adds performed and what kind of people have opened them. Information is also transferred to suppliers and service providers. These people analyze how Facebook's services are used. They measure how many impact the adds have had. Last but not least, the collected information is used for academic and scientific research.

2.6 A manipulating technique: Framing

Aimed at answering the second part of the research question, there should be clarified how to define manipulation, or even more precise, psychological manipulation. Manipulation works mentally, because the mind is involved in making decisions. It is more or less an intellectual process. Psychological manipulation is a social influence that tries to change someone's behavior or perception through underlying techniques. For this research, the framing technique has been applied. Framing is a way of presenting information, with the aim of influencing the recipient's behavior (Maas, 2013). But what exactly is a frame? A frame exists of visual and language-related elements that are used to present a desired interpretation of the message (Jong, 2012). The idea behind the framing technique is that the frame surrounding a situation or issue is altering the recipient's perceptions. Key here is to choose words or representations that lead to inventing aspects which the intended recipients are most sensitive for. Frames could be used in multiple settings and could have many advantages: they stick in the mind and respond to emotions of the public (de Bruijn, 2011). It is a convincing strategy in communication without using arguments and without changing the actual facts (Tversky & Kahneman, 1986). The framing technique is mostly used in politics, media, journalism and advertising, sometimes consciously, but also often unconsciously. One example in marketing is that books sell well because they are in the top 10 presentation in the book shop. Another example on framing was applied by Chupa Chups lollipops. They presented a healthier image of their product by claiming that their product was fat-free. These products could happily be described as such, even if they are full of sugar. Framing could also be applied to win actions. A win action is a proposal that through attractive images and language invites a person to participate. The aim of win actions is to increase the amount of customers. An advertiser tries to respond to interests of potential customers in a smart way in order to create a need at the customer for his products.

3. Related literature and interpretation

3.1 The online experience

Recently TNO, a research institute in the Netherlands, has done an investigation in February 2015 on the online experience at the request of the Dutch minister of Economic Affairs (Roosendaal, Nieuwenhuis, Ooms, Bouman-Eijs, & Huijboom, 2015). The questions were really general and not applicable to a specific company or website. The survey was executed among 1006 Dutch consumers. First of all, the analysis looked at the general opinion of the respondents with regard to privacy. The Dutch population attaches great importance to the protection of their personal details. One has just little trust in the attitude of the use of these details. In the view of the respondents, commercial parties are too less reliable. Social Media, web shops and charity organizations are mostly criticized. It seems that almost 75% doesn't trust Social Media companies. According to the respondents, governments and public institutions, like the police and the tax authorities are more trustworthy. The privacy experience research was executed based on seven factors – three personal factors: personal details (age, gender, education level and daily hours spent on the Internet), experience (with identity fraud and trust in the performance of the government) and actual behavior (the use of several online services, the willingness to provide information and the reading of terms and conditions) – two contextual factors: context (in which organizations ask for information and are being trusted) and type of technology (that is used to collect information) – and finally two factors that create framework conditions: influence & control (the need for control and privacy protecting techniques) and awareness (knowledge of the social playing field and risks). Consumers do not always know how to protect their details. However, 88.5% claims to install protecting software and 68.4% says that they have changed the profile settings. Two other percentages are worth to keep in mind for the rest of this paper: It is very remarkable that just 12% of the respondents claims to know who has insight into their data. Almost half of the respondents claims to read terms and conditions, which is relatively high compared to other countries.

3.2 How to deal with privacy on Facebook?

This paper will be complementary to another research among 1500 Dutch people by Maurice de Hond, who is famous in the Netherlands because of his opinion surveys for his profession. Key to this survey is privacy settings on Facebook and how to deal with the privacy-related concerns according to users and non-users of Facebook (van Hoek, 2013). This research is more company-specific than the research of TNO. The majority of the respondents, namely 1035 respondents, appeared to have a Facebook-profile, which is 69% of the respondents.

The respondents were divided in three age categories: younger than 30, between 30 and 50, and older than 50 years old. This investigation has shown that the older the target audience, the less they knew about the default privacy settings on Facebook and the less they adjusted these settings. On average, 88% of the respondents was aware of Facebook's Privacy Policy and 79% has amended the settings at least once. More than half of the respondents seemed to have difficulties with the fact that everyone, users as well as non-users of Facebook, is able to find their profile. Especially young people cared about this. This could explain that younger people in particular want Facebook to change its Privacy Policy. In total 79% of the respondents found this important, although older people did not consider the current Facebook Policy as a real issue.

4. Methodology

4.1 Experimental Design

To investigate whether one is willing to pay for privacy on Facebook and how to manipulate this willingness to pay, the creation of a survey was required. To look at the amount one wants to pay, the CV method is used (as described in paragraph 1.6). As can be derived from the research question, this paper is not focused on social media in general, but on Facebook specifically, since this is the most used networking platform worldwide at this moment. To make sure that the research became as reliable as possible, it was desirable that the respondents had already heard of the site and knew what the aim of the platform is, before they started with the questions. The survey was completely anonymous. Owners as well non-owners of a Facebook account were asked to participate in order to secure the widest possible sample. The English version of the Dutch survey has been attached in Appendix I. The distribution of the survey was executed via Facebook to reach Facebook users and via e-mail and face-to-face to reach respondents without an account on Facebook. On top of that, people were asked to share or forward the link to the survey[1]. The website Qualtrics (www.qualtrics.com) was used because of the big choice in question types and the useful initial report, which gives an overview of the results directly. Initially the aim was to reach at least 200 people with the survey. However, the time did not allow this goal. Therefore, sometimes one needs to be satisfied with less, so a minimum number of 100 respondents was necessary to represent the Dutch population as a whole.

[1] The distribution of the survey has been done partially via email to some family members, colleagues of my mother and some friends of my father without a Facebook account. We knew that they all had the Dutch nationality and were all above 18 years old. The survey has been distributed via Facebook several times to reach Facebook users. It was also asked to my Facebook friends if they were willing to share it with their friends and family. Many people have done this. In the invitation it was made clear that it was meant for people older than 18 years old with a Dutch nationality. Unfortunately I didn't put a question in the survey that controlled for nationality. Besides the email and Facebook distribution, I have talked to some friends and family face-to-face. I told them that I would be very grateful for their help if they would fill it in. It is unknown how many respondents are from face-to-face distribution.

4.1.1 The use of a survey

Many economists are very skeptic towards the use of survey data, because they are often convinced that respondents do not take the questions very seriously. It might indeed be true that there exists a discrepancy between the answers that the respondents reported and their actual behavior. A counter argument could be that surveys are more user-friendly for the respondents. They can make it whenever and wherever they want, which stimulates them to fill it in at their own rate. The survey was also created in their own language to make it easier for them. On top of that, the data of an online survey could be collected immediately.

4.2 The content of the questions

The purpose of the research was to collect as many data of the respondents as necessary, focusing on making the survey not too long. If matters take too long, respondents will lose interest. To avoid possible priming effects, questions about personal details were put in the end. Priming works purely psychological and is a non-conscious form of human memory concerned with perceptual identification of words/objects. Thus, the gender, age and level were asked at the end. The same age categories were used as in the survey of Maurice the Hond. Furthermore, in the Netherlands there are three education levels after primary- and high school, called Middelbaar Beroepsonderwijs (MBO), Hoger Beroepsonderwijs (HBO) and Wetenschappelijk Onderwijs (WO). MBO is comparable with Intermediate/Medium Vocational Education and HBO is almost the same level as Higher Vocational Education. WO is the education level that equals studying at University. The research starts with a very essential question: whether one has a Facebook account or not. Both users and non-users were asked to give their arguments about joining the social media site or not. Did users choose to go on Facebook to keep fully informed about their family and friends or because they are maintaining a business account? In contrast, don't the other ones have a Facebook account because of privacy concerns or don't they like Social Media by definition? One question also tries to distinguish between active and passive users. Active users, as mentioned in the survey, are defined as users that share pictures, videos and status-updates with a certain regularity and/or look sometimes in the news overview and on other people's profiles. On the contrary, passive users just pay little attention to Facebook.

Then the first question with regard to privacy was asked: ''How important do you find privacy in general, on a scale of 1 to 10, where 1 is totally not important and 10 is very important?'' After this question, there followed eight sub questions. Before every question, there was a short description with an explanation of the category, so that the respondents were able to answer these questions matching with their opinion. As mentioned in the Theoretical Framework, the categories were as follows: Things that you do & information that you provide, Things that others do & information that they provide, Networks & connections, Payments, Devices, Websites & apps, Facebook companies and External Partners. Given these categories including the explanation, respondents were asked how they would grade each category (also on a scale from 1 to 10) in terms of the extent in which they would like to protect their information, not only from Facebook as a company, but also from Facebook's third-party partners and clients. The research became more privacy- and company specific with these questions. After this, questions came up that approached the research question of the paper, like ''How often would you be willing to pay a financial fee in order to guarantee your privacy?'' The possible answers were ''Never'', ''Once'' and ''Yearly''. To measure how much everyone values privacy, respondents were asked how much they were willing to pay for each of the mentioned categories, in case it was just a one-off payment, with a maximum of eight Euros.

Finally the survey went to the second part of the research question: could the willingness to pay for privacy be manipulated? Protecting the privacy through to payment of a fee on Facebook excludes the presentation of win actions on the users Facebook account. Thus, when a user would like to participate in win actions, the user has to give up more of his privacy. It would be interesting to know if people who initially cared a lot about their right to privacy, now care less about their privacy, because otherwise they cannot participate in these win actions. The respondents were asked to suppose that Facebook organizes and promotes different kinds of win actions in certain age categories. The presentation of these actions has been made attractive for the (potential) users. Here, the framing technique has been applied. Two examples of these chances to win are given to the respondents. One of these examples is as follows: ''You are a 20-year-old Dutch boy and Facebook knows that you love soccer, because of your pictures and messages of your soccer team. You are eligible to win 2 tickets to the next World Championships of Soccer, because you are between 18 and 25 years old and you live in the Netherlands.'' Does their willingness to pay for privacy change by these advantages?

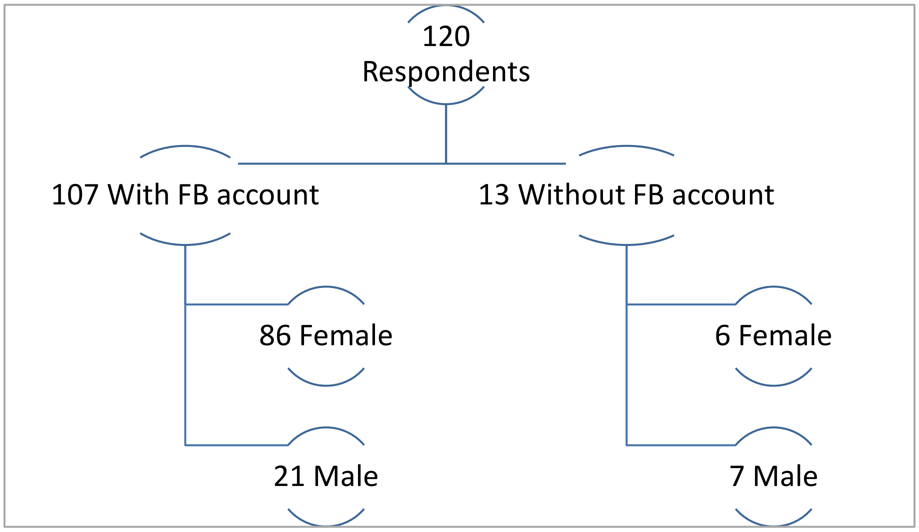
5. Results

The questionnaire was online for about two weeks, to be more precise, between May 27th 2015 and June 9th 2015. There were 120 respondents that started and completed the survey. First of all, there will be implemented some descriptive statistics. The trimmed mean of the survey duration was 12 minutes.

5.1 Descriptive Statistics

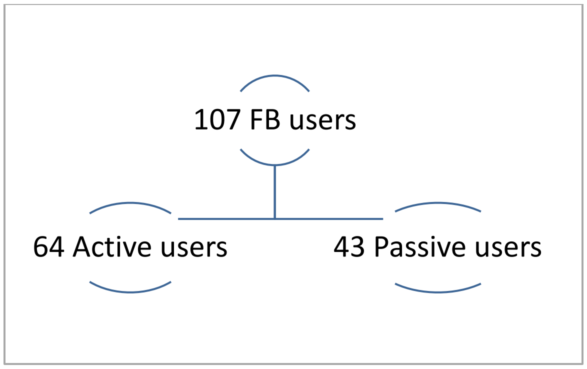
5.1.1 Features of the respondents

Among the respondents, there were 92 women and 28 men. The organization chart in picture 1 shows that there appeared to be 107 Facebook users. Of these 107 people, 21 were male and 86 were female. This means that just 13 respondents did not have an account while reporting, of which 7 were male and 6 were female.



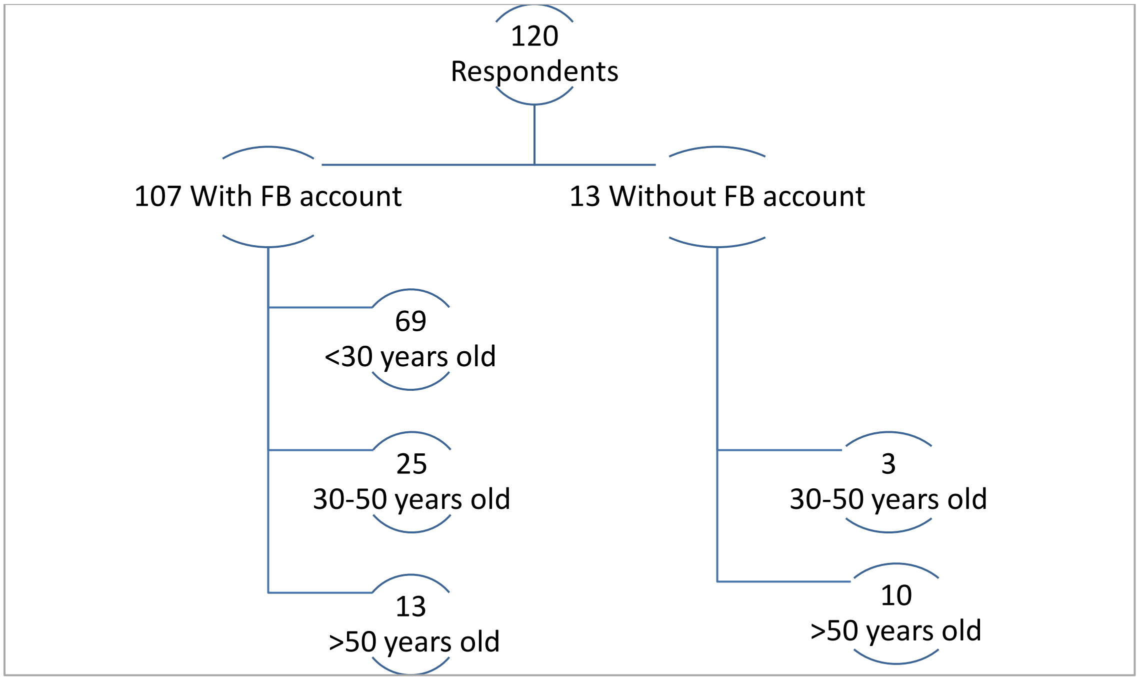
Picture 1

One question also tries to distinguish between active and passive users. It seems that 60% of the Facebook users describes themselves as more active than passive on Facebook, while the other users considered themselves as more passive, as can be seen in picture 2.



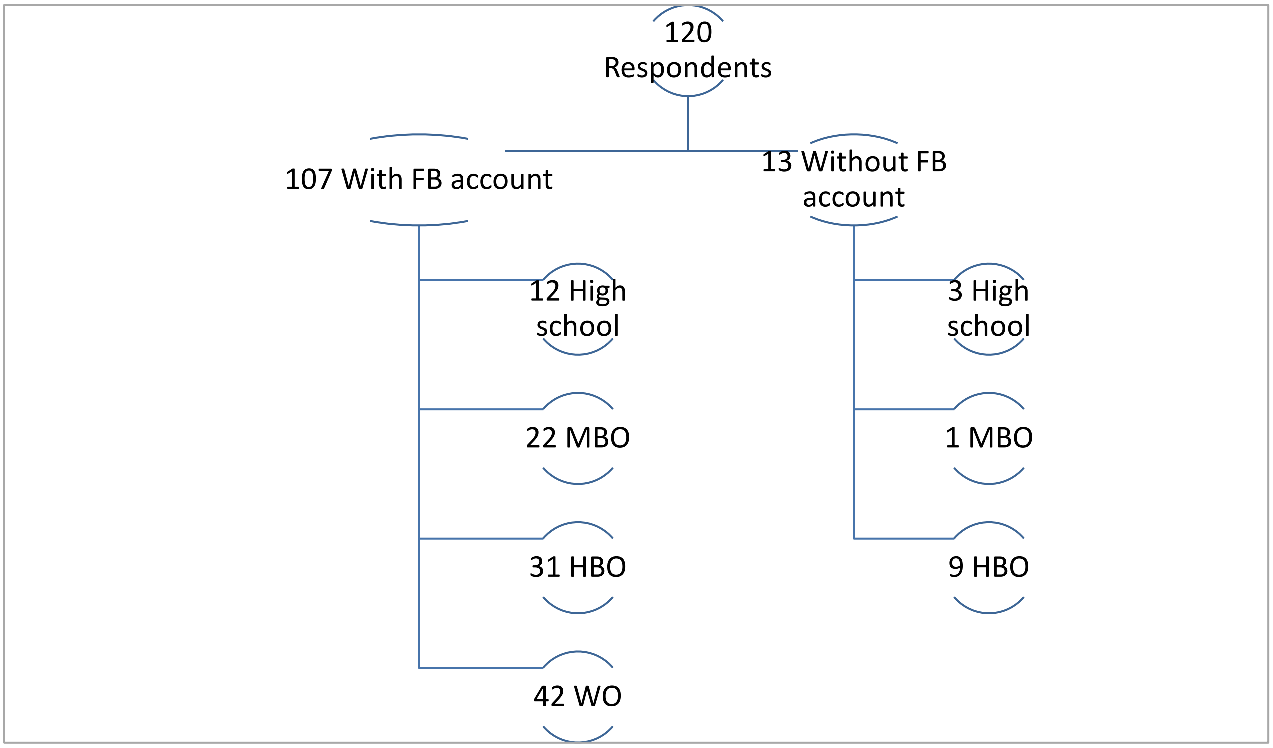
Picture 2

Fifty-eight percent, so 69 respondents were younger than 30 years old. Everyone in the youngest category had an account on Facebook. Twenty-three percent was somewhat older and belonged to the between 30 and 50 year old category, this were exactly 28 people. Just three of them did not have an account on Facebook. The oldest category, the 50 plus category, contained 19% of the respondents, which equaled 23 people. Among these, there were thirteen Facebook users. These amounts are shown in the organization chart in picture 3.



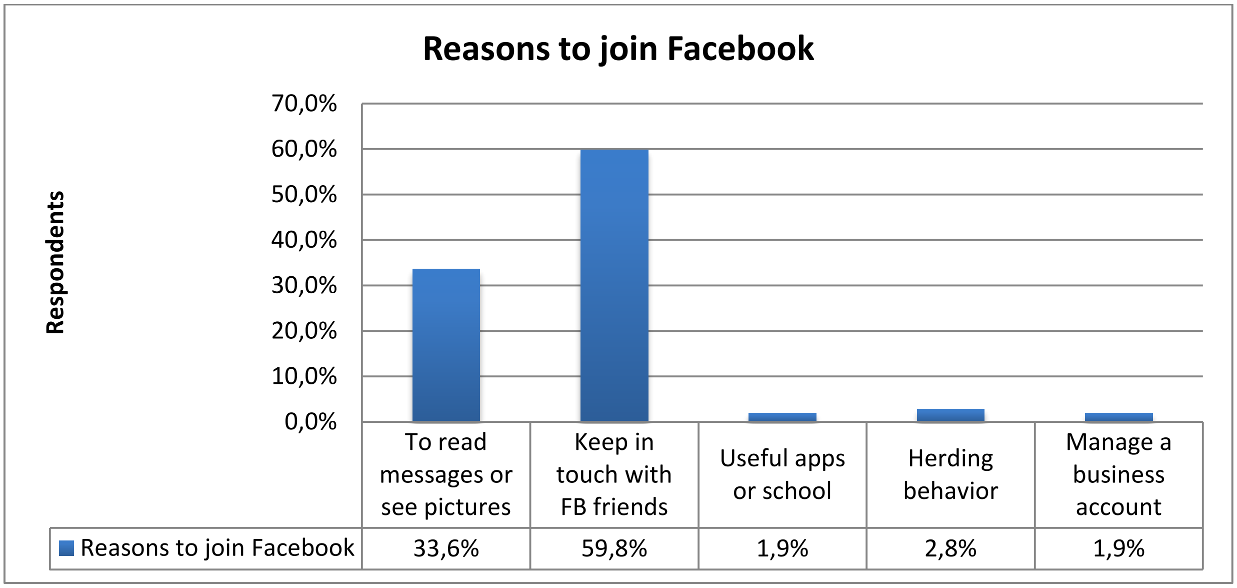
Picture 3

The last organization chart in picture 4 shows the education level of the respondents. These levels were described in paragraph 4.2. In total, there were 15 persons that only completed high school. Just two of them, did not have a Facebook account. Twenty-three respondents have finished the Dutch MBO education level. Among them, there was just one person without a Facebook account. The biggest group that filled in the survey is studying at the University or has a University degree. They all joined Facebook. And finally, the Dutch HBO education level contained 40 respondents. The most people without a Facebook account were found in education level HBO.



Picture 4

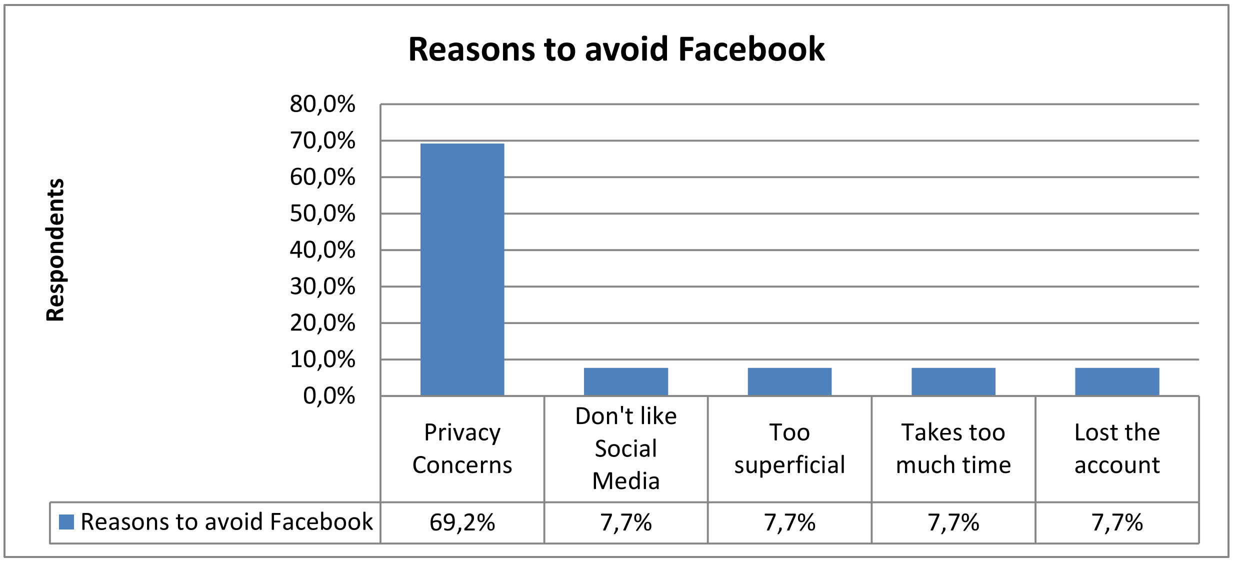
Owners of a Facebook account were asked why they decided to join Facebook. The histogram in picture 5 shows that the majority of almost 60% has a Facebook account, because they want to keep track of the pictures and messages of their friends and family. The second biggest reason is that the users want to keep in touch with their Facebook friends. A few others emphasized that Facebook was necessary or useful to use apps (e.g. games) or to make school tasks. Then there were two respondents that needed Facebook to maintain a business account and three respondents admitted that they followed herding behavior, in terms of creating an account just because others did it too and they otherwise would have felt a little bit old-fashioned.



	To read messages or see pictures	Keep in touch with FB friends	Useful apps or school	Herding behavior	Manage a business account
🟦 Reasons to join Facebook	33,6%	59,8%	1,9%	2,8%	1,9%

Picture 5

The thirteen respondents without a Facebook account were asked a similar question: why don't they use Facebook? Nine of them (so almost 70%) made a conscious choice to avoid Facebook because of privacy concerns. There was one respondent that brought forward that he/she didn't like Social Media at all. Another person simply lost its account details. According to the other two respondents, Facebook either takes too much time or the way of contact is too superficial: the respondent concerned preferred to keep in touch with friends and family by telephone. These figures are shown in picture 6.



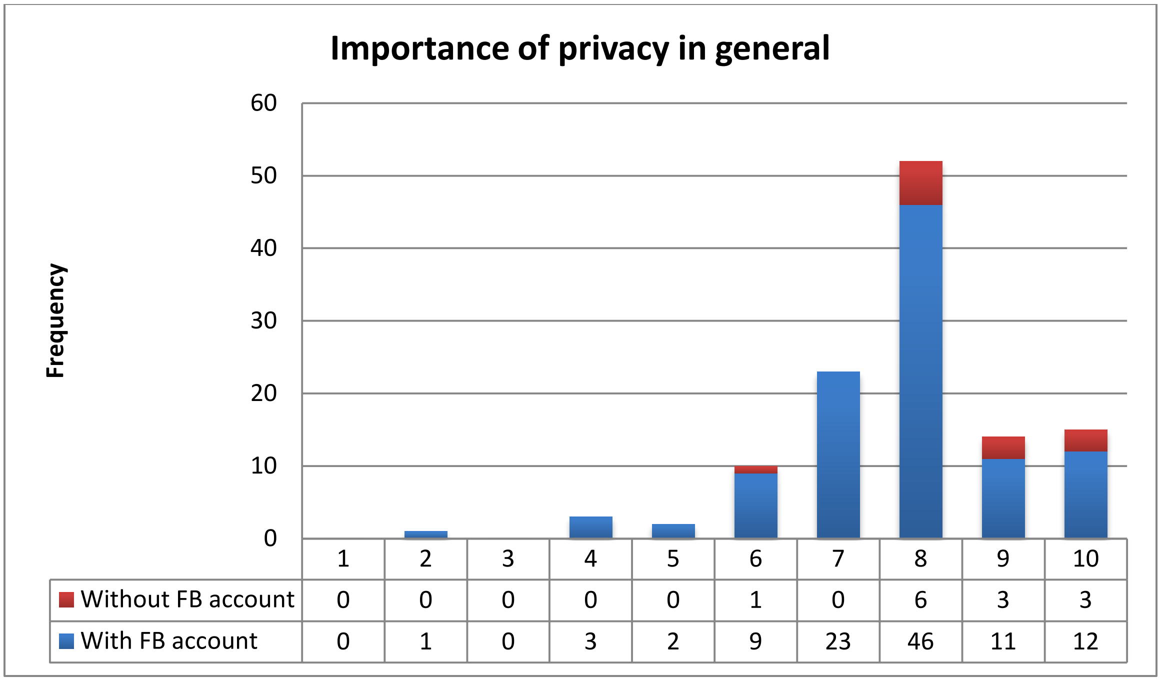
	Privacy Concerns	Don't like Social Media	Too superficial	Takes too much time	Lost the account
🟦 Reasons to avoid Facebook	69,2%	7,7%	7,7%	7,7%	7,7%

Picture 6

Although there were fewer men than women and the category of respondents without a Facebook account was under-represented in the sample, the Dutch sample was (with a certain margin for error) still representative for the Dutch population. However, it would be more ideal to have larger groups with better-distributed variables.

5.1.2 Privacy related opinions

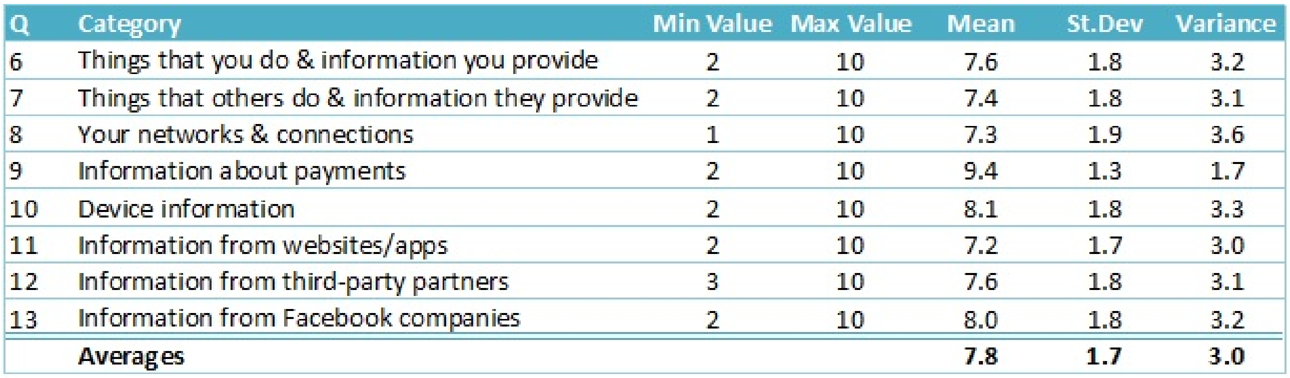
On average, people graded importance of privacy in general with 7.8. A high grade was already expected, because earlier research showed that most people think that privacy is very important. The exact answers are shown in picture 7. The mean of the group that joins Facebook was 7.7, while the group that does not join Facebook had a mean of 8.5. This matches with the most given reason of this group to avoid Facebook: they care very much about their right to privacy – apparently not only on Social Media, but in general. It is striking that almost half of the respondents (43.3%) graded this question with an 8.0. The minimum value given was 2.0 (just given by one person) and the maximum value was a 10.0 (given by 12.5% of the respondents). It can be seen that the respondents that were younger than 30 years old graded this question with a 7.7 averagely, whereas the mean for the two age categories above 30 years old both were 8.0.



	1	2	3	4	5	6	7	8	9	10
🟥 Without FB account	0	0	0	0	0	1	0	6	3	3
🟦 With FB account	0	1	0	3	2	9	23	46	11	12

Picture 7

In picture A till H of the Appendix, one can see how everyone rated the different categories of information that Facebook collects. The table below in picture 8 shows the more statistical data of these concerned questions, like the range, mean, standard deviation and variance. Definitely, the category that the respondents wanted to protect most is the information about payments. This seems a very important category, with an average grade of 9.4 for the majority and 85 people gave this category a grade of 10. The second most important category is the device information. The mean of this category was 8.1. Almost every category was rated between 2 and 10. The least important category seemed to be the information from websites and apps that use Facebook's services. Overall, these questions are assessed with a 7.8 on average. The standard deviation per category was not higher than 1.9 and the mean of the variance was 3.0.

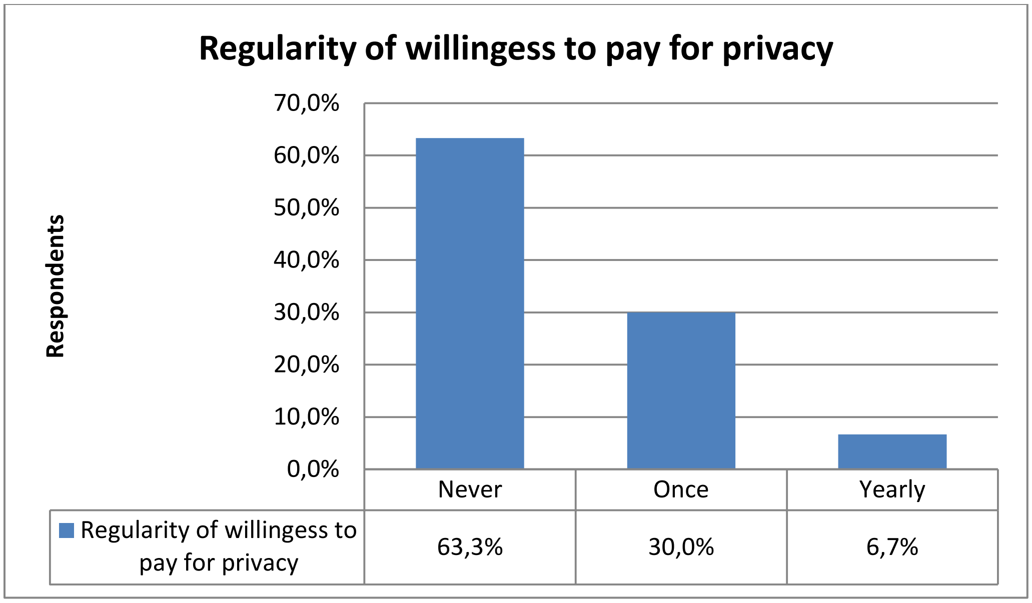


Q	Category	Min Value	Max Value	Mean	St.Dev	Variance
6	Things that you do & information you provide	2	10	7.6	1.8	3.2
7	Things that others do & information they provide	2	10	7.4	1.8	3.1
8	Your networks & connections	1	10	7.3	1.9	3.6
9	Information about payments	2	10	9.4	1.3	1.7
10	Device information	2	10	8.1	1.8	3.3
11	Information from websites/apps	2	10	7.2	1.7	3.0
12	Information from third-party partners	3	10	7.6	1.8	3.1
13	Information from Facebook companies	2	10	8.0	1.8	3.2
	Averages			**7.8**	**1.7**	**3.0**

Picture 8

About the next question, 85.8% of the respondents (101 persons) thought that it was a strange idea to pay for privacy on Facebook. Most of them rightly considered privacy as a human right. Some other people found that it should be enough to just pay for an Internet connection. Maybe they did not think of paying for privacy (or whatever right) before they filled in this survey. Therefore, it could sound as a crazy thought. Contrasting to these people, there were 17 people that were more positive about paying for privacy, which is a 14.2%. They agreed with the fact that it might be a necessary change in a world that becomes more digital. Some respondents noted a condition that people should be better informed about their own responsibility.

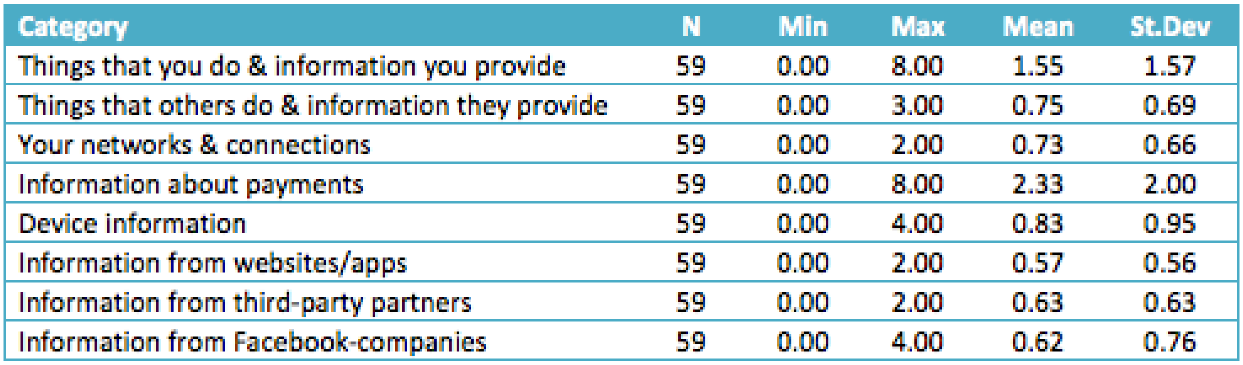
It is, however, surprising how many people are willing to pay just once to guarantee their privacy on Facebook, namely 30% of the respondents (or, 36 out of 120 persons). This is striking compared to the question before about the strangeness of the idea to pay for privacy. The results of this question are shown in picture 9. The term ''pay'' could have had a discouraging effect, because for example household members or students did not want to have additional fixed costs every month. The fact that there was not mentioned a certain regularity of paying in the previous question could have scared some respondents off. This question therefore focused on the regularity. There were still 76 respondents, so 63.3%, that would never be willing to pay for privacy anyway. At the same time, there were eight people, so 6.7%, that wanted to pay at least a yearly fee. Adding a regularity in the question leads to 31 people that found it initially a strange idea to pay for privacy, that now want to pay at least once or even yearly.



Picture 9

5.1.3 Willingness to pay for privacy

The following question was more money specific: how much would one be willing to pay once for each mentioned category in order to guarantee their privacy. The intention was to require a maximum of 8.00 Euros in total, divided over eight categories. This range was invented in order to keep the standard deviation low and to compare averages easily. There has been computed an additional variable (Total WTP) to sum the amounts per category for the purpose of knowing how much one is willing to pay for the categories together. Although the ''maximum of 8.00 Euros'' was emphasized in the textbox above the question, it was not applied in the settings of the survey. More practically, there was made a technical mistake. Initially, respondents could fill in whatever amount they wanted, except for a total of 0.00 Euros, which was a technical mistake. The survey was already a few days online before this was noticed and changed correctly on the website. Furthermore, a lot of people have misinterpreted the question. For example, the mean of the Total WTP was 9.54 Euros, more than people should have paid in total. The descriptive statistics including frequencies can be seen in figure I and J of Appendix II. Unfortunately, the results of this question have therefore to some extent been weakened and could not be used for the initial meaning. The willingness to pay is unreliable because of the huge differences in answers. However, this question could be used for another purpose now. There were 59 people that wanted to pay 8.00 Euros in totals spread over eight categories. The following assumption is made: if they did not want to pay anything, they would not have paid 8.00 Euros in total, but then the amount was likely to be less than 8.00 Euros. There has been added a filter in order to deselect everyone that did not have a total willingness to pay of 8.00 Euros. The descriptive statistics are shown in picture 10. On average, one is willing to pay the most to protect information about payments, namely 2.33 Euros. This was more or less expected because people found this the most important category. Also not surprisingly: people did attach the least importance to the protection of information from websites and apps that use Facebook's service and it seems that they want to pay the least for this category too (0.62 Euros). There seems to be a certain hierarchy or pattern for these two categories in particular, at least among the 59 mentioned persons. This result could be assumed as reliable, because after all, the size of this group is almost half of the respondents. Looked at the whole respondents sample, it can also be concluded that the relative willingness to pay for the ''information about payments'' category is the highest (mean: 2.80) and the lowest for the ''information from websites/apps'' category (mean: 0.63). Although some people understood this question wrong, this information is still informative. The table for the sample of 120 respondents can be found in figure K of Appendix II.

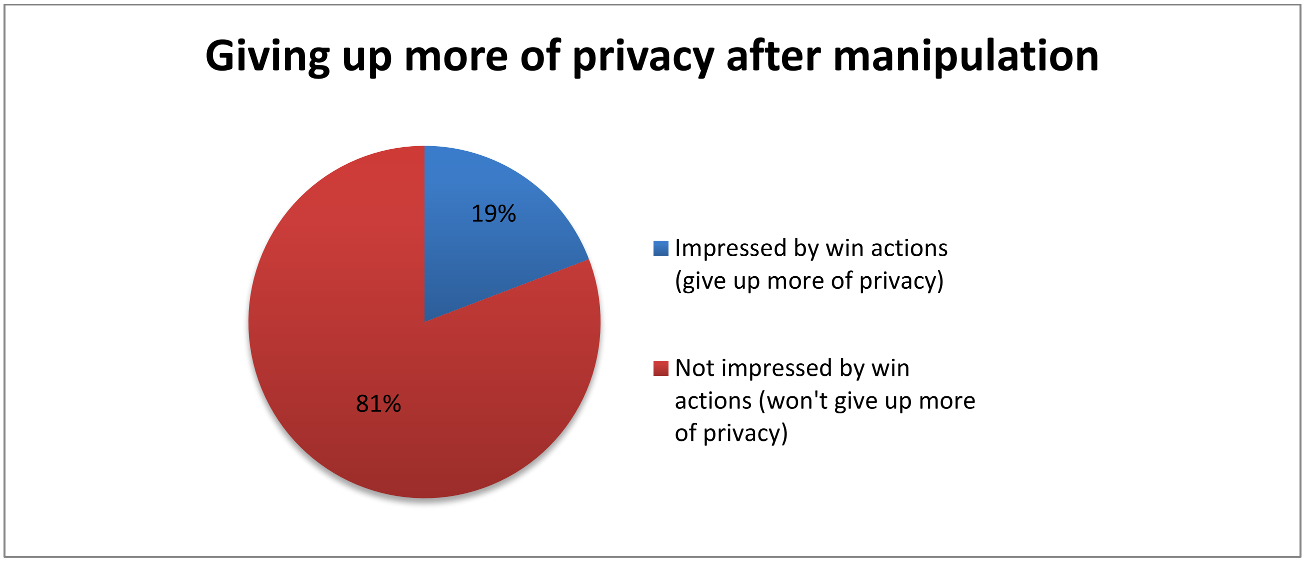


Category	N	Min	Max	Mean	St.Dev
Things that you do & information you provide	59	0.00	8.00	1.55	1.57
Things that others do & information they provide	59	0.00	3.00	0.75	0.69
Your networks & connections	59	0.00	2.00	0.73	0.66
Information about payments	59	0.00	8.00	2.33	2.00
Device information	59	0.00	4.00	0.83	0.95
Information from websites/apps	59	0.00	2.00	0.57	0.56
Information from third-party partners	59	0.00	2.00	0.63	0.63
Information from Facebook-companies	59	0.00	4.00	0.62	0.76

Picture 10

5.1.4 The impact of win actions

Now, the results of the impact of the win actions will be discussed. There has been examined if it is possible to affect the willingness to pay for privacy based on a manipulating technique: framing (as explained in the Theoretical Framework). The framing technique was applied by the suggestion that Facebook now organized some ''win actions'' per age category based on the preferences of their users. For example, Facebook has insight in the love for cooking of a 42-year-old Dutch woman, because the company can look at her messages and pictures. The idea is that this woman – based on her preferences, age and country- eligible to win a professional tableware set. Did the win actions have impact on people? Would people care less about their right to privacy through the introduction of these win actions? The word ''win action'' should attract the audience and influence them in a direction where they are convinced to lower their standards concerning their privacy. The manipulation method has worked well to 23 people, so to 19.2% of the respondents. The win actions have created a positive representation at them, so this has resulted in wanting them to give up more of their right to privacy. They would not mind if Facebook would have insight in their messages and pictures, because they like the win actions. However, four-fifths of the respondents were not impressed by the introduction of these actions. The results of this part are shown in picture 11.

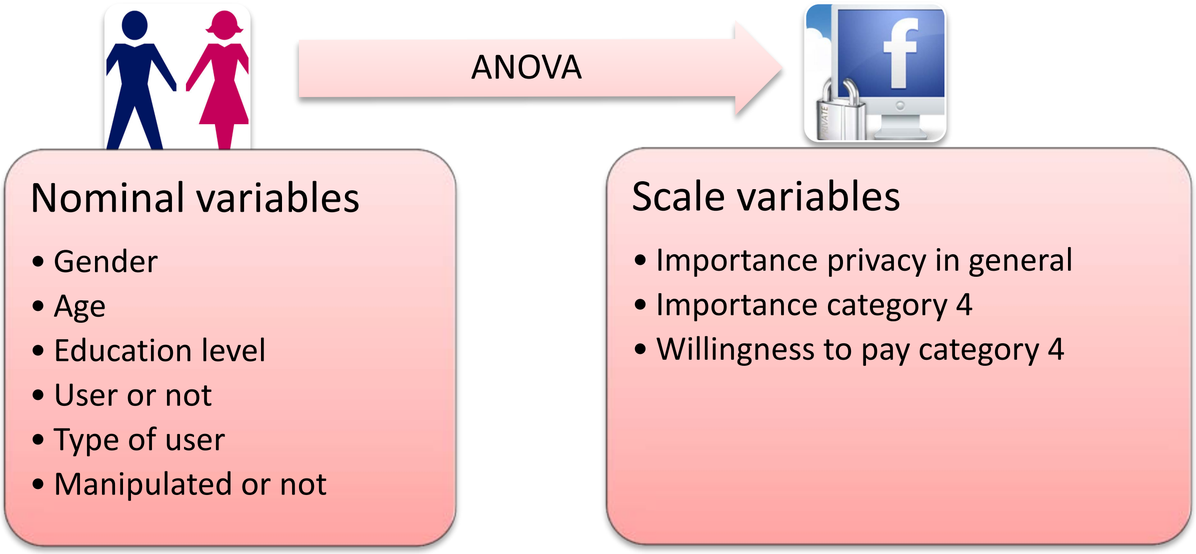


Picture 11

Due to the possibility of various interpretations of question 18 (see Appendix I) the answers of this question were not analyzed in this paper.

5.2 Testing Statistics

Some remarkable results could be further analyzed. Now it is important to compare groups in terms of means. This is done by multiple one-way between-subjects analysis of variance (ANOVA) tests. There are four assumptions to apply an ANOVA: means are allowed to differ within groups, the number of observations might differ per group, in every group there should be a normal distribution and there should be an equal variance within each group. Following the procedures for running an ANOVA, means that for every single test one continuous (scale) variable and one categorical (nominal) variable with two or more levels have been used (Meyers, Gamst, & Guarino, 2006). The General Linear Model has been applied multiple times. The aim is to find significant differences between means through the analysis of variances. There has been focused on the means of three dependent variables: the importance of privacy in general, the importance to protect information about payments and the willingness to pay for this category in particular. This category was graded highest in importance as well as chosen as the category one was willing to pay the highest amount of money for. There have been used six specific nominal variables in terms of independent variables: owning a Facebook account or not, active versus passive users, manipulated by the win actions or not, male versus female, different age categories and education level differences. These variables have been chosen because these are the most essential for this research. A scheme is attached in picture 12 to clarify which tests (6 times 3 in total) have been executed. The last two called variables exist of three or more groups/levels, but fortunately ANOVA is able to compare these groups. The only thing that is necessary in addition is a so-called Tukey's Honest Significant Differences (HSD) Post Hoc test for these nominal variables with three or more groups.



ANOVA

Nominal variables

- Gender
- Age
- Education level
- User or not
- Type of user
- Manipulated or not

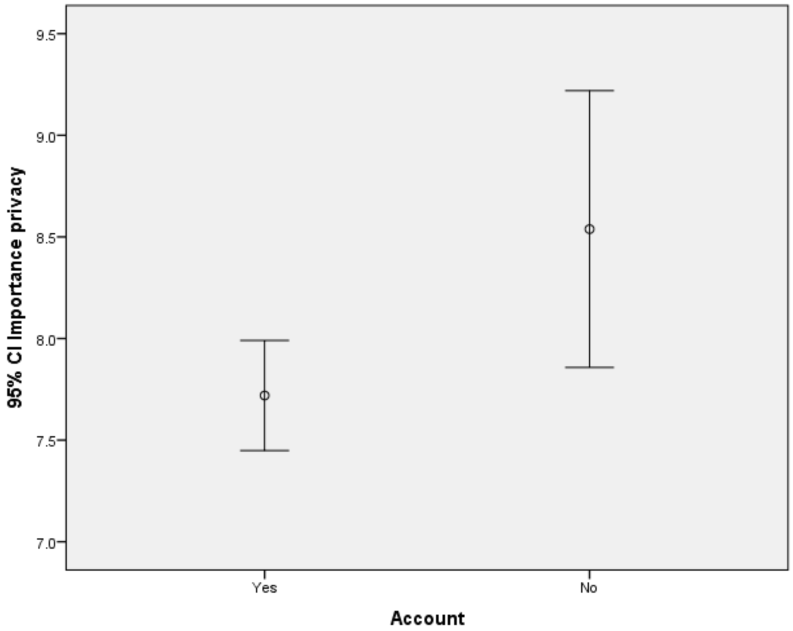
Scale variables

- Importance privacy in general
- Importance category 4
- Willingness to pay category 4

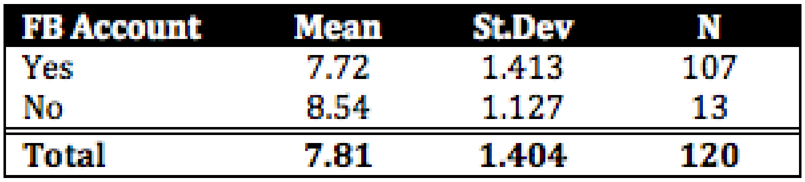
Picture 12

Differences in the means of men versus women could not significantly explain differences in none of the three mentioned scale variables and so didn't the means of different age categories, education levels, active versus passive users or the fact of one was manipulated or not by the framing technique. The differences between the means within groups were not big enough.

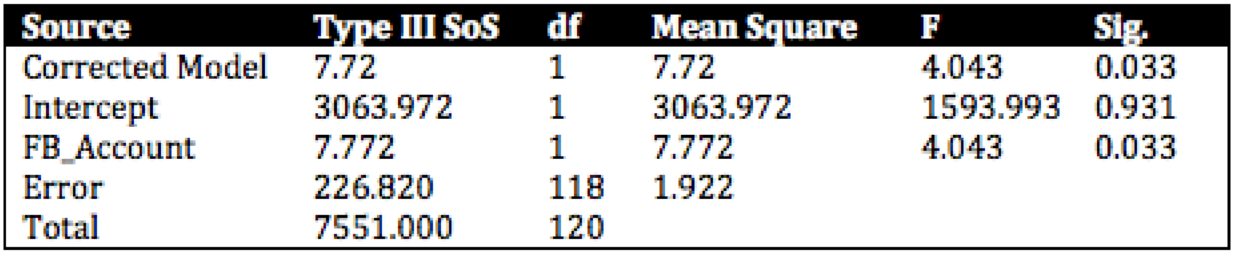
A one-way between-subjects ANOVA compared the mean importance of privacy in general ($M = 7.8$) from respondents that had an account versus did not have an account on Facebook. The error bar chart is shown in picture 13, where on the left one can see the average privacy importance of users and on the right the average privacy importance of non-users of Facebook. For the SPSS output, including descriptive statistics, one can look at picture 14. This assessment was statistically significant on a 95% Confidence Interval, $F(1, 1, 118) = 4.04$, $p < 0.05$. This indicated that the mean of non-users of Facebook ($M = 8.5, SD = 1.31$) was significantly higher than the mean of users of Facebook ($M = 7.7, SD = 1.13$). This outcome could be interpreted as follows: people that do not join Facebook find their privacy much more important than people that join Facebook. This is consistent with the reasons why non-users did not have an account: almost 70% had chosen to avoid Facebook because of privacy concerns.



Picture 13



FB Account	Mean	St.Dev	N
Yes	7.72	1.413	107
No	8.54	1.127	13
Total	**7.81**	**1.404**	**120**

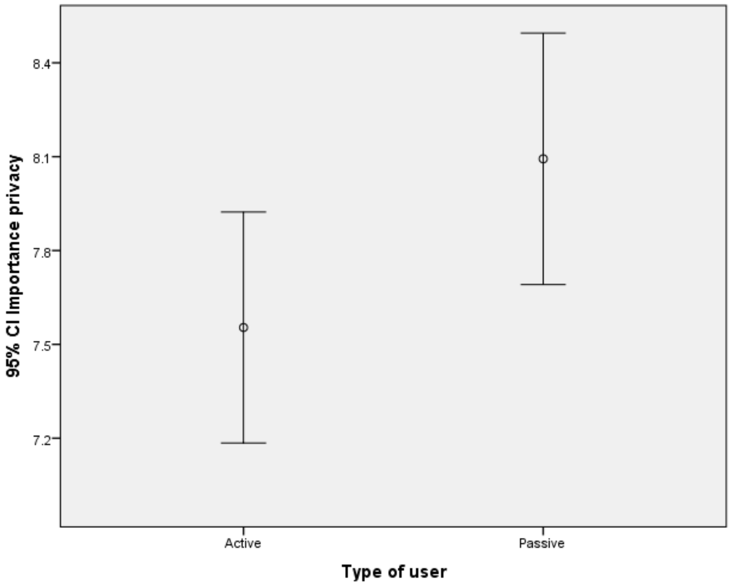


Source	Type III SoS	df	Mean Square	F	Sig.
Corrected Model	7.72	1	7.72	4.043	0.033
Intercept	3063.972	1	3063.972	1593.993	0.931
FB_Account	7.772	1	7.772	4.043	0.033
Error	226.820	118	1.922		
Total	7551.000	120			

Picture 14

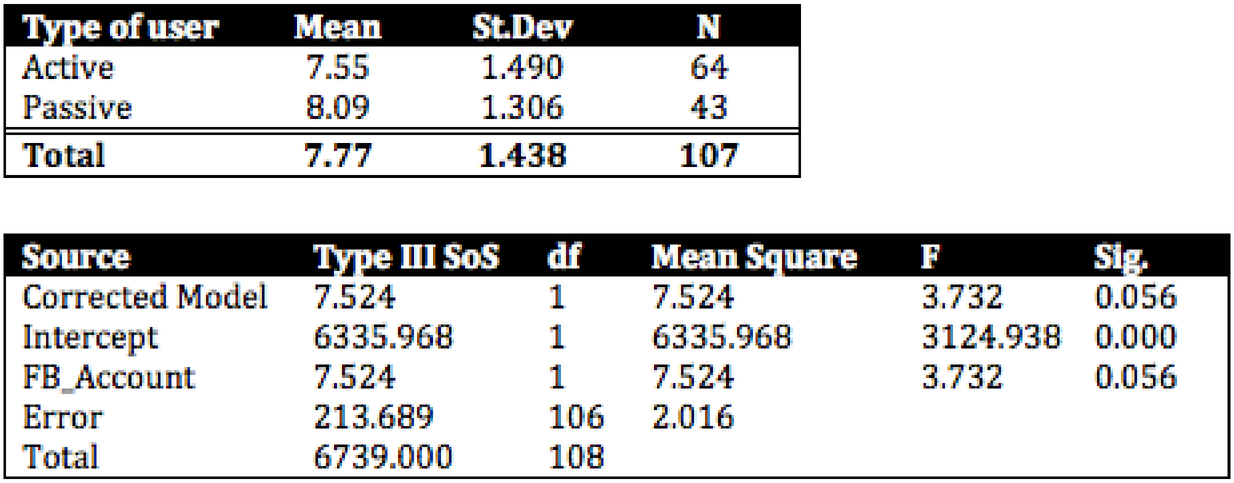
6. Further research and limitations

Some outcomes were close to significant. The nominal variable, that indicated if people described themselves as rather active or passive, gave a remarkable result. A one-way between-subjects ANOVA compared the mean importance of privacy in general (*M = 7.8)* from active versus passive users. To see the variance of the means of active versus passive users, one can look at the error bar chart in picture 15. The SPSS output with the descriptive statistics table and the between-subject effects table can be seen in picture 16, below the error bar chart. On the left there is the error bar for the active users of Facebook and on the right is the error bar for the passive users of Facebook.



Picture 15

This visualizes that the mean of passive users (*M = 8.1, S = 1.31*) is almost significantly higher than the mean of active users (*M = 7.6, S = 1.49*) as can be seen in table one of picture 16. This could be explained as follows: perhaps passive users are not that active because of privacy concerns. They simply attach more value to privacy. Although there was no significance (*p = 0.056 > 0.05*), the user type variable could be analyzed in further research. A limitation could be that this variable is based on a self-assessment, so it is probably not reliable enough. However, in the future, making a division between active and passive users could be based on real Facebook activities.



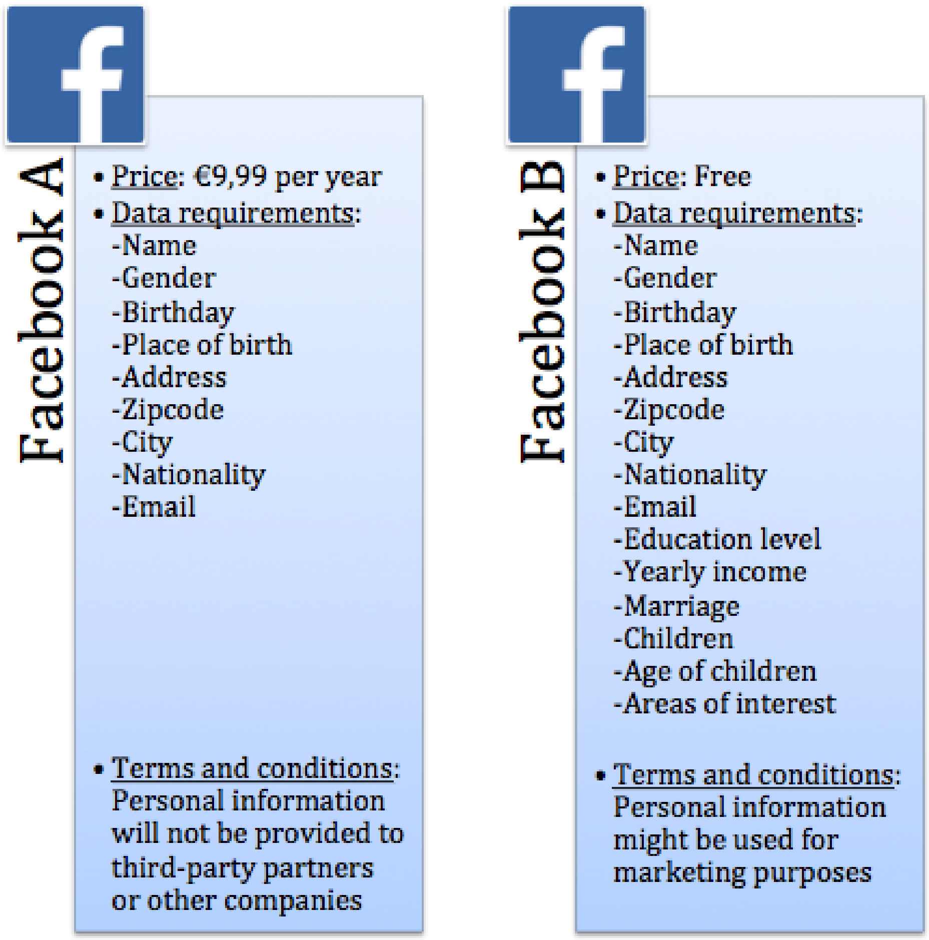
Type of user	Mean	St.Dev	N
Active	7.55	1.490	64
Passive	8.09	1.306	43
Total	**7.77**	**1.438**	**107**

Source	Type III SoS	df	Mean Square	F	Sig.
Corrected Model	7.524	1	7.524	3.732	0.056
Intercept	6335.968	1	6335.968	3124.938	0.000
FB_Account	7.524	1	7.524	3.732	0.056
Error	213.689	106	2.016		
Total	6739.000	108			

Picture 16

Respondents were asked (question 16, Appendix I) how much they would pay for privacy per category that was mentioned in Facebook's Data Policy. Maybe this question was open to a number of different interpretations, or this question was a little excessive. The formulation of this question could have been the problem, but this could be improved in further research. The formulation was as follows: ''*Suppose that the amount of the one-off financial fee is build from protecting the 8 above categories, mentioned in Question 6-13. The more you are willing to pay for each category, the more you want this category to be protected. You can pay a minimum of 0.00 Euros and a maximum of 1.00 Euros per category. This means that you should spend a maximum of 8.00 Euros to protect your privacy on Facebook.''* It seems that the third sentence has created confusion among the respondents, so it would be better to formulate it as follows: ''*You can divide 8.00 Euros over all categories. It is also allowed to spend 0.00 Euros to a category if you want.*'' Unfortunately, question 18 (Appendix I) was also open for discussion. Therefore, this question was skipped from the analysis. This question was meant as a control question to see if respondents that were initially very protective about their private information, would have changed their opinion through the win actions.

There are alternatives for future research concerning the way of measuring the willingness to pay for privacy on social media. One possibility is shown in picture 17: Suppose that there are two almost identical Facebook websites. The platforms differ in three ways: in price (B: Free, A: €9,99 per year) and in data requirements (B: many data required, A: less data required). Besides that, personal information might be used for marketing purposes at Facebook B, while personal information at Facebook A won't be provided to third-party partners or other companies. This example could be used in future research to see if respondents would rather join a paid privacy protecting Facebook (A) or a non-paid Facebook (B) that shares your data with third-party partners and companies. This could be an improvement for upcoming investigations. One of the disadvantages of this approach is that it is unclear which part of their privacy people would like to protect the most.



Facebook A

- Price: €9,99 per year
- Data requirements:
  -Name
  -Gender
  -Birthday
  -Place of birth
  -Address
  -Zipcode
  -City
  -Nationality
  -Email
- Terms and conditions: Personal information will not be provided to third-party partners or other companies

Facebook B

- Price: Free
- Data requirements:
  -Name
  -Gender
  -Birthday
  -Place of birth
  -Address
  -Zipcode
  -City
  -Nationality
  -Email
  -Education level
  -Yearly income
  -Marriage
  -Children
  -Age of children
  -Areas of interest
- Terms and conditions: Personal information might be used for marketing purposes

Picture 17

Furthermore, there are some omitted variables in this paper. This was noticed, when the survey was already online and distributed. For example, the income of the individuals was not included in the survey. Income could also have been an independent variable that could have affected the willingness to pay.

Finally, there are some other options to manipulate people that could have resulted in a changing view on the importance of privacy. Framing is not the only alternative, there are for example some more aggressive strategies (like indoctrination), but these methods are not very subtly. Focusing on the framing technique: what could have been done better? There could have been added nice and attractive photos of the win actions, so that people would be willing to give up more of their privacy. Pictures would certainly have captured the imagination more.

7. Conclusion and Discussion

It has never been investigated before if and how much one would be relatively willing to pay to protect privacy on Social Media. Based on a survey (according to the CV method) among 120 respondents in the Netherlands, the following can be concluded with respect to privacy in general as well as to privacy on Facebook. On average, people attach great importance to privacy. They prefer to hide their information, but in line with the privacy paradox, the majority has a Facebook account. More than half of the Facebook users assessed themselves as active users, which means that they use the Facebook possibilities with certain regularity. Sixty-nine percent of the people that do not join Facebook avoid the social media platform because of privacy concerns. These non-users attach significantly more importance to privacy than users of Facebook. Facebook's Data Policy was divided up into eight categories of information that the company collects: Things that you do and information you provide, Things that others do and information they provide, Your networks and connections, Information about payments, Device information, Information from websites/apps that use Facebook's services, Information from third-party partners and Information from Facebook-companies. What seemed to be the most important category that people wanted to protect was information about payments. Descriptive statistics showed that this was, on average, also the category that half of the respondents would be willing to pay the highest amount for. Apparently, people do not want that companies have insight in their payment overview and in their account details regarding payments, like their credit card number. This result was striking in comparison to other categories. The least important category was the protection of information from websites and apps that use Facebook's services. About 85% of the respondents felt uncomfortable about paying for privacy initially, but more than one-third of the people is willing to pay for privacy once (30%) or even yearly (6,7%). On top of that, almost one-fifth would be willing to give up more of their privacy when win actions are introduced. If Facebook would guarantee safety about personal details through collecting money via financial fees, Facebook could perhaps be accessible in the future for everyone that does not join the social platform now. There could be reached many more people then, also the people that are now passive users of Facebook that could become more active. This might be a win-

win situation for both Facebook (because of expanding its number of users) and passive- and non-users of Facebook. Furthermore, this approach could be beneficial for other social media.

Bibliography

Atkinson, G., & Mourato, S. (2008). Enviromental Cost-Benefit analysis. *Annual Review of Environment , 33*, 317-319.

Barnes, S. B. (2006, September 4). A privacy paradox: Social networking in the United States. *First Monday , 11* (9).

BBC. (2012, December 12). *Facebook changes privacy settings*. Opgeroepen op July 4, 2015, van BBC: http://www.bbc.com/news/technology-20693203

Beresford, A. R., Kübler, D., & Preibusch, S. (2012). Unwillingness to pay for privacy: A field experiment. *Economics Letters , 117* (1), 25-27.

Caudill, E. M., & Murphy, P. E. (2000). Consumer Online Privacy: Legal and Ethical Issues. *Journal of Public Policy & Marketing , 19* (1), 7-19.

Culnan, M. J. (2000). Protecting Privacy Online: Is Self-Regulation Working? *Journal of Public Policy & Marketing , 19* (1), 20-26.

de Bruijn, H. (2011). Framing - Over de macht van taal in de politiek. Atlas Contact.

Facebook. (2015). *Facebook Reports Fourth Quarter and Full Year 2014 Results.* Acquire Media.

Facebook Inc. (2015, January 30). *Data Policy.* Opgeroepen op May 16, 2015, van Facebook: https://www.facebook.com/privacy/explanation

internet.org. (2014). *State of Connectivity: 2014 - A Report on Global Internet Access.*

Jong, J. d. (2012). *Waarom maken politici graag gebruik van framing?* Opgehaald van Taalcanon: http://www.taalcanon.nl/vragen/waarom-maken-politici-graag-gebruik-van-framing/

Krishnamurthy, B., & Willis, C. (2009). On the Leakage of Personally Identifiable Information Via Online Social Networks. *Sigcomm 2009* (pp. 7-12). New York: ACM.

Maas, A. (2013). De redenloze consument. Rotterdam: Rotterdam University Press.

(2006). In L. S. Meyers, G. Gamst, & A. J. Guarino, *Applied mutivariate research: Design and interpretation.* Thousand Oaks, CA: Sage Publications.

NRC.nl. (2012, May 18). Facebook gaat vandaag naar de beurs. Wat gaat het alle partijen opleveren? *NRC* .

Oxford Dictionairies. (2015). *Privacy*. (Oxford University Press) Opgehaald van Oxford Dictionaries: http://www.oxforddictionaries.com/definition/english/privacy

Ozawa, N., & Barlow, J. (2013). *2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters.* Javelin.

Parker, R. B. (1974). A Definition of Privacy. *HeinOnline* , pp. 275-276.

Roosendaal, A., Nieuwenhuis, O., Ooms, M., Bouman-Eijs, A., & Huijboom, N. (2015). *Privacy beleving op het internet in Nederland.* Rijksoverheid. TNO.

The Nielsen Company. (2010, June 15). *Newswire*. Opgeroepen op May 20, 2015, van nielsen.com: http://www.nielsen.com/us/en/insights/news/2010/social-media-accounts-for-22-percent-of-time-online.html

Trend Micro. (2013). Uw privacy beschermen op sociale media.

Tversky, A., & Kahneman, D. (1986, October). Rational Choice and the Framing of Decisions. *Chicago Journals* .

van Hoek, C. (2013, May 2). *Vooral jongeren wijzigen privacyinstellingen Facebook*. Opgeroepen op June 2015, van www.nu.nl: http://www.nu.nl/internet/3411687/vooral-jongeren-wijzigen-privacyinstellingen-facebook.html

Westin, A. F. (1968). *Privacy and Freedom* (Vol. 25). Washington.

Appendix I

Questionnaire – Are you willing to pay for privacy on Facebook?

Dear respondent,
Thank you for participating in this research. The survey is completely anonymous. Please answer the questions as honest as possible.
Thank you very much!
Rebecca

1) Do you have an account on Facebook?

- ○ Yes, *[you can go to Question 2]*
- ○ No, *[you can go to Question 4 and in the following questions: please act like you are a Facebook-user]*

2) Why do you have a Facebook-profile?

- ○ Especially because I want to get in touch with friends/family
- ○ Especially because I want to read messages/see pictures from friends/family
- ○ Especially because it's necessary to use apps or websites, like playing games
- ○ Especially because I feel old-fashioned when others have Facebook and I don't: I'm just herding
- ○ Another reason, especially because…

An active user of Facebook places photos, videos and status-updates on his/her profile and/or looks on other profiles or in the news feed regularly. On the contrary, a passive user barely uses Facebook.

3) Would you describe yourself as rather an active or a passive user of Facebook?

- ○ I am rather an active user than a passive user
- ○ I am rather a passive user than an active user

4) Why don't you have a Facebook-profile?

- ○ Especially because of privacy concerns
- ○ Especially because I don't like Social Media (e.g. Twitter/Instagram) at all
- ○ Another reason, especially because…

The right to privacy is a right that every human has and offers a kind of personal freedom.

5) In general, on a scale of 1 to 10 (1 = totally not important, 5 = neutral, 10 = very important), how much do you care about your right to privacy?

Totally not important << 1 10 >>Very important □

Facebook collects an incredible amount of information/data about its users to offer, improve and develop their services, to communicate with you, to advertise and to improve the safety. Facebook is sharing this information via its services and with external partners and clients. In Question 6 till 13 there are mentioned 8 categories: it will be asked how important you think it is to protect information from Facebook as a company, as well as from third-party partners and clients of Facebook.

Totally not important << 1 10 >>Very important

Category 1: Things that you do& information you provide

Your own status-updates, pictures, videos, locations and dates of your updates, the type of content you look at, to which types of content you respond and the regularity/duration of your activities.

6) Could you please grade category 1 (1 = totally not important, 5 = neutral, 10 = really important) in willingness to protect the information from Facebook as a company and its external partners? □

Category 2: Things that others do& information they provide

Content and information that other people share, including information about you, for example when they share a picture of you or if they send you a message.

7) Could you please grade category 2 (1 = totally not important, 5 = neutral and 10 = really important) in willingness to protect the information from Facebook as a company and its external partners? □

Category 3: Your networks and connections

Information about people and groups you are connected to and the way that you treat this people and groups, like the people you communicate with most of the time. Also included in this category are the data when you upload your addresses from your telephone.

8) Could you please grade category 3 (1 = totally not important, 5 = neutral, 10 = really important) in willingness to protect the information from Facebook as a company and its external partners? □

Category 4: Information about payments

Information about purchases or financial transactions, for example when you buy something on Facebook, when you buy something in a game or when you donate an amount of money for charity. But also information about your payment details, like the number of your debit/credit card etc.

9) Could you please grade category 4 (1 = totally not important, 5 = neutral, 10 = really important) in willingness to protect the information from Facebook as a company and its external partners? □

Category 5: Device information
Information of and about the computers, mobile phones and other devices on which you open/install Facebook, for example your operating system, battery and signal strength of your device, geographical locations (via Bluetooth or Wi-fi), your mobile provider, the language of your telephone and your IP-address.

10) Could you please grade category 5 (1 = totally not important, 5 = neutral, 10 = really important) in willingness to protect the information from Facebook as a company and its external partners? □

Category 6: Information from websites/apps that use Facebook's services
Information about websites and apps of external parties, that use Facebook's service (e.g. they have the ''like'' button, they offer a possibility to register via Facebook or they use Facebook's service for measuring and advertising), for example information about websites that you visit and your use of Facebook's services on these websites and apps.

11) Could you please grade category 6 (1 = totally not important, 5 = neutral, 10 = really important) in willingness to protect the information from Facebook as a company and its external partners? □

Category 7: Information from third-party partners
Information about you and your activities from third-party partners, for example when one of Facebook's partners and Facebook provide services together, or when an advertiser gives data about your experience and interactions.

12) Could you please grade category 7 (1 = totally not important, 5 = neutral, 10 = really important) in willingness to protect the information from Facebook as a company and its external partners? □

Category 8: Information from Facebook-companies
Information about you from companies that are owned or controlled by Facebook (in accordance with the terms and policies), for example information about you from WhatsApp.

13) Could you please grade category 8 (1 = totally not important, 5 = neutral, 10 = really important) in willingness to protect the information from Facebook as a company and its external partners? □

14) In general, do you think that it is a strange idea to pay for privacy?

○ Yes, privacy is a human right
○ No, paying for privacy might be necessary in a world that becomes more digital
○ Different opinion, namely…

Suppose that Facebook has an option to guarantee that your privacy on all above information is protected from websites, apps, Facebook-companies and third-party partners. However, this option is only possible when you pay a financial fee.

15) How often would you be willing to pay the financial fee to maintain your privacy?

○ Never *[please suppose in Question 16 that you want to pay once anyway]*
○ Once
○ Yearly

Suppose that the amount of the one-off financial fee is built from protecting the 8 above categories, mentioned in Question 6-13. The more you are willing to pay for each category, the more you want this category to be protected. You can pay a minimum of 0,00 Euros and a maximum of 1,00 Euros per category. This means that you should spend a maximum of 8,00 Euros to protect your privacy on Facebook.

16) How much are you willing to pay (just once) for each category to protect your privacy on Facebook. Make sure you don't exceed 8.00 Euros in total.

○ Things that you do & information you provide	€…	
○ Things that others do & information they provide	€…	
○ Your networks and connections	€…	
○ Information about payments	€…	
○ Device information	€…	
○ Information from websites/apps that use Facebook's services	€…	
○ Information from third-party partners	€…	
○ Information from Facebook-companies	€…	+
Total fixed fee I am willing to pay to protect my privacy	€…	

Suppose that Facebook organizes and promotes win actions in certain age categories in the Netherlands. Two examples:

1. *You are a 20-year-old Dutch boy and Facebook knows that you love soccer, because of your pictures and messages of your soccer team. You are eligible to win 2 tickets to the next World Championship of Soccer, because you are between 18 and 25 years old and you live in the Netherlands.*
2. *You are a 42-year-old Dutch woman and Facebook knows that you love cooking, because of your self-made food pictures. You are eligible to win a professional tableware set, because you are between 30 and 45 years old and you live in the Netherlands.*

In this case, Facebook has the right to collect information, in exchange for creating the chance to win prizes in certain age categories.

17) Would you give up more of your privacy based on these Facebook-introduced win actions?

- ○ Yes, now I am willing to give up more of my privacy, because I like these win actions
- ○ No, these advantages don't make sense to me: I still care the same about my right to privacy
- ○ Different opinions, namely…

18) Would you be willing to pay a higher financial fee (compared to your total answer in Question 16) to protect your privacy, when you automatically have the chance to win these actions?

- ○ Yes, namely €…
- ○ No, I would pay the same

19) What is your gender?

- ○ Male
- ○ Female

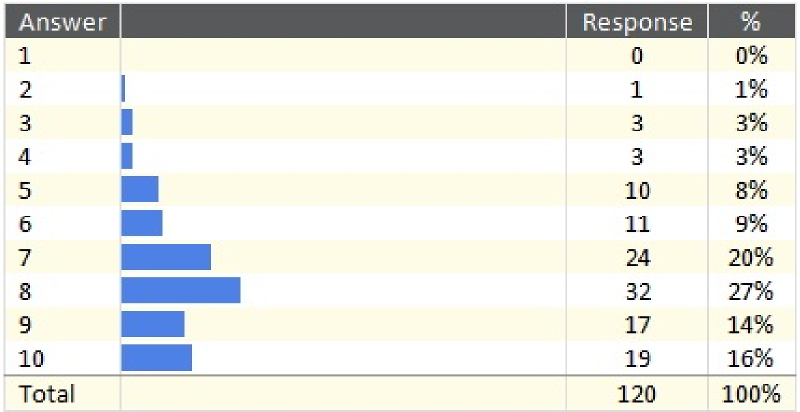
20) How old are you?

- ○ Younger than 30 years old
- ○ Between 30 and 50 years old
- ○ Older than 50 years old

21) What is the highest level of education you have achieved?

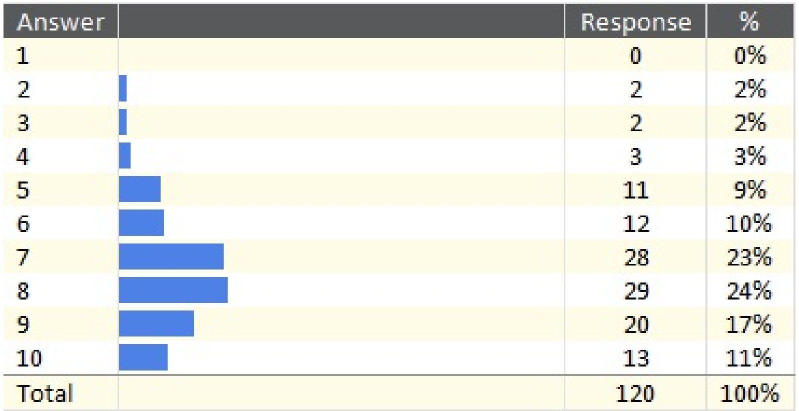
- ○ Basisonderwijs
- ○ Middelbaar Onderwijs
- ○ MBO
- ○ HBO
- ○ WO
- ○ Different, namely…

Appendix II



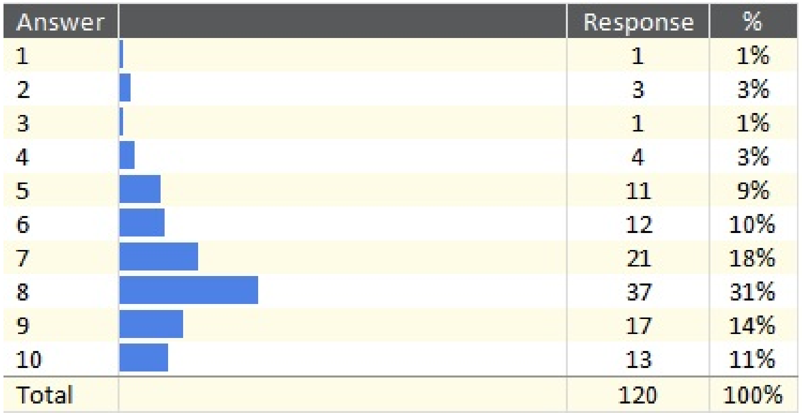
Answer		Response	%
1		0	0%
2		1	1%
3		3	3%
4		3	3%
5		10	8%
6		11	9%
7		24	20%
8		32	27%
9		17	14%
10		19	16%
Total		120	100%

Figure A – Grades on category ''Things that you do & information that you provide''



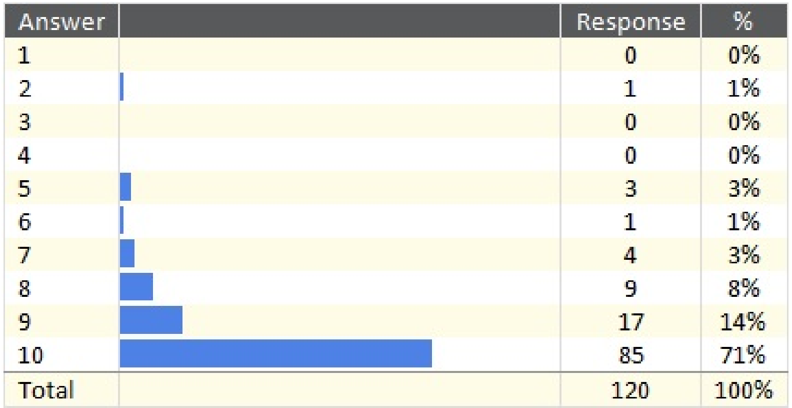
Answer		Response	%
1		0	0%
2		2	2%
3		2	2%
4		3	3%
5		11	9%
6		12	10%
7		28	23%
8		29	24%
9		20	17%
10		13	11%
Total		120	100%

Figure B – Grades on category ''Things that others do & information that they provide''



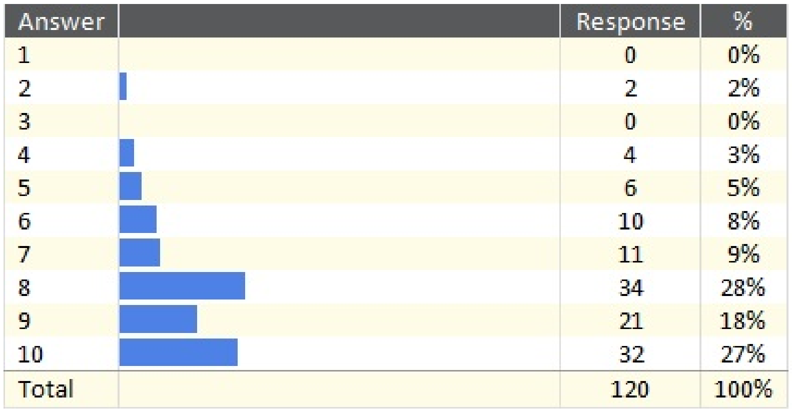
Answer		Response	%
1		1	1%
2		3	3%
3		1	1%
4		4	3%
5		11	9%
6		12	10%
7		21	18%
8		37	31%
9		17	14%
10		13	11%
Total		120	100%

Figure C – Grades on category ''Your networks and connections''



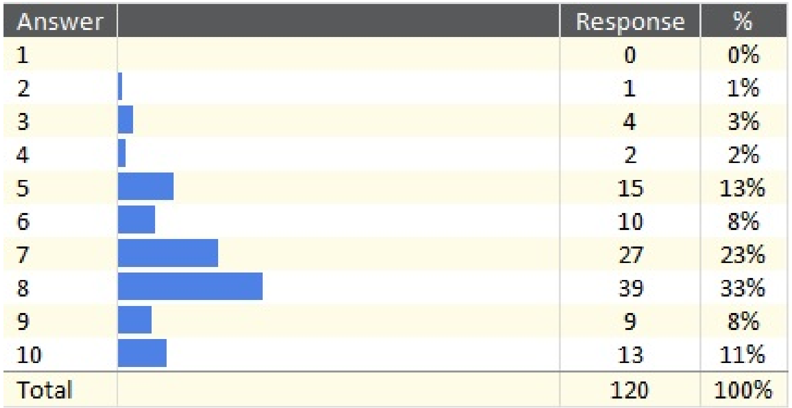
Answer		Response	%
1		0	0%
2		1	1%
3		0	0%
4		0	0%
5		3	3%
6		1	1%
7		4	3%
8		9	8%
9		17	14%
10		85	71%
Total		120	100%

Figure D - Grades on category ''Information about payments''



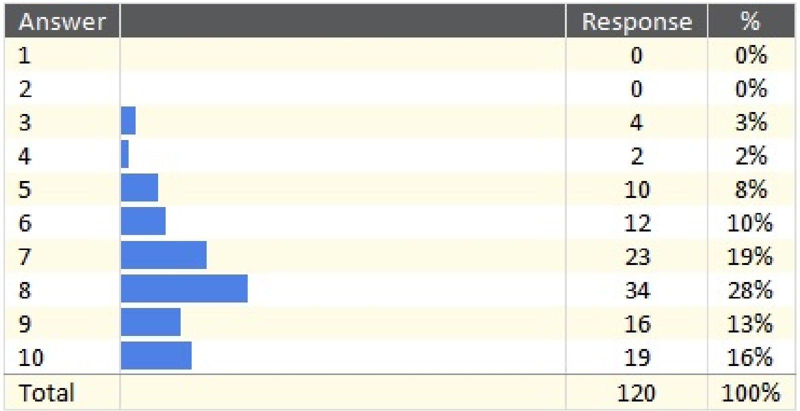
Answer		Response	%
1		0	0%
2		2	2%
3		0	0%
4		4	3%
5		6	5%
6		10	8%
7		11	9%
8		34	28%
9		21	18%
10		32	27%
Total		120	100%

Figure E - Grades on category ''Device information''



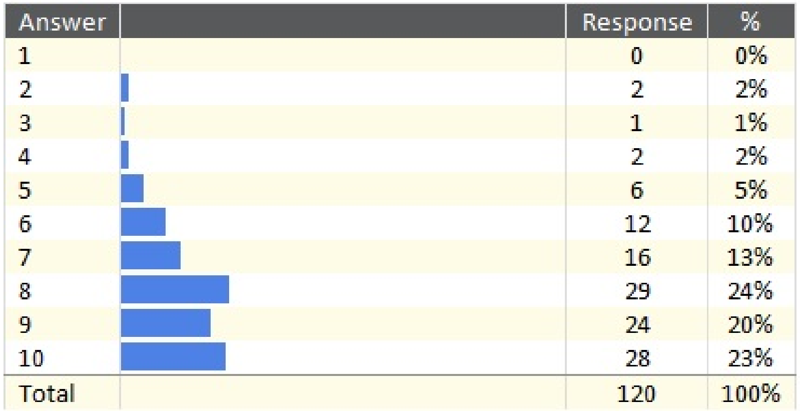
Answer		Response	%
1		0	0%
2		1	1%
3		4	3%
4		2	2%
5		15	13%
6		10	8%
7		27	23%
8		39	33%
9		9	8%
10		13	11%
Total		120	100%

Figure F - Grades on category ''Information from websites and apps that use Facebook's services''



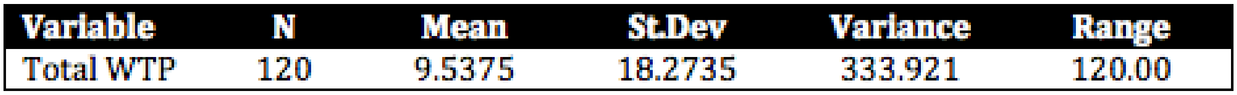
Answer		Response	%
1		0	0%
2		0	0%
3		4	3%
4		2	2%
5		10	8%
6		12	10%
7		23	19%
8		34	28%
9		16	13%
10		19	16%
Total		120	100%

Figure G - Grades on category ''Information from third-party partners''



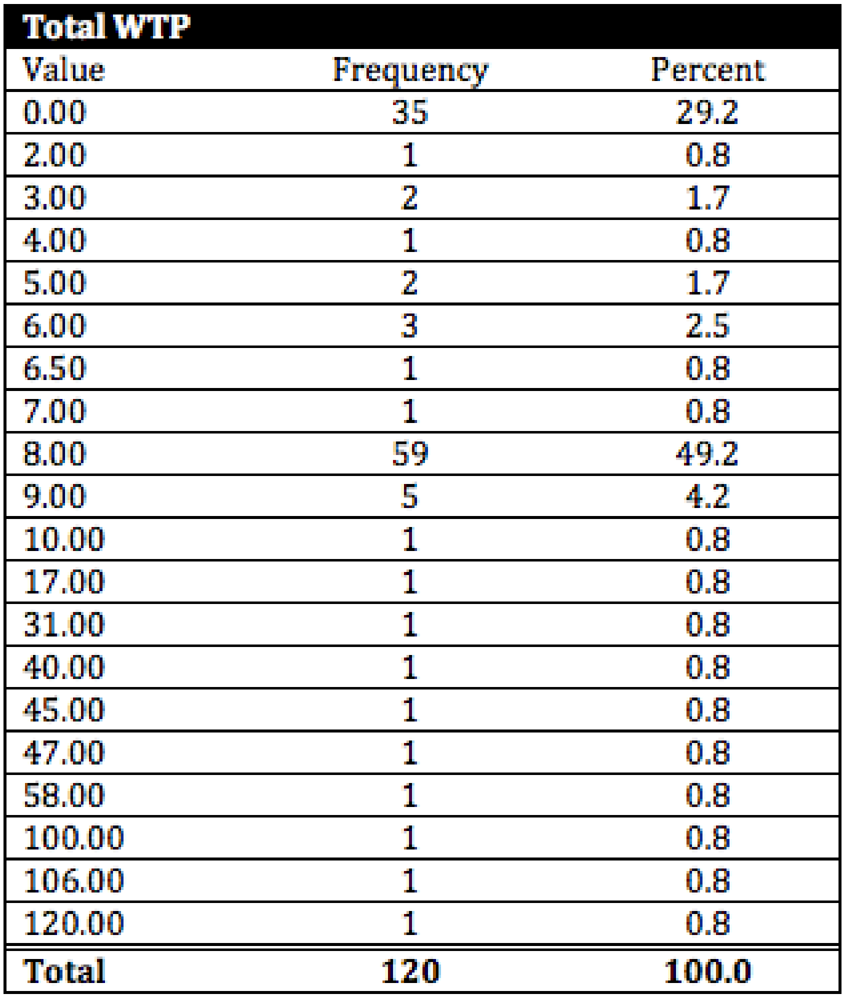
Answer		Response	%
1		0	0%
2		2	2%
3		1	1%
4		2	2%
5		6	5%
6		12	10%
7		16	13%
8		29	24%
9		24	20%
10		28	23%
Total		120	100%

Figure H - Grades on category ''Information from Facebook companies''



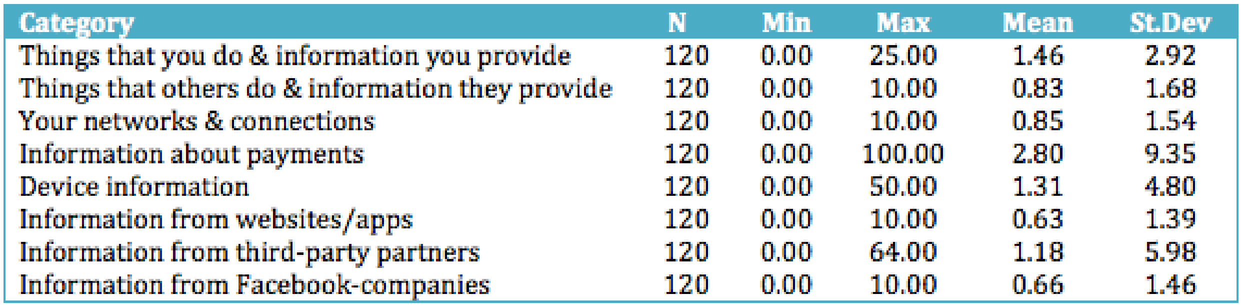
Variable	N	Mean	St.Dev	Variance	Range
Total WTP	120	9.5375	18.2735	333.921	120.00

Figure I – Descriptive statistics on Total willingness to pay (Total WTP)



Total WTP		
Value	Frequency	Percent
0.00	35	29.2
2.00	1	0.8
3.00	2	1.7
4.00	1	0.8
5.00	2	1.7
6.00	3	2.5
6.50	1	0.8
7.00	1	0.8
8.00	59	49.2
9.00	5	4.2
10.00	1	0.8
17.00	1	0.8
31.00	1	0.8
40.00	1	0.8
45.00	1	0.8
47.00	1	0.8
58.00	1	0.8
100.00	1	0.8
106.00	1	0.8
120.00	1	0.8
Total	**120**	**100.0**

Figure J – Frequencies on Total willingness to pay (Total WTP)



Category	N	Min	Max	Mean	St.Dev
Things that you do & information you provide	120	0.00	25.00	1.46	2.92
Things that others do & information they provide	120	0.00	10.00	0.83	1.68
Your networks & connections	120	0.00	10.00	0.85	1.54
Information about payments	120	0.00	100.00	2.80	9.35
Device information	120	0.00	50.00	1.31	4.80
Information from websites/apps	120	0.00	10.00	0.63	1.39
Information from third-party partners	120	0.00	64.00	1.18	5.98
Information from Facebook-companies	120	0.00	10.00	0.66	1.46

Figure K – Descriptive statistics on willingness to pay per category