1 INTRODUCTION
With the recent growth and popularity of Social Networking Sites (SNSs), there has been a great volume of all kinds of data generated by the users, such as: texts, photos, videos, collections of points of interest, etc (Yang, Zhang, Yu, Yu & Zeghlache, 2014). Being on a SNS has become one of the most popular activities of users of the web. Facebook, Twitter, LinkedIn and Instagram can be found in the top 30 of most visited sites according to Alexa (2015). The popularity of the SNSs is rising especially among the younger generation. Acquisti and Gross have found out that 80% of the American university students are active SNS users (2006). Research of Dwyer has even shown that the ubiquity of social networking in the youth culture has been compared with an addiction (2007). With the advent of mobile/smartphones the SNSs are everywhere and the user is able to access them at any moment. Being able to access the SNSs at any moment or place and exposing personal information such as textual updates, photos, videos and locations has raised privacy concerns.

Waters and Ackerman state in their article that interpersonal disclosure used to be something that was intimate and private. June the 1\textsuperscript{st} in 2010 was designated as a protest day against the SNS Facebook that would involve all its 500 million users at that time (Facebook Statistics, 2010). The protest was designated because of the new privacy policies that Facebook adopted. Most users did not take part in the protest against the new privacy policy and continued using Facebook. The reason that Facebook changed their policy after several critiques spoke about the privacy problem that Facebook was sharing personal information with advertisers without the agreement of the users. The change of the privacy policy made the users privacy less secure (2011).

The accessibility, the popularity and the huge amount of users of SNSs do bring some problems with them. The Social network companies want to make it as attractive as possible for people to disclose information about themselves. This has lots of benefits for the Social network companies, because knowing more information about a user means more precious data that can be sold to third parties such as advertisers on the SNSs. The is the main source of income for the SNSs. (Tucker, 2014) In terms of transparency SNSs do not have the best reputation when it comes to how the data that the SNSs collect will be used.

There are several problems at different levels that concern the privacy of the users on SNSs. If users would not disclose any information with regard to sharing information, liking things or commenting on SNSs there would not be less concern about their privacy. Since this is not the case Folkert Heeneman researched the factors that influence the users self-disclosure on SNSs with a focus on Facebook. Heeneman found out that the following factors are most problematic for Facebook users:

- A mismatch of expectations.
- Lack of flexibility.
- Lack of transparency.
- Abuse of permissions.

According to the research of Altman (1975), it is people’s natural habit to disclose information because this will strengthen and form social bonds. If too much information is restricted, this will have an effect on the bonds, which will then maybe not be created within a community. Privacy policies should have the role of communicating the privacy implications of using a SNS to the user.

2 RELATED WORK
As mentioned in the introduction, the activity in a networked community such as SNSs can be stimulated by the exposure of user-generated content (Erickson & Kellogg, 2000). In SNSs such as Facebook, Google +, Twitter and Instagram users post status updates, share pictures, share links and like things, this kind of activity drives the page views. According to Acquisti and Gross the attitude that users have towards privacy might affect the amount and type of content that is being shared on a SNS (2006). This has an impact on the activity of an SNS, which could also have a negative impact on the income of the SNS because the data about the users is less rich for selling to third party advertisers.

The unintentional exposure of personal data might lead to the current location of the user, for example that the user is not at home but on vacation. Burglars can abuse this information. Physical stalking and identity fraud based on personal information can also be results of abusing personal information from SNSs (Gross & Acquisti, 2005). Cyber bullying, online harassment (Valkenburg & Peter, 2009) are also result of abusing personal information that can be the result of extracting information from SNSs.

In this research there will be researched if there is a difference between the privacy policy of the social network and the perceived privacy of the user. This will be done by looking at the current privacy policy implementation in
SNSs, looking at the things that influence the users decisions about their privacy and finally if the previous points are true, there will be research done to possible solutions for closing the gap between the privacy policy implementation and the users perception of them.

2.1 Policy Implementation

2.1.1 Definition
Privacy policies by SNSs can be long and confusing, according to Bonneau and Preibusch (2009) and McDonald and Cranor (2009) the privacy policies are often criticized as being difficult and time consuming to read.

2.1.2 Presentation
As already mentioned how a privacy policy is defined. The privacy policies are often too long in presentation, which makes it not attractive for the user to read the policy.

According to Strater and Lipford designers need to find a way to educate users in protecting themselves while still being able to use the social network in its full functionality (2008).

2.1.3 Integration in the usage
Problems with relation to the interface occur, the difficulty and the lack of privacy settings are the result of that. Strater and Lipford are relating to Facebook, in many practices the users expectations did not match with what happened according to their privacy setting. This can result in accidental disclosures, which are more difficult for the user to hunt down (2008).

Another problem for the users lies in expending their profile with other applications or websites where they need to log in with a social network ID. Within the new applications and websites the user discloses new information. According to Strater and Lipford the users rarely revisit their privacy setting to look if their setting are still appropriate according to their growing profile (2008). This is an important finding that can be spread out to most SNSs, because the SNS does rarely or not remind the user to reflect about their disclosures after creating a profile.

2.2 User Related Issues
Liu, Gummadi, Krishnamurthy and Mislove found out in their research that the privacy management settings of Facebook, in only 37% of the time matched the actual users expectation (2011).

Krishnamurthy and Wills (2008) state in their article that the users of their research provide personal information on SNSs without having a clear idea of who has access to it or how it might be used. They also found out that between 55 and 90% of users on SNSs allow their profile information to be viewable and 80 to 97% of the users allow their set of friends to be viewed. This means that the users expose lots of personal information about themselves. Again it should be the privacy policy that tells the users who can have access to their account and how their data is being used.

From a study of Waters and Ackermann (2011) can be concluded that 51% do not trust a SNSs at times. This is remarkable because in a research from Jones and Soltren (2005) is being stated that only 10% of the users in their surveys claim to have read the privacy policy of their SNS. Examinations of server logs show that the actual rate may be far less than 1% (Wham, 2001).

According to the research results of Waters and Ackerman (2011) there are four motivations for active users of Facebook to disclose information. These might be extendable to other Social Networks. The first one is pure sharing information with others, and in some cases sharing private information can be seen as a fun and enjoyable activity. Another motivation is to store information that is meaningful for them. The third one is that users were getting motivated to disclose information to keep up with trends. The fourth one is to show off.

The problem is not that SNSs/applications have the access to private data; the real problem is that users expect that the SNSs/applications will only access the private data to do its job. This problem is all about the awareness of the users of a SNSs. SNSs and their applications can hoard the personal information to transfer it to third parties, this can be a violation of the user expectations (Viswanath, Kiciman, Saroiu, 2012).

Different cultural users of SNSs can have different perceptions of privacy and awareness. An example is the research from Krasnova and Veltri (2010), they found out from a survey of Facebook members that “German users expect more damage and attribute higher probability to privacy-related violations. On the other hand, American users show a higher level of privacy concern, they extract more benefits from their social networking activities, have more trust in the service provider and legal assurances as well as perceive more control” (p. 1). It is interesting to ask if the behavior and perception with regard to privacy is culture/socially dependent.

The user can be active on different kinds of SNSs, all these SNSs can have different kinds of default settings and may not reflect the users privacy needs and desires. An example is if a user posts a picture on Facebook that can only be seen by his or her friends and wants to share the photo on Twitter, it can be possible that the default settings are still on public. This means that a photo that was supposed to only be seen by friends can be made public without knowing it.

2.3 Existing Privacy Solutions
There are several solutions proposed by several researchers, a couple of them will be described. There are several researchers that are researching the opportunities to implement technologies and privacy policies for the SNS administrators. They have been focusing on addressing the privacy concerns but still enabling the free flow of content. With regard to the design researchers, they have been busy to create systems that support/guide the user in sharing con-
tent while reducing the risk of violating their own privacy (Hawkey & Inkpen, 2006; Nov & Wattal, 2009).

Cranor, Reagle, and Ackerman (2000) found out in their research that transparency by posting a privacy policy and giving users more control of their personal information had a positive factor in online disclosure.

Krishnamurthy and Wills (2008) state in their research that SNSs should only indicate the bare minimum of personal information that is required for a particular set of interactions.

In the article of Felt and Evans (2008) they talk about the privacy by proxy approach. Through this approach a SNS can have the control over the output and can control/support external applications without compromising personal data about the user.

3 PROBLEM STATEMENT
The problem to be addressed is the possible gap between the privacy policy of the SNS and the perceived privacy of the user. As mentioned in the Relevant Work section the privacy policy should have an important role in communicating the privacy regulations of the certain SNS to the user, research has shown the opposite.

Liu et al. (2011) found out in their research that the privacy management settings of Facebook, in only 37% of the time matched the actual users expectation. Krishnamurthy and Wills (2008) found out that the users of their research provide personal information on SNSs without having a clear idea of who has access to it or how it might be used. Jones and Soltren (2005) state that only 10% of the users in their surveys claim to have read the privacy policy of their SNS. Examinations of server logs show that the actual rate may be far less than 1% (Wham, 2001).

Research results from the Relevant Work section show that the users expose lots of personal information. This might be the result of the low percentage of users that reads the SNSs privacy policy. Without reading the policy the users do not know which kind of impact their actions on a SNS have on their own privacy. A SNS can publish something as a privacy policy, but users can understand them in a different way. There might be a gap between what the intention/the understanding of the company is and the actual understanding or the so-called perceived understanding of the users.

The goal of this thesis is to study the current state of the art privacy policies, explore the factors that influence people’s perception of privacy and finally identify the aspects that align the two.

4 RESEARCH QUESTION(s)
Based on the goal of this thesis the following research question will be researched:

Is there a difference between the privacy policy of the social network and the perceived privacy by the user?

The following sub research questions will be used to answer the main question. Within these questions there will be focused on four SNSs: Facebook, Google +, Twitter and Instagram.

- How is the privacy policy implemented in the social network and how does this connect to the context of use?

There will be focused on the definition, presentation and integration of the privacy policy in the SNS. As a result there will be a table with a measurement scale that tells how well the elements are implemented in the SNSs.

- What are the things that influence the users decisions about their privacy?

There will be focused on the categories of services and the categories of content of the SNSs, the categories of users will also be researched. The awareness of their privacy will also an important role for the research. The result will be focused on the research results of the categories and if they influence the users behaviour on a SNS.

- What are solutions for closing the gap between the privacy policy implementation and the users perception about them?

If the first two questions indicate a gap there will be focused on finding possible solutions and describing a written advice as a solution to bridge the gap.

5 METHODS
The process of finding the answer to the main research question will be split in multiple stages. These stages are the three sub questions that are described in the previous section. They will help answering the main question. In this section there will be focused on shortly describing the approach of researching those sub questions. An important thing to mention is that in this research there will be focused on four SNSs: Facebook, Google +, Twitter and Instagram.

5.1 Qualitative Analysis Privacy Policies
To answer the main research question the following sub questions will be researched.

The first sub question:

- How is the privacy policy implemented in the social network and how does this connect to the context of use?

This sub question is about the policy implementation. To research the first sub question about the privacy policy implementation the following points will be researched:

1. How is it defined?

The presentation of the privacy policy will be researched based on: clarity, simplicity and the comprehensibility of the language.

2. How it is presented?
The transparency of the privacy policy will be researched in the whole workflow for the individual users.

3. How it is integrated in the usage?

The context of the privacy policy will be researched. Where it is applied and for which of the services it appears. With services are activities meant such as: posting, commenting, sharing and liking.

These points will be researched on the four SNSs. To research them a qualitative analysis will be done of the four SNSs. As a result there will be a table made in which the different kinds of SNSs are implemented with the elements that need to be researched, how the policies are defined, presented and integrated in the usage. There will be some kind of metric made which tells how well the elements are implemented in the different SNSs. All this will be visualized in a table with different kind of columns that have to be identified in terms of definition, presentation and integration.

5.2 Questionnaire With Users

The second sub question:

- What are the things that influence the users decisions about their privacy?

The second sub question is about the user. There will be researched: What influences the users perception of privacy? How much awareness about privacy do the users have? And how it all differs in different context of use, for example: categories of services and categories of content and to what extent are all these culture/socially dependent

These are the things that have to be studied and after that categories will be created. Possible categories that can be researched are described below.

Categories of services: categories of transparency, platforms, and realisations will be researched. This is whether a user shares, posts, likes etc. There are existing vocabularies that describe social web activities, such as like, post, comment, read and so on.

Categories of content: different kind of categories of content, services and users, which describe the users perception of privacy and how it can be influenced, will be researched.

Categories of users: different kind of categories of users, dependent of different cultures will be researched.

User studies will be used to gather data. This will be done through an online survey/questionnaire, because this will give the possibility to reach more people in a short period of time and it gives the possibility to research people from different nationalities. Face-to-face questionnaires can be used to add more participants next to the participants of the online questionnaire. Open interviews will be used to research the more underlying motives of the users of the SNSs.

5.2.1 Sample and target group

According to Borg and Gall the rule of thumb is about 100 observations for each of the major sub groupings in a survey. The target group for doing this research are users of SNSs. If multiple nationalities will be researched the number of nationalities will be limited, for example four times 25 participants for four nationalities.

5.2.2 The Questionnaire

In order to be able to compare the data from the different participants from the questionnaire, a likert scale will be used to answer the questions in the questionnaire. The format will be based on the typical five-level likert item: 1. Strongly disagree, 2. Disagree, 3. Neither agree nor disagree, 4. Agree and 5. Strongly agree.

Once the data is collected it will be possible to observe and analyse the data.

5.2.3 Data analysis of the API’s

The API’s of the four social networks will be used to observe the existing data of the users of SNSs.

5.2.4 Data analysis questionnaire

Using a quantitative research method it is possible to do statistic tests. By using the statistic test it is possible to given an answer to the second sub question. The descriptive statistics have to be reported first. Mean and Median, along with the Mode and the standard deviation and range for dispersion statistics can be made up.

Secondly, the Likert scale is used and these data are ordinal in scale, this means that non-parametric tests can be done. For two categories (as in male and females) the Mann-Whitney can be used, and for three or more (as in age groups) the Kruskal-Wallis test can be used. After the analyses of the data it could be possible to give an answer to the second sub question.

5.3 Solution For Closing The Gap

If the answer of the first two sub questions can be answered with yes, then sub question three will be researched and answered.

- What are solutions for closing the gap between the privacy policy implementation and the users perception about them?

As already mentioned if the answers of the first two questions indicate that there is a gap between the implementation and how the user deals with it or perceives it. Then there should be possible solutions described for bridging in these gaps.

There will be looked at what kind of solutions are there at the moment and to research if there is a missing piece.

For answering sub question three a design and implementation will be described of a possible solution. This will be a written advice that can be used by the SNSs and by the users itself to create more awareness.
5.4 Evaluation Of Solution
If the solution only needs to solve one problem, the solution can be easier evaluated. If there are more problems it might not be easy to evaluate. If there are more problems that the solution needs to solve, there will be chosen to evaluate only one problem instead of all.

The solution will be evaluated with a small group of two till five SNS users. As an evaluation method open interviews will be used to find out what the users of the SNSs think of the possible solution to bridge the gap between the privacy policy and the perceived privacy by the user. The results of the interviews will give an indication if the gap has been bridged.

6 SCHEDULE
• April 1 – 12: Literature review RQ 1, 2 and 3 and construct hypotheses for RQ 2.
• April 13 – 19: RQ1, Analyze privacy policies and make table with measurement scale.
• April 20 – 26: Q1, Fill table with results.
• April 27 – May 3: RQ2, Make the questions for the online questionnaire.
• May 4 – 24 May: RQ2, Gathering data questionnaire and gathering data API’s.
• 25 May – 7 June: RQ2, Analyzing data questionnaire and analyzing data API’s.
• June 8 – 21: RQ3, Prepare and make advice for solution.
• June 22 – July 12: Evaluation of solution with users.
7 REFERENCES


