NTNU – Trondheim
Norwegian University of
Science and Technology

Interdependent Privacy on Facebook

Esther Bloemendaal
Ida Malene Hassel Øveråsen

Submission date: November 2013
Responsible professor: Jan Audestad, ITEM
Supervisor: Gergely Biczók, ITEM

Norwegian University of Science and Technology
Department of Telematics

Abstract

With the evolvement of the online social networks, the incentive to share personal information has grown drastically. Our focus is directed toward the largest online social network, Facebook. With the enormous data sharing, privacy concerns arise. The privacy of an individual user is bound to be affected by the decisions of others, and are therefore to some degree out of the users control. This phenomenon lays the basis for the term *interdependent privacy*.

Interdependent privacy is one specific part of the privacy issues that exists on Facebook. In order to get a full overview and understanding on this matter, we have looked into different aspects. We have mapped the development of the default privacy settings and human awareness in regard to Facebook privacy, looked at the most important features introduced by Facebook over the years, and how these features have affected the users' privacy.

To map human awareness, we conducted a survey. In order to get a good image of people's awareness we distributed the survey on Amazon Mechanical Turk (AMT). This is a marketplace for work that requires human intelligence. One of the key benefits of using AMT is that it provides one of the largest subject pool, with both diversity and low cost. The survey was available on AMT for 3 weeks, and got a total of 250 responses. We analyzed these results with focus on awareness of privacy settings (including app settings). We wanted to see if there was a connection between privacy settings, and app settings and awareness of the permissions requested when installing apps.

Results: What's the answer? Give specific results.

Conclusion: What are the implications of your answer? summary of the discussion of the results and conclusion

Preface

This study was performed as a specialization project on behalf of the Department of Telematics at the Norwegian University of Science and Technology. The specialization project is part of two main profiles, information security and tele-economics, and this report is the final result of the project and is worth 15 ECTS points. The study was conducted between September and December 2013. The project description was outlined in cooperation with our project supervisor PhD Gergely Biczók at the Department of Telematics.

We would like to thank Gergely Biczók who has guided us through our project, and contributed with helpful ideas, feedback and support. We would also like to thank everyone who answered our answer, and helped us with valuable research information. A special thanks to our friends Aurora Klæboe Berg, Kine Aasjord Omholt and Thomas Normann for sharing the survey on their Facebook page, and making the survey reach out to a wider audience.

Trondheim, December 16, 2013

Esther Bloemendaal

Ida Malene Hassel Øveråsen

Contents

List of Figures

List of Tables

Chapter 1
Introduction

1.1 Motivation

1.2 Problem Description

Interdependency is a reciprocal relation between two or more decision-making entities, whose actions have consequences for each other. Interdependency is a very important issue when it comes to social networks, since your privacy is affected by the privacy decision of others. This project will be directed towards the interdependent privacy issues on Facebook.

Since Facebook came out in 2006, there has been a major change in privacy and security settings. At the same time Facebook's features have been significantly upgraded (e.g., Apps), and the platform itself has expanded to several different platforms (e.g., iOS and Android). Owing to this development, the complexity of privacy-related issues has made the originally embedded privacy requirements inadequate. We are going to map and analyze this development to see how privacy settings has changed over time. We will also look at human behaviour with regard to Facebook privacy. How this affects people when it comes to, for example, personal life and future job prospects, and to what degree people are aware of the unanticipated consequences the use of Facebook can bring.

In order to carry out the behavioural research we will use Amazon Mechanical Turk, enabling us to reach a wide audience. Amazon Mechanical Turk is a marketplace for work that requires human intelligence, and works well for conducting surveys. The key benefits of Amazon Mechanical Turk when you are conducting behavioural research is that it provides one of the largest subject pools, with both diversity and low cost. By using the results of the survey we will look into what kind of privacy settings different types of people value and map their awareness when it comes to the importance of different privacy settings.

1.3 Methodology

Our assignment is divided into parts, where one consists of collecting data from Facebook users regarding their view on Facebook privacy settings, and the other is a theoretical research of how Facebook privacy settings has evolved since the introduction of Facebook. This means that we have used different approaches to be able to retrieve the information desired.

Approach In this section we will describe our approach of collecting data from Facebook users regarding their view on Facebook privacy settings. Facebook is a global social network, so to be able to get more accurate information it is important to reach out to a wide and diverse audience. We decided to use Amazon Mechanical Turk for this purpose. To gather the data, we made a survey for the users to answer. Survey is a common used research method that involves the use of standardized questionnaires or interviews to collect data about people and their preferences, thoughts and behaviours in a systematic manner [6]. Survey, as a research method, has several advantages in comparison to other methods of doing research. Survey is a good method of retrieving unobservable data, like for example peoples attitudes, behaviours, characteristics, preferences, and demographics. Surveys are great when you want to cover a large group of people, like a country, that otherwise would be difficult to observe. With large groups and large amounts of data, surveys allows small effects to be detected, and makes it easy to compare the subgroups that may appear. Survey are in an economically sense cost effective. It is a lot cheaper for a researcher to make and send out a survey than to use other methods like experimental research. Survey as a research method also has some disadvantages. The method is often exposed to biases, like sampling bias, non-response bias, and social desirability bias. Surveys have a reputation for low responses, hence the non-response bias. This was one of the reasons for choosing AMT as a platform for publishing your survey.

We started by implementing the survey in Amazon Mechanical Turk (AMT), but learned that the templates provided by AMT was missing some of the features we wished to include, like dividing the questions into several pages. So mainly for design purposes we chose to create our survey in SurveyMonkey. This is easily integrated with AMT and a often used option. Using SurveyMonkey also made it a lot easier to keep track of answers and see summaries. SurveyMonkey has a great and easily understandable user interface, and made it easy to share the survey to other mediums like Facebook, to reach out to an even larger and more diverse audience.

In AMT we set the requirements that the users had to be "Master Workers". This is users that through a good reputation has earned the title, and by setting this requirement we rule out unserious users and answers. This will save us a lot of time in the screening process. When a user chooses to take our survey, they first get some information about the purpose and incentive of the survey, and a link to SurveyMonkey to take the survey. When the survey is finished the user receives a code that they have to provide before submitting their HIT in

AMT. This is an assurance for us that all users on AMT has finished the survey before they get paid. Throughout the lifetime of our survey we have changed this code, just to make sure that nobody tries to get paid without actually doing the work. When the survey is completed in a serious manner the workers get paid $1,5. On average, the users spent 13 minutes and 37 seconds to take the survey, this gives an effective hourly rate of $6,61.

Limitations Trenger vi det?

Chapter 2
Related Work

2.1 Social Network Services

A social network service (SNS), is a platform used to establish social networks of different people. These people often share a common interest or activity [7]. Online social networks (OSNs) is a large part of the social network services. From online social networks was first introduced until today, the popularity and complexity has grown drastically, with a hundreds of millions active users [8]. OSNs have a peer-to-peer architecture, and therefore makes it easy for members to initiate communication with whom they want, given that they are also connected to the network. OSNs also enables the possibility for people to easily publish and retrieve information about subjects of interest [9]. The internet has caused the creation of several information sharing systems [10]. Among these systems are the Web and OSNs. As mentioned before, the popularity of OSNs has grown drastically, and have become among the most popular sites on the Web. With this change, there has also been a change in what is centralized and in focus. The Web is to a large extent organized around content, while OSNs on the other hand are organized around users. This change has lead to the importance of understanding user behaviour. You can say that the expansion of OSNs has lead to a shift in how context is exchanged over the Web. End users are no longer just content consumers, but now also required to be content creators and managers [11].

A user is often represented with a profile on OSNs. To obtain a profile the user, in most cases, must register the site. When a user is given a profile, it is normal for the users to provide information about themselves. This information could for example be date of birth, home town, sex, name (or pseudonym) and maybe a profile picture. The social network is formed when users start connecting with each other. The reason for these connections are numerous; real-life friends, real-life acquaintances, colleagues, share an interest/activity or if you are interested in the information contributed by the other user.

Since Facebook was introduced to the public in 2006, it has grown to be the largest online social network (OSN) in the world. The growth of Facebook has made it necessary to

introduce new ways to manage privacy and ensure a secure online environment. The privacy embedded in the program/app etc. is not enough to ensure such an environment, due to the interdependent privacy issues. Your privacy is to a large extent affected by the privacy decision of others.

2.2 The History of Facebook

When Mark Zuckerberg (Chairman and CEO of Facebook, Inc.) enrolled at Harvard in 2002, he had decided to major in psychology. "I just think people are the most interesting thing—other people," he said. "What it comes down to, for me, is that people want to do what will make them happy, but in order to understand that, they really have to understand their world and what is going on around them" [12]. He showed an interest and passion for connecting people together and create Harvard more open.

Figure 2.1: The Facebook icon as we know it today.

It all started in October 2003 when the Harvard sophomore Mark Zuckerberg and three of his classmates created the web page Facemash. Zuckerberg hacked into the administrative database to extract the ID photos of all the students of the different houses. The web page presented two and two photos creating a "hot or not" game for his fellow students. The votes were counted and created a top-ten list of the cutest people in each house. Within the first hour Facemash had 450 visitors and 22 000 votes. After numerous complaints from professors and fellow students, Harvard administration shut down Zuckerberg's Internet connection after a few days. Harvard charged Zuckerberg for violating individual privacy, violating privacy and breach of security for stealing the photos. Zuckerberg agreed to take the web page down and got away with just a warning.

After Facemash, Zuckerburg was known around campus as a programming prodigy. Harvard seniors, Tyler and Cameron Winklevoss and Divya Narendra had since 2002 been working on a social networking page, called HarvardConnection. This was a page where students could create a profile, and through that share some personal information and post pictures and share this with large and small communities that one could be part of. They wanted Zuckerberg's help to finalize their project so that the page could be up and running before they graduated. Zuckerberg agreed to help at the same time as pursuing his own projects. Harvard offers a class directory to all freshmen, this directory is also known as the

"Facebook". This "Facebook" contains a picture of all the students and name, date of birth, home town and high school. The purpose of the "Facebook" was that the freshmen could get to know each other. Harvard's plan was to eventually get this online. Since Harvard had not gotten to it yet, Zuckerburg decided to do the job himself. He wanted to create a page where people signed up and created their own profiles, and in that way could post some personal information about themselves, and have control over what was posted. After ten days of intensive work, Zuckerberg almost finished the site. The site was kept simple and intuitive, and everybody with a Harvard e-mail address could create a profile. The profile consisted of a profile picture, name and some personal information such as taste in books, music, films and favourite quotes. Users could link to their friend's profiles and by using a "poke" button let others know that you have visited their profile. Thefacebook went public February 4, 2004, and to get the word spread they sent it out on the Kirkland house mailing list, that contained over 300 students. It did not take long until the other houses heard and within twenty-four hours, close to fifteen hundred people ha registered. "I think it's kind of silly that it would take the university a couple of years to get around to it," he said. "I can do it better than they can, and I can do it in a week." [12]. Later the same year the three founders of HarvardConnection, now called ConnectU, filed a lawsuit against Zuckerburg. Stating that he broke their oral contract, stole their idea, and delayed working on their site to be able to finish his own site, Thefacebook, first. Zuckerburg denied doing anything wrong, and stated that he had proof that he did not steal the idea from the HarvardConnection. Just a few months later Facebook filed a countersuit. Facebook accused ConnectU with defamation. The case went on for years. In 2011 the Winklevoss brothers dropped the lawsuit and accepted a 65 million settlement [13].

There was already similar pages out there, like Friendster and myspace.com. Especially on myspace.com people played roles, giving themselves out to be someone else. Teenage girls pretending to be older and grown men giving themselves out to be young girls. There is nowhere to validate that the person really is who they give themselves out to be. This limits to what extent people posts personal information. With Thefacebook.com you had to sign up with a valid Harvard e-mail address, in that way you know that they are actual people, and mostly students. This made it easier to post more personal information like cell-phone number, home address and even sexual orientation. The concern was not about security, but more about wasting time, it became an addictive pleasure.

It didn't take long before Mark Zuckerberg began to receive e-mails from other colleges, requesting to get Thefacebook at their schools. The site was easily scalable, the concern rather laid in how to maintain the intimacy and the clubby appeal. When Thefacebook expanded to the colleges Colombia, Yale and Stanford, students were only able to search and see people from their respective college. Only with permission from a student from another college could you add the person to your friend list. This is a key factor to Facebook's

success. Zuckerberg wanted people to post personal information and create a more open school community.

In June 2004, when the school year was over, Thefacebook had expanded to over forty schools, with 150 000 users. With the rapid expansion, the need for investors and more capacity increased. Zuckerburg moved his base to California and removed the "the" from the name. Thefacebook became just Facebook.

October 2005 Facebook expanded to universities in England, Mexico and Puerto Rico, and in September 2005 a high school version was available [14]. This was a big step for Facebook. All high school members needed an invitation to be able to join. Zuckerburg launched the possibility for all users to see the profiles and send friend request to everyone in the network, the older users had strong objections. College students did not like the idea of high school kids looking at their profiles and being able to befriend them. But with the rapid expansion Facebook was forced to make the site more open and knock down some of the walls dividing the users. Facebook made it possible for employees at different companies like Apple and Microsoft to join the network. At the end of 2005 Facebook was used at over 2000 colleges and at over 25 000 high schools in United states, Canada, Mexico, England, Australia, New Zealand and Ireland.

Up to this point you had to be a student at a college of high school, or employee at a certain company to be able to join the network. After September 2006 everyone over the age of thirteen, with an valid e-mail address, could join. The site was no longer restricted to schools and was now open to the whole world.

By 2009 Facebook had 200 million active users, and was finally getting more users than Myspace, becoming the world's biggest social network [15]. With the release of iPhone in 2007, and the launch of Facebook's mobile application in 2008 a new way of sharing became reality. The mobile application enabled Facebook users to send pictures, status updates and comments in real-time. Facebook introduced the "like" button in 2010, together with the growing application and gaming platform.

The movie "The Social Network" directed by David Fincher and Aaron Sorkin came out in October 2010. It is an american drama movie based on the early days of Facebook's history. The popular movie has received many awards, among them 3 oscars [16].

In April 2012 Facebook announces that they are buying the photo sharing application Instagram for $1 billion. This was the biggest acquisition that Facebook has done [17]. Instagram just finished a great year with the launching of the android application and a huge growth, with more than 30 million users, and more than five million pictures being uploaded every day [18]. Just a month later Facebook goes public, another big step for Facebook. Each stock were sold for $38 dollars, giving the company a market value of $104,2 billion dollars,

becoming the highest valued company in history. Facebook's market value was almost 4 times higher than Google in 2004 [19].

Facebook today As of September 2013 Facebook has 5 794 employees divided on 13 offices in the United States, and 24 international offices [20]. Worldwide, Facebook has 1,19 billion monthly active users. About 80% of the daily active users (727 millions) are from outside of the U.S and Canada.

2.3 Facebook Privacy

There exists numerous articles and papers written on the development of Facebook privacy, and many researchers have tried to map the human behaviour in regard to Facebook through for example the use of surveys. One of these articles is "Facebook privacy settings; Who cares?" by danah boyd and Eszter Hargittai [21]. The paper addresses a survey conducted on a cohort of 18- and 19-year-olds in 2009 and in 2010. The survey focused on their attitude and practice when it came to Facebook privacy settings. During this period, between 2009 and 2010, Facebook made many changes to their privacy settings. This was a turbulent period in Facebook history, with a lot of attention in media.

The demographics collected in the survey described in the paper by boyd and Hargittai was sex, age, race and ethnicity and parents' highest level of education. The ladder was used as a "measure" for socio-economic status. The demographics showed a diversity in the people taking the survey. The other data collected in the survey consisted of information within these topics: "Internet experience", "Use of Facebook", "Engagement in certain activities on social network sites among Facebook users" and "Experience with Facebook's privacy settings". Based on their discussion and conclusion, we have highlighted some of their findings:

1. Majority of young adults using Facebook have to some degree checked their privacy settings. Number of people who had checked increased from 2009 to 2010. One reason for this may have been the media attention Facebook received as mentioned above.

2. How familiar someone is with technology plays a role in how they handle their Facebook privacy settings. The reason for this assumption is withdrawn from the relationship between changing privacy settings and the frequency of Facebook use, as well as Internet skill. Considering the default settings, this is especially important since the least skilled people get more vulnerable when Facebook changes the default privacy settings.

3. Among the majority both genders are equally confident in changing their Facebook privacy settings.

danah boyd and Eszther Hargittai concludes, based on their findings, that experience and Internet skill is important to take into account in regard to how people handle their privacy settings on Facebook. It is incorrect to think that the Facebook users have the same approach to the site. This kind of thinking leaves a part of the users more exposed. It is therefore very important that the people who configure the default privacy settings take these users into consideration. They should be aware of the fact that every user is different and have a different basis of understanding.

Another relevant article on the topic of Facebook privacy settings is "Analyzing Facebook Privacy Settings: User Expectations vs. Reality" [11]. It addresses to what degree the Facebook privacy settings match the expectations of the users. To find information about the users view on the topic, they conducted a survey via Facebook with people recruited from Amazon Mechanical Turk (more information on Amazon Mechanical Turk can be found in section 2.5). They got 200 users who completed the survey. The average values for the users were: 248 friends, 363 uploaded photos, 185 status updates, 66 links, 3 notes, 2 vidoes. Their analysis is centred around two questions, and one of these questions are interesting for us to look at: *"What are the ideal privacy settings desired by users? How close are these to the actual settings that users have?"*

They had some very interesting results on their survey, and these are the ones we wanted to highlight:

1. Facebook privacy settings match the users expectations 37% of the time, and when the settings are not as expected they are almost always more open, and exposes the content to a wider audience than desired.

2. Modified privacy settings match the users expectations only 39% of the time. This implies that even though you are aware of your privacy settings, you can still have problems configuring them correctly and as desired.

3. Nearly half of the content shared by the users are shared with all Facebook users. This was desired 20% of the time.

4. When the privacy settings on photos has been changed by the user, the privacy settings on these photos match the users expectations less than 40% of the time.

As mentioned before there exists much material on the topic of Facebook privacy. We chose to shed light on these two articles, because of the similarities in topic to our paper. Later in our paper we will see if we can draw comparisons between the results in these two articles and our own survey result.

2.4 Interdependent Privacy

In today's society Internet is no longer a privilege, it is a human right. With the evolvement of the online social networks (OSNs) the incentive to share personal information has grown drastically. People create profiles at different OSNs and share personal information, pictures and comments with each other. With the enormous data sharing, privacy concerns arise. The privacy of an individual user is bound to be affected by the decisions of others, and are therefore to some degree out of the user's control. This phenomenon lays the basis for the term *interdependent privacy* [22].

Privacy Roger Clarke defines privacy as *the interest that individuals have in sustaining a 'personal space', free from interference by other people and organisations* [23]. Further Clarke divides privacy into multiple levels; bodily, personal behaviour and information privacy. Bodily privacy is concerned with the integrity of an individual's body, such as blood transfusion without consent, compulsory immunisation and compulsory sterilisation. Personal behaviour privacy relates to all aspects of behaviour, like sexual preferences, and political and religious actions. Information privacy is a collective term including personal communication and privacy of personal data. This includes the ability to communicate, using the desired media without being monitored by others, and claim that data about themselves not automatically should be available to others, even when there is data that should be processed by others.

In this article our focus will be on online privacy, the level of privacy and security of personal data published on the internet. For a user, the privacy and anonymity is the most important factor taken into consideration when using online services. It is a hot topic and now more important than ever, especially when the consequences are unforeseen, and the extent of them are often hard to predict. Biczók and China defines online privacy risks with the basis in Clark's privacy definition as described in the list below [22]:

- Personal: Potential loss of information about a user and the user's behavioural data. This can be done by phishing, hacking to steal secure and sensitive user data, like passwords and pin codes.
- Relational: Revelation of how a user relate to and communicate with others. Spyware is an offline application that can obtain a user's data without the consent of the user.
- Spatial: Invasion of the virtual space of an online user. An example of this can be unwanted comments and posts on a user's blog or social networking page.

Interdependent privacy In today's interconnected world, we share enormous amounts of data every single day. Protecting personal, relational and spatial privacy of individuals is no longer just dependant of only your individual actions, but increasingly depending on the

actions of others [22]. With the continuous growing use of social networks, data sharing has become very easy. We share photos, comments, videos, and links. This increasing data sharing arises concerns regarding interdependent privacy.

An example can be if Alice posts and tags a picture of her Facebook friend Bob. Alice finds the picture of Bob funny and sees no problem in posting it. Bob on the other hand, does not share Alice's opinion, he finds the picture embarrassing and inappropriate. Bob wants the picture removed, but by the time Alice comes around to remove it, people have already seen it, and maybe reposted it. Bob's privacy was dependent on what Alice did, and out of his own control.

Sharing information without consent from the users can lead to the emergence of externalities. In economics externalities is defined as the unintended costs or benefits that are imposed on unsuspecting people and that results from economic activity initiated by others [24]. When the effect is beneficial it is considered a positive externality. A negative externality is when the side-effect is negative. Let us relate this to our example with Alice and Bob. When Alice shares the photo without Bob's consent, it might be at benefit for Alice (in personolized experience), but for Bob it will be received as a negative externality, a loss of his online privacy. Another example of interdependent privacy is the Facebook platform for third-party applications (apps). How your privacy depend not only on your actions, but also on the actions of your friends. We will discuss this in more detail in subsection 3.3.2.

The article "Third-Party Apps on Facebook: Privacy and the Illusion of Control" was written in the end of 2011 and looks at the privacy threats with the use of third-party apps on Facebook [25]. In this paper the authors look at what information the third-party applications request when you install them, and how easy it is for an application to retrieve more information from a user than what the user initially wanted to. There has not been done any other studies on this topic before the time this article was written. Their aim is to increase user control of the apps' data control and alert the users when the apps' violate your initial privacy setting. When a user wants to add an application, the application is required to ask for permission to access certain information, like your "basic information", which includes name, profile picture, gender, networks, list of friends and other information that a user has publicly available to everyone. Other permissions that apps frequently ask for is "post to my wall", "send me email" and "access my profile information". You can later go to your settings and change what information you share with the apps, but by this time you may already have shared information that you initially wanted to keep private. As an example say that a user, we call her Alice, would like to keep her birthday private and have stated this in her privacy settings. Alice then install an app called "Happy Calendar", that let her keep track of friends' birthdays. When installing the app, they asked for permission to access hers and her friends' birthdays in addition to her basic information. Alice allows the app premission, to later find out that "Happy Calendar" has created an album with a calendar image showing the profile pictures to all her friends and herself. This album was posted on

her wall and Alice's friends received a notification about the album. The birthday that Alice initially wanted to keep private is no longer private. The article states that there should be more evident to the user when the app ask for information that is in conflict with the user's privacy settings. In the article two new designs of the approval page are presented and tested. From the tests it was clear that users was not always aware of what they share, and that a more extensive and informative permission-page would be necessary. It is important that the users understand what they are sharing and that apps often ask for information that you do not want others to see.

2.5 Amazon Mechanical Turk

The growth of the Internet have made it easier to conduct studies, surveys and so on. One commonly used technique for conducting these studies and surveys are called *crowdsourcing*. Crowdsourcing is a technique where you outsource a job to a undefined group of people. The beneficial aspects with crowdsourcing is that you are provided access to a large set of people who are willing to do the tasks you want done, for low pay [26].

Amazon Mechanical Turk is a good example of a crowdsourcing site. Amazon Mechanical Turk is a Internet marketplace where human intelligence is utilized to perform various tasks [27]. The people using Mechanical Turk are separated into two groups. You have the *requesters* that post jobs/tasks, and the *workers* who can choose from these jobs/tasks, and execute them for pay [26]. The jobs are posted as HITs (Human Intelligence Tasks). HITs are individual tasks that workers can complete to make money.

The Turk The name "Mechanical Turk" comes from a chess-playing automaton from the late 18th century. The Turk, as it was called, was a construction made to seem like a automatic chess-playing machine. In reality there was a chess-pro inside the machine, that steered the arms of the doll that was on the other side of the chess-board. The Turk was constructed in 1770 by the Austro-Hungarian Wolfgang von Kempelen. The reason for this construction was that von Kempelen wanted to impress the Empress Maria Theresia of Austria. The Turk toured around Europe and in America for decades, without anyone knowing the secret of the machine. The chess-pro that operated the construction played and defeated many, including Benjamin Franklin and Napoleon Bonaparte. Although many suspected that the Turk was steered by a hidden human, the trick was not exposed before 1820. The Turk was ruined in a fire in 1854 [28].

Advantages with Amazon Mechanical Turk There are several advantages of using AMT for conducting behavioural research surveys. Amazon Mechanical Turk enables the opportunity to reach out to a wide audience, since it provides access to a large subject pool [26]. When conducting a survey or other research for example in connection with school projects etc., you seldom have access to a large subject pool. Usually you may get your friends to

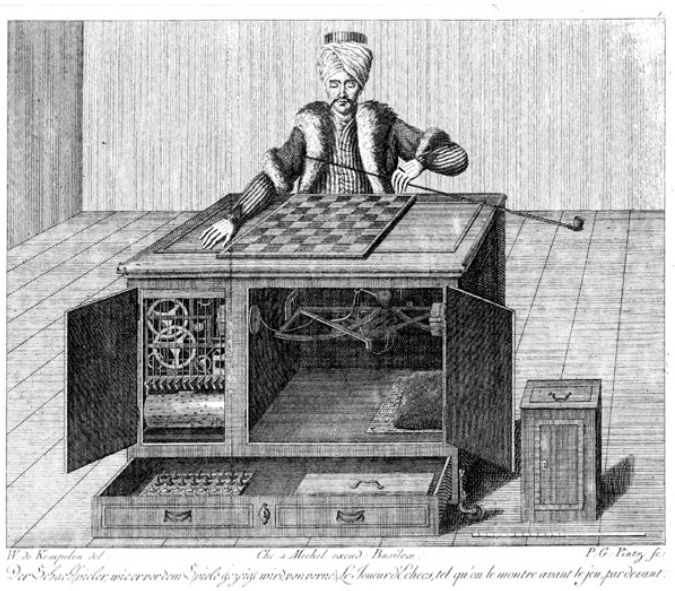

Figure 2.2: Engraving of the Turk. This figure shows the Turk with open doors and the different parts inside of the Turk. Wolfgang von Kempelen may have drawn this picture himself, since he was a talented engraver [28].

contribute, and maybe some other people going to the same school or a few people living in the same place. The results of this survey or research will most likely be reflected by lack of diversity. If you use Amazon Mechanical Turk instead, you get yet another advantage; subject pool diversity. The workers on Mechanical Turk are spread all over the world, and have different backgrounds. They have different religions, ethnicity, languages, different positions in society (economical), and age. The one last advantage with Mechanical Turk worth mentioning is that you get access to all the aspects mentioned above at a low cost. The workers are willing to take jobs and perform task for relatively low pay [26].

Financial Incentives Some concerns regarding the financial incentives are brought up in connection with Mechanical Turk (MTurk). One question is whether or not lower pay result in lower quality in the work conducted by the workers. It is important to have knowledge about the relationship between how good the workers perform, and the financial incentives given to them [29]. Research done by Horton and Chilton [30] shows that the least amount of pay a worker is willing to accept for a task on MTurk is $1.38 per hour, and they refer to this amount as the *reservation wage*.

The article "Analyzing the Amazon Mechanical Turk Marketplace" [31] written by Panagiotis G. Ipeirotis in December 2010 shows that the effective hourly wage on MTurk

is $4.80. This is calculated based on some observations, and also on some assumptions. What they observed was that the median arrival rate was $1.040 per day, and that the median completion rate was $1.155 per day. They then assumed that MTurk acts like an M/M/1 queuing system. Based on these observations and assumptions they used basic queuing theory and calculated that a task worth $1 is completed with an average of 12.5 minutes. Like mentioned earlier, this results in an effective hourly wage of $4.80.

Winter and Mason [29] conclude that if you increase the pay, the quantity of participants increases, but the quality of the work done does not increase. They think the reason for this is the *anchoring effect*. The anchoring effect describes that it is common for humans to depend too much on the first information given to them when making decisions [32]. In the case Winter and Mason presents: the workers who get more pay, also assume that the work they are about to conduct is more extensive, and therefore do not get more motivated to perform the work.

2.6 SurveyMonkey

SurveyMonkey is the world's leading provider of web-based survey solutions [33]. SurveyMonkey was founded in 1999 by Ryan Finley, and had 15 million users in 2013 [34]. Using SurveyMonkey as a tool you are allowed to create your own survey based on templates. To get started with SurveyMonkey and to create surveys you have to register the site, and choose an account type that matches your needs. The different account types have different prices. The more expensive, the more is included. There are several features available when using SurveyMonkey [35]. It is easy to create questions, with 15 question types available. You can also add logic to the questions. It is easy to customize the appearance of the survey, with the colors you prefer and so on. Getting responses on the survey is done by sharing an URL, for example on Facebook or in emails. When you have gotten answers on your survey, you get the data presented in graphs and charts. You can also export the results in various ways, for example all response data or just individual responses.

Chapter 3
Facebook Privacy

In this chapter we are going to look into what kind of privacy settings that exist on Facebook. We will also look at, and map, how the default privacy settings has evolved over time. In addition to this we will look at some of the features introduced by Facebook over the years, and how these features have effected the privacy on Facebook. Finally we will review some of Mark Zuckerberg's thoughts and comments in regard to Facebook privacy.

3.1 Privacy on Facebook

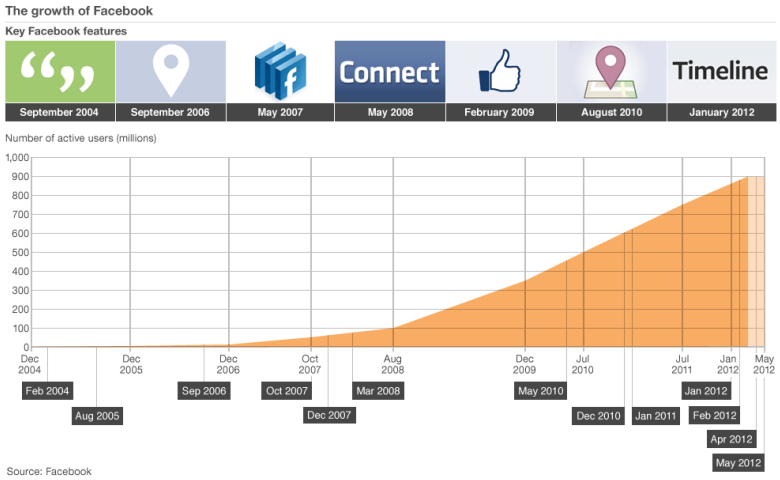

Figure 3.1: The development of Facebook users and introduction of new features. The orange field in the graph shows the increasing number of Facebook users over the years. Key Facebook features are shown over the graph according to when they were introduced [18].

There is no doubt that Facebook has had a remarkable development, both when it comes to number of active users and the development of new features, as shown in Figure 3.1.

Along with new users and new features, there has also been made major changes to what kind of privacy settings exists and what kind are needed.

3.1.1 Facebook Settings

Whenever Facebook make an update to the settings, the users usually get a personal message informing them about the change. Because of the high number of users, this change happens gradually. This means that not everyone will get a notification about the changes made at once [36]. Despite the changes over time, the main control of ones privacy lies in the hands of the users. The users have the opportunity to make their profile more secure, than what is set to default.

The settings that exists

There exists numerous settings one can edit to make their Facebook profile more, or less, secure and/or private. The main problem to why people do not change them is probably that many are not aware of these settings, as well as the impact of having a public profile. An other problem can be that people are not confident enough in changing them. When they do not know hat the setting mean, it can be scary to change them. Regardless of this the settings exists, and it is up to each of the users how they are configured. On the Facebook settings page you have different tabs regarding different kind of settings. The settings available are elaborated in Table 3.1.

Table 3.1: The settings that exist on Facebook [1].

Setting tab	Description
General	Under this tab you can edit your name, username, email, *password*, which network you are part of and language.
Security	Under this tab you can do changes that makes it harder for someone else to hack into your Facebook account. Here you can enable/disable **Secure Browsing** (the use of https when possible). It is possible to turn on **Login Notification**. This means you will get notified either by email or text message (after you choice) when your account is accessed from a computer or mobile device that you have not used before. It is possible to enable something called **Login Approvals**, where a security code is required to access your account from a unknown browser. This code can be given to you in a text message sent to your mobile. You have the choice to use **Code Generator** on your Facebook mobile app to reset your password or generate login approvals security codes. Under the security tab you can create **App Passwords**, add **Trusted Contacts**, view **Recognized Devices** and **Active Sessions**. Under active sessions you can see all sessions active via your accout. Here you can look for unfamiliar devices or locations, and if you find a session that is not you, someone else have been logged into your account. This session can easily be ended.
Privacy	Under this tab you can change the audience for your future posts. You can also chose who can send you friend requests, who can look you up using the email address you provided and who can look you up using the phone number you provided. The last setting concerns whether or not you want other search engines to link to your timeline. This can either be turned On or Off.
Timeline and Tagging	Under this tab you can choose who can post on your timeline, who can see posts you've been tagged in on your timeline and who can see what others post on your timeline. You can also choose whether or not you want to review tags people add to your own posts before the tags appear on Facebook, and you can choose the audience for a post you're tagged in if they aren't already in it.

Blocking	Under this tab you can block users, app invites from specific users, event invites and specific apps. Under this tab you can also make a **Restricted List**. Your friends on this list will only be able to see the information and posts that are public.
Notifications	Under this tab you can control how you get notifications, and what you get notified about.
Mobile	Under this tab you can add your phone number(s), and activate registered phone(s) for text messaging.
Followers	Under this tab you can turn on follow, this makes it possible for other people to follow you. Followers will only see your public posts and will not be added as friends.
Apps	Here you can choose whether or not you want to use apps, plugins, games and websites on Facebook and elsewhere. You also get a list of the apps you use, and you can edit the audience for things posted via these apps. The people on Facebook who can see your information can bring this information with them when they use apps. This is to improve the user experience. Under **Apps other use** you can control the categories of information that people can bring with them when they use apps, games and websites. You can also turn on something called **Instant personalization**, which let you see relevant information about your friends the moments you arrive on select partner websites. Finally, under this tab you can choose the audience for the things posted using old Facebook mobile apps that do not have the in-line audience selector.

3.2 Default Settings on Facebook

Facebook has evolved from being a networking site for students attending Harvard to becoming a global phenomenon. Facebook's user interface has gone through several changes over the years, which has brought both joy and frustration to the users. When these changes have been made, there has also been adjustments to the default privacy settings as well [37]. At the beginning, in 2005, when Facebook first was applied outside of Harvard University, the users personal information was only accessible to a users Facebook friends and to people connected to the same network on Facebook [2]. This is far from reality today. We will now look into how the default privacy settings on Facebook has developed.

3.2.1 Development of Default Settings

The main changes to the default privacy settings are emphasized in Table 3.2.

Table 3.2: Changes in the default privacy settings on Facebook from 2005 until today. [2, 3]

Year	Default Privacy Settings
2005	Personal information (e.g., name and profile picture) is only visible to specific groups specified in your privacy settings.
2006	The only information displayed in your profile is your school and specified local area.
2007	Name, name of school (network) and profile picture (thumbnail) is available to all Facebook users.
November 2009	Name, profile picture and demographics is available and searchable to the entire Internet. In addition to this, list of friends are visible to all Facebook users.
December 2009	Your name, profile picture, list of friends, pages you are fan of, demographics and likes are available for the entire Internet.
April 2010	The entire Internet can see everything, except wall posts that are limited to friends and photos that are limited to your network.
2011	
2012	
November 2013	The entire Internet can see everything, except posts you've been tagged in on your timeline and others posts on your timeline, which are limited to friends of friends.

3.2.2 Default Settings 2013

To examine the default settings on Facebook anno 2013, we created a new Facebook profile. Figure 3.2, Figure 3.3, Figure 3.4 and Figure 3.5 shows the outline of the different settings without any alterations, in other words the default settings.

Figure 3.2 shows how the default security settings look like in November 2013. As we can see from the Figure, secure browsing is enabled by default. This became default in july 2013, but has been an option since 2011 [38].

Figure 3.3 shows the default privacy settings in November 2013. *"Who can see your future posts?"* is set to *Public*, which means everyone can view you posts. *"Who can send you friend requests?"* is set to *Everyone*. *"Who can look you up using the email address you provided?"* and *"Who can look you up using the phone number you provided?"* is set to *Public*, which means it is easier for people to find you on Facebook if they know you email

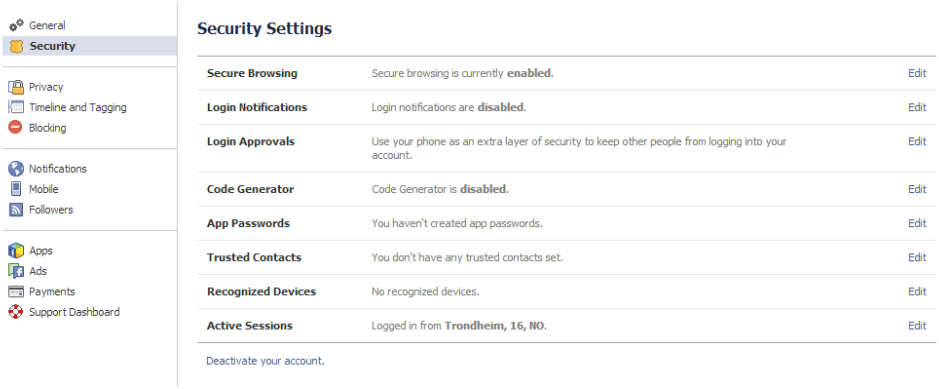

Figure 3.2: Default security settings on Facebook November 2013.

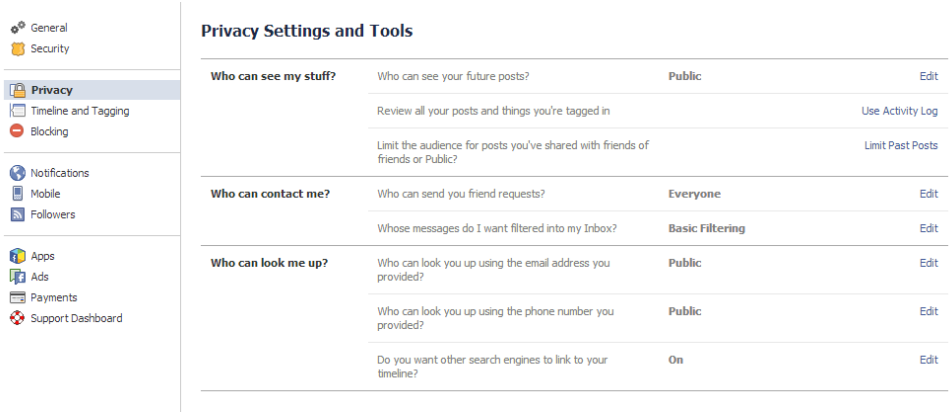

Figure 3.3: Default privacy settings on Facebook November 2013.

or phone number. The setting *"Do you want other search engines to link to your timeline?"* is turned *on*. This means that for example if you google a person, the Facebook profile will appear in the search. To summarize, the privacy settings are *as public as they can get* by default.

Figure 3.4 shows the default settings for timeline and tagging on Facebook in November 2013. *"Who can post on your timeline?"* is set to *Friends*, which means that only Facebook friends can add things (photos, comments, links, etc.) to your timeline. *"Review posts friends tag you in before they appear on your timeline?"* is set to *off*. This means when friends tags you in something, it will appear on your timeline before you have had a chance to review it. In most cases this is probably fine, but it may occur that a Facebook friends tag you in

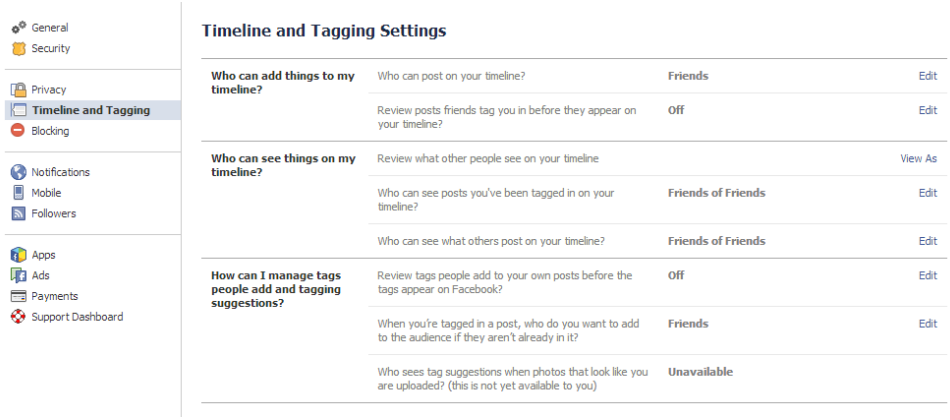

Figure 3.4: Default settings for timeline and tagging on Facebook November 2013.

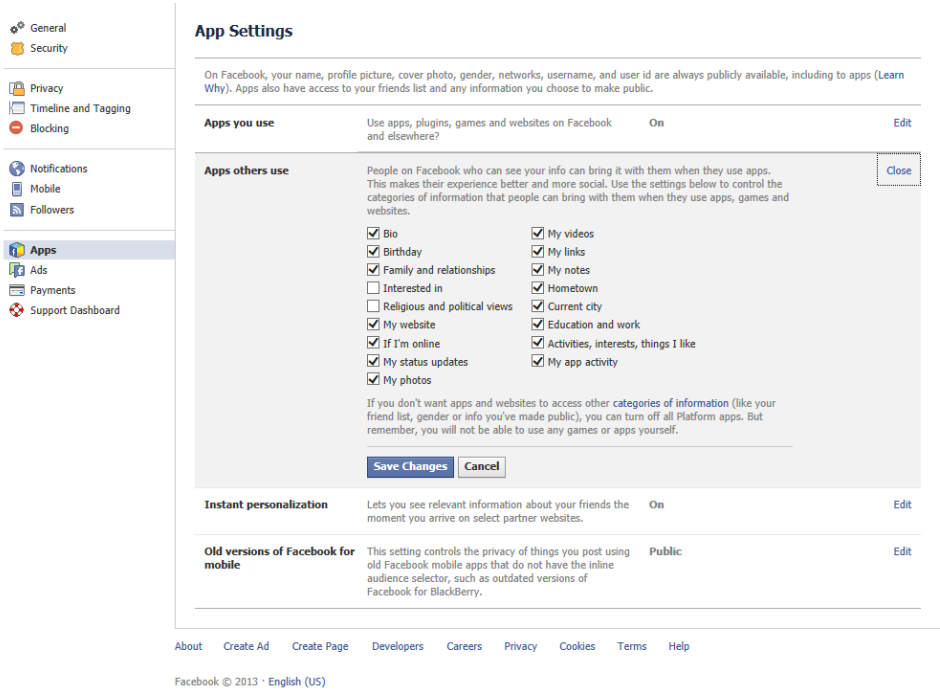

Figure 3.5: Default settings for apps on Facebook November 2013.

something you would not prefer to have displayed on your timeline. In these cases it would be desirable to have the review-setting turned on. *"Who can see posts you've been tagged in*

on your timeline?" and *"Who can see that others post on your timeline?"* is set to *Friends of Friends*. In contrary to those who can post on your timeline, which are friends, friends of friends are able to view the content added to your timeline. If you have many friends on Facebook, and these friends have many friends each, the audience for posts are suddenly extremely large.

Figure 3.5 shows the default settings for apps on Facebook in November 2013. Usage of apps, plugins, games and websites on Facebook and elsewhere are turned on by default. Under "Apps others use" you can choose which categories of information that people can bring with them when they use apps, games and websites. As you can see in the figure, almost every box i checked as default. The only exception is "Interested in" and "Religious and political views". Also shown in the figure, instant personalization is enabled by default and the privacy settings for the information you post/have posted using old Facebook mobile apps is set to public as default.

Default settings does not preserve privacy It is safe to conclude that the default privacy settings on Facebook anno 2013 is far too public. Unless there are conducted changes to the privacy settings, the timeline will be publicly available, with the exception of posts you've been tagged in and other's posts on your timeline which is "only" visible to friends, and friends of friends.

3.2.3 Default Settings for Teens

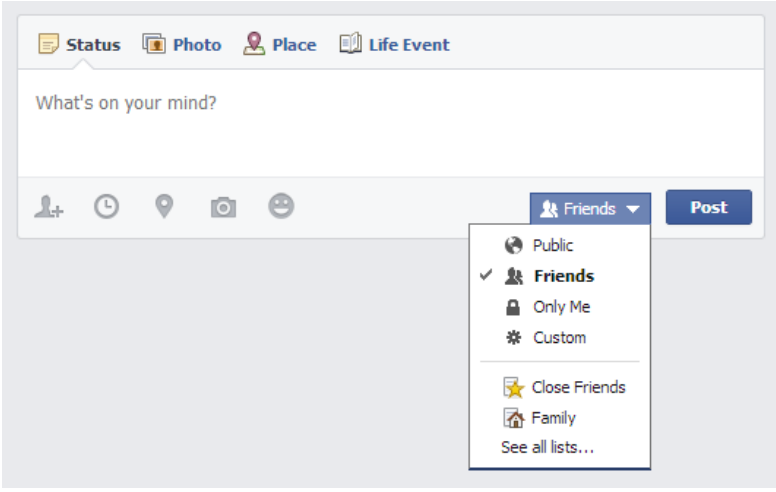

Figure 3.6: Choosing who can see a status update. When posting a new post the user can choose the audience the post will be visible to. This can either be "public", "friends", "only me" or "custom".

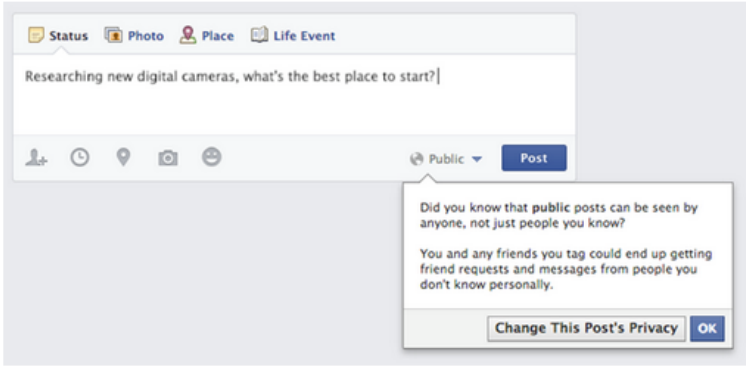

Figure 3.7: The message shown to teens when posting to the public for the first time. After the first time they post to the public the message in Figure 3.8 is shown [39].

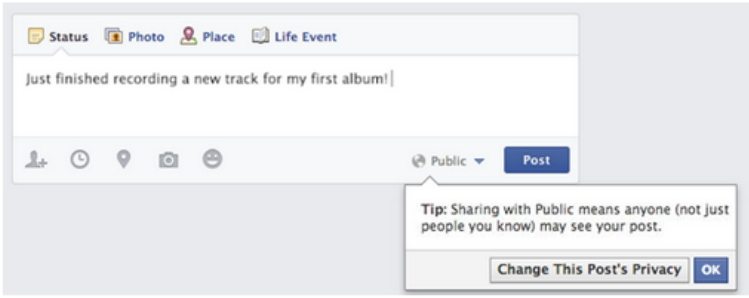

Figure 3.8: The message shown to teens when posting to the public, except for the first time. The first time they post to the public the message in Figure 3.7 is shown [39].

Each time a user on Facebook share a status update, the user chooses who the post is visible to, see Figure 3.6. The change you make will remain the same in future posts, unless you decide to change it. Up until today the default audience is set to "public", but for teens between 13-17 years, it has been "friends of friends". On October 16th, 2013, Facebook announced to change the default setting for teens [39]. Now the initial audience for posts are "friends". Teens can later change this to "public", this was not a option before. Teens are active users of social media, and want to be heard, either it is political engagement or an opinion on a movie. Further Facebook allows teens to turn on Follow, by doing this their public posts will show up in people's news feeds. Facebook designed these changes to improve the facebook experience for young people. In [39] Facebook also makes it clear that they take the safety of teens very seriously, and therefore have created a more extensive warning message, shown in Figure 3.7. This message appears when a teen changes the audience for their post. If they continue to post to the public, they will will get an additional

reminder message, as shown in Figure 3.8.

3.3 Facebook Features - Impact on your Privacy

3.3.1 News Feed

News Feed is the first thing you see when you log into your Facebook account. It is a list that constantly is updated. This list includes the activity from your friends and info about Pages you follow on Facebook. Examples of activities that are shown on the News Feed are photos, status updates, links, apps, likes, comments, posts written on timelines and so on. Often are activities with many comments or likes on top of your News Feed. The reason for this is that Facebook uses a algorithm to determine "top stories". The algorithm takes several elements into account when deciding top stories; number of comments, who posted it, and what kind of post it is. The users also have the opportunity to filter their News Feed to for example activity just from close friends, most recent activities, activities of the users in a same network etc. [40].

When News Feed was introduced in 2006, many users showed disapproval because they was not given the control of who could see their updates, and was not able to opt out. A consequence of this disapproval was the creation of a group called "Students Against Facebook News Feed", which got 300 000 members in two days. This lead to an apologize by Zuckerburg: "We really messed this one up. We didn't build in the proper privacy controls". He stated that this was a big mistake on their part [41].

3.3.2 Facebook Platform - Apps

The Facebook Platform was launched in May 2007 at a developers conference in San Fransisco. This feature enabled a third-party developer to build social applications [18]. These applications will then be integrated with Facebbok, both mobile and on the web. "Right now, social networks are closed platforms," Zuckerberg said. "And today, we're going to end that" [42]. Zuckerburg promised the developers a level playing field, and the opportunity to build apps that could compete with the ones Facebook created themselves. As well as access to the network's at that time 24 million users. In [42] McKenzie talk about the launching moment as the moment when Facebook transitioned from having MySpace as a competitor, to getting Google as the competitor. And that Facebook went from being a wall to start being a platform.

18 months after it was launched, Facebook had abandoned the idea of a level playing field, and had started baking in features that cut of developers who tried to develop similar products as Facebook. Terms as "Zucked over" became more normal amongst developers. What was once looked at as a beautiful piece of engineering, had became a disappointment. Today the platform is mainly used to distribute games. Zynga, who made popular games like Farmville, is about the only company who have managed to build their whole business

inside the Facebook Platform. The platform did not become what it intended, and as big as everybody was hoping for. And according to Facebook's own developers it has been a hard one to swallow.

Even though Platform did not reach out to all the areas originally intended, it is still popular. By the the end of March 2012, there were more than 9 million apps and websites integrated with Facebook through the Platform [43].

As mentioned in section 2.4, apps is one area that highly concerns the users to interdependent privacy. Facebook Help Center [44] explains that apps are designed to enhance the user experience with engaging games and useful features. In order for the apps to do this they ask you to share personal information. All apps ask for your basic information, this consists of your name, profile picture, cover photo, gender, networks, username, and user id. This is information that always is publicly available. Apps also have access to your friends list and any information you choose to make public. The apps ask for this information to enhance the users experience by personalising content, helping the user find friends that also uses the app, and make sharing of information easier. As well as speeding up the sign-up process, so that the user can start using the game or app right away.

Application permissions. As of November 2013 Facebook has 54 permissions divided into 6 different categories [45]. These categories are email, permissions, extended, extended profile properties, open graph permissions, page permissions and public profile and friend list.

Apps privacy control. In the Facebook settings [1] under the tap "Apps" the user can manage apps, Figure 3.5, and control what information that will be shared with apps others use. The user also has the opportunity to turn off all platform applications. The user will then no longer be able to use any games or other applications.

Installing an Application

We will now look at the process of installing an application from Facebook Platform. As mentioned when installing an app, the user will be asked to give permissions to share information. This information vary a lot, some just ask for your basic information, some ask for relationship status, birthday and also permission to post to your Timeline in your name. We have looked at the very popular application TripAdvisor. According to the site secure.me [46] TripAdvisor have a poor reputation because it may be a threat to your privacy.

Installing on a PC. When opening TripAdvisor in Facebooks App Center on a personal computer, we are directed to TripAdvisors page, as shown in Figure 3.9. The page contains information about the application, as well as the permissions required. These permissions are shown in the top right corner. The permissions that TripAdvisor requires exceeds beyond

on basic information. We can put these permissions in the follwing privacy groups; personal privacy, relational privacy and spatial privacy. Personal privacy contains the permissions to access personal information about the user like location, education, hometown, work history, your photos, your status updates, e-mail address and likes. Relational privacy includes retrieving friends' profile information; education history, hometown, likes, locations and work history. As well as photos shared with you, and status updates shared with you. The last privacy category, spatial privacy, concerns posts that the app post on your behalf on your Timeline. By default these posts are set to public, but you can easily change the setting before installing the app. When pushing the "Go to App"- button, you automatically give your consent to the required permissions and install the App. this can be misleading, since the user might look for a installation button, or some kind of verification that the installation has started. This may lead to an app being installed without the user knowing. The permissions are all shown, and explained, but not as visible as they used to be before App Center was introduced. Figure 3.10 shows the authentication dialogue as of 2011, before App Center was introduced. You got a pop-up windows stating all the permissions requested by the app. The use of pop-up windows like these made it much easier for the user to review the permissions, and to not miss out on them.

Figure 3.9: The application TripAdvisor inside Facebook's App Center.

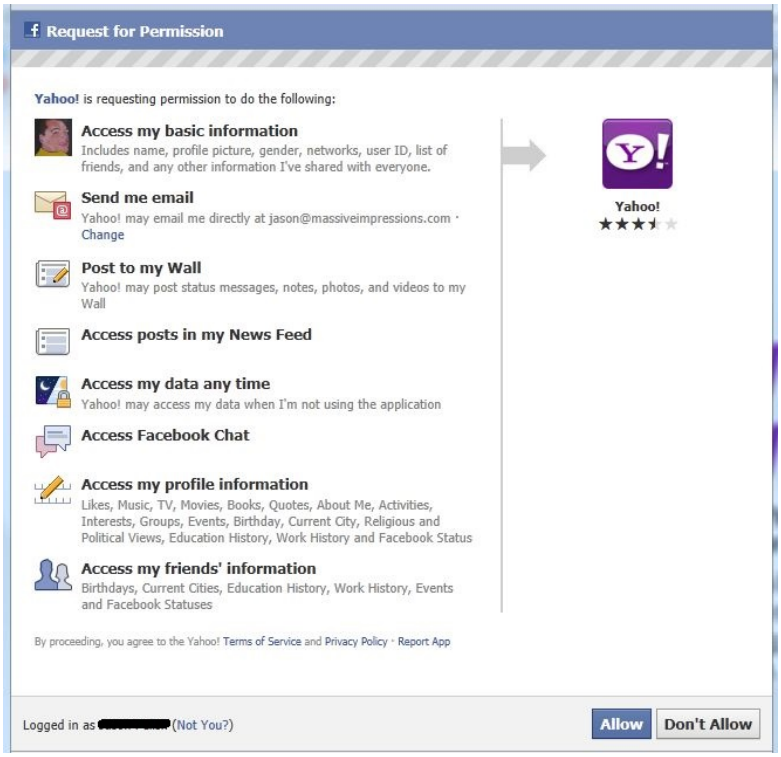

Figure 3.10: Request for permission when installing app anno 2011.

Installing on a mobile phone. The installation process looks a bit different when you install an app on the Facebook application on a mobile phone. When clicking on the application TripAdvisor in the Facebook mobile app, the user is directed to Apples App Store or Android's Play store. Figure 3.11 shows the application in Android's Play Store. When TripAdviser is installed, the user can choose if he/she would like to connect with Facebook as Figure 3.12 shows. If the user choose to connect with Facebook the request for permissions will appear in a pop-up window, this you can see in Figure 3.13. The user can then choose either to cancel or press OK, which means that you give your consent.

3.3.3 Beacon

At the end of 2007 Facebook launched the feature Beacon. Beacon was created to help users easily share information from other websites with their Facebook friends [47]. Beacon was a key part of the Facebook Ads system. The aim was to connect businesses and users and create a more targeted advertising towards the users.

When Beacon was launched it had 44 partner sites, among these were Live Nation,

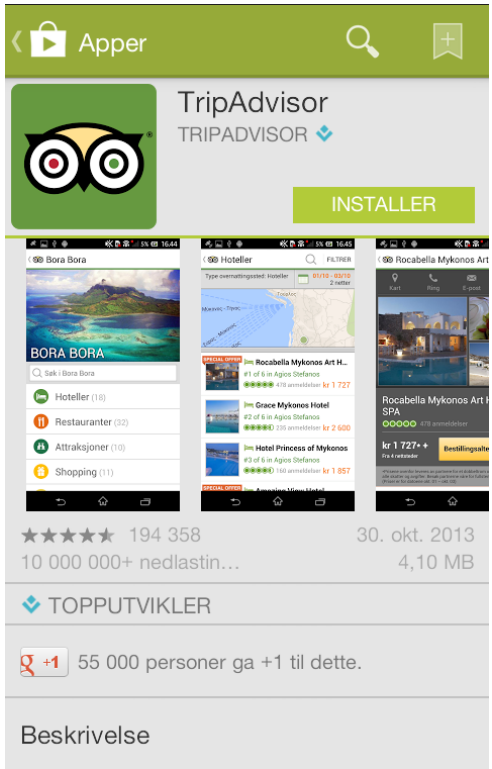

Figure 3.11: Installation page for TripAdvisor. This figure shows the installation page for TripAdvisor in Android's Play Store.

fandango.com, Trip Advisor, STA travel, eBay, the Knot and Zappos.com. According to the Facebook announcement [47] these websites could determine which actions was most relevant and appropriate for a user to share on Facebook. This could be anything from watching a video, a new high score on an online game, posting an item for sale or completing a online purchase. When a user, that is logged on to Facebook, enters a website that is part of Beacon, they will receive a message asking whether they would like to share their actions on Facebook. If a users agrees, the users actions on that page will be shown in their news feed or mini feed and shared with their friends.

Beacon received a lot of attention and privacy concerns. Some websites posted to Facebook without asking the users if they want to share the information first. Beacon is a very short piece of code provided by Facebook. The participating websites implement this code on the actions that they would like people to share. An example described in [48] is with the blog page TypePad. The user have the opportunity to chose whether Beacon should be turned on or not. When creating a post and publishing it the user receives a small pop-up

Figure 3.12: The page where you can choose "Log in with Facebook". On this page you can choose whether or not you want to log in with Facebook. If you choose to log in with Facebook you are redirected to the page shown in Figure 3.13.

window in the lower right corner stating that you are now sharing this information with Facebook. The pop-up allow you to decline, but here you have to be quick, the window is not visible for long. When entering Facebook a message is shown at the top of the users wall. Telling the users that a website have shared information with Facebook. You then have the opportunity to go through and select whether that website is allowed to share at all, to just friends or to the public.

But not all websites have created an option for the users to choose for themselves whether or not to opt-in. And pushes to Facebook without notifying the users or lets the users select themselves that they want to share it. An much used example of this is a man buying an diamond engagement ring online [49]. Within hours he starts receiving congratulations from friends and family. The website had posted the purchase on the guys public Facebook page, including a link to the purchase and the price. All his friends received an notification, including his coming fiancée. So much for the surprise engagement. There are several similar

Figure 3.13: Facebook's request for permissions on mobile phone This figure shows the page where Facebook states what permissions they are requesting before you can start using the app. Here you can choose to either cancel or press OK.

stories. This is unfortunate for the users, but also for the companies using Beacon, it puts them in a negative light. Beacon could have been a great asset for different companies, and a great way for them to broadcast themselves.

Another problem is that Beacon only checked that someone was logged on Facebook. When several people use one computer it could create problems, since Beacon was machine specific. One family member, the mother, could be logged on while her 10 year old son plays an online game, and manages to make a new high score. This high score will then be posted in the News Feed on the mothers Facebook profile, and shown to the mothers friends. This is not very fortunate for the mother. Beacon only checks that there is a valid Facebook cookie on the machine and then pushes the content to that Facebook user, without any validation.

In a blog post, Mark Zuckerberg apologized for the way the feature was created and for the handling of the complaints in hindsight [50]. Zuckerburg explains that one of the problems with making the system opt-out, was that if a Facebook user forgot to declilne

something Beacon still went ahead and posted and shared with the users friends. Further he explains that it took them too long from they started receiving complaints to they were able to decide on a solution to the issues. Facebook released features that gave the user more control. And the users got the ability to turn off Beacon completely. In addition Facebook promised their users that they did not save the information Facebook received from the participating websites when the user had chosen to not use Beacon.

All of beacons issues resulted in a lawsuit against Facebook, and some of the participating companies. The lawsuit resulted in a settlement, where Facebook agreed to shut down the feature and gave $9,5 million to found a new non-profit foundation that would work with online privacy, security and safety [51]. Beacon was shut down in September 2009. Beacon is mentioned as one of the darkest marks in the history of social networks.

3.3.4 Facebook Connect - "Log in with Facebook"

From may 2008 users had the ability to connect and log in to other web pages via Facebook, "log in with Facebook". The users are allowed to connect their Facebook identity, friends, and privacy to any website supporting this feature. This was Facebook's first attempt to allow access to user data from Facebook outside of Facebook itself. The important features of Facebook Connect are stated in Table 3.3.

Table 3.3: Facebook Connect Features [4, 5].

Feature	**Description**
Trusted Authentication	Authentication when users connect their account to a third party. During the user's experience the developer could at any time like to add additional social context. These activities need authentication from the user. In other words, the user have total control over the permissions that are granted.
Real Identity	The users can port information linked to their real identity with them on the web to a third party website. This information includes basic profile information, profile picture, name, friends, photos, events, groups etc.
Friends Access	As mentioned, the users take their friends with them to third party sites. This makes it possible for the developers to add social context to the sites. You will also get notified if some of your friends already have an account on the site.
Dynamic Privacy	When the users move around from one place on the web to another, they always bring their privacy settings with them. This is done so one can be sure that their information and privacy settings are updated at any time. In other words, when you update your privacy settings on Facebook, they will automatically be updated on third party sites.

3.3.5 Places

The feature Places was launched in the United States August 2010, and later in te rest of the world, this enabled the users "check in" using their mobile device [52]. This feature enables the users to share a place that they really like with their friends. This can be a cafè, a new restaurant, a concert or maybe a nice hiking trail. Have you ever been to a concert and found out afterwards that several of your friends also where there? This is what the feature places solves for you. You can for example check in to the concert, and see who else is there or see who of your friends is close by. After you have checked in at a place, your check-in will appear in your friends News Feed. It is possible to tag the friends you are with. The user are in control of what is shared and who it is shared with. A user chooses weather or not they want to share the location they are at. If a user is tagged in a check-in, they will will always be notified. The default audience is "friends", unless the users chooses to share differently, for example with "everyone", or a more restrict option, just specific friends.

This feature is also used with third-party applications, like Tripadvisor or other travel planning applications. They collect your check-ins to generate a mat that shows where you have been in the world. So if you are planning on going to Paris you can see who else has been there and also at what places, restaurants etc., they have checked in to. When you write a post on Facebook you can decide if you would like to add a location to the post. And when creating the post you also decide the audience. On the mobile phone it is a little different. Here the location setting is located in the phone settings and not in the Facebook settings on the phone. The places setting on the phone can get your location by using Wi-Fi, mobile network or GPS signals. if one of these are turned on, the users location will appear on chat messages. When a user writes a post and wants to add a locations, the phone asks the user to turn on GPS, this to get a more accurate location. If the users desires not to turn it on he/she can write in a location, for example "Oslo", and Facebook will suggest places. A feature on the Facebooks mobile application is "places nearby". Here the user can see what places that is close to their current location, and what friends that have liked the page and rating from other users. This is shown in Figure 3.14 and Figure 3.15. A user also have the ability to add locations to photos that they post themselves or that others have posted.

3.3.6 Timeline

Facebook timeline was introduced in December 2011 [19]. This feature made the entire history of the users visible: your posts, posts by others, likes, photos, links, pages liked, comments and other things that you have shared on Facebook. The timeline showed much more than the old profile did, and it was far more visual [53]. On the top of your timeline it is room for a big photo. This photo is called a *cover photo*. Cover photos are publicly available, and it is not possible to change the settings for them. You can of course choose

Figure 3.14: Nearby function on Facebook mobile. Where in the mobile application of Facebook to find the "places nearby"-feature.

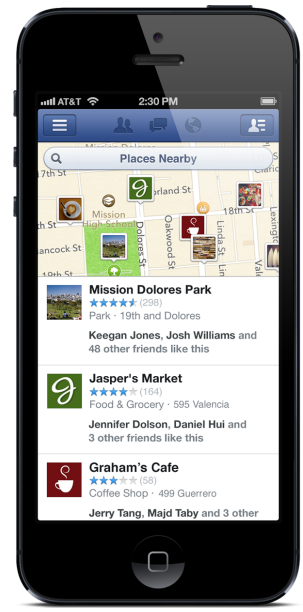

Figure 3.15: Places nearby feature. Displaying the screen where the users can see what kind of places that is close to their current location. It shows which friends like the certain place or has checked in there.

which photo you want as your cover photo, or just choose not to have a photo there at all. When scrolling down your timeline , you'll see photos, posts etc. and different events in your life in order of when they happend in time [53]. You can look at it as the story of your life. You get the opportunity to "go back in time" and fill in the blanks. If you want to emphasize, for example an event or a photo, you can highlight it with a star, or on the other hand, if you

want to hide something from the timeline you can also do so.

Privacy concerns regarding Facebook timeline When timeline was introduced many people became overwhelmed by the changes, and felt they lost control over their privacy. When you agreed to start using timeline, you got a certain period of time to review and edit your timeline before making it public. This gave the users the opportunity to clean up their timeline before everyone else could view the content of it. Cleaning up the timeline can be done using something called the "Activity Log" [54], which is shown in Figure 3.16. The activity log is basically a list over everything ever done in connection with you on Facebook, either done by you or by others. The activity log also makes it easy to view and change the audience for the different "activities". If you are an active user of Facebook, reviewing the whole activity log can be very time consuming.

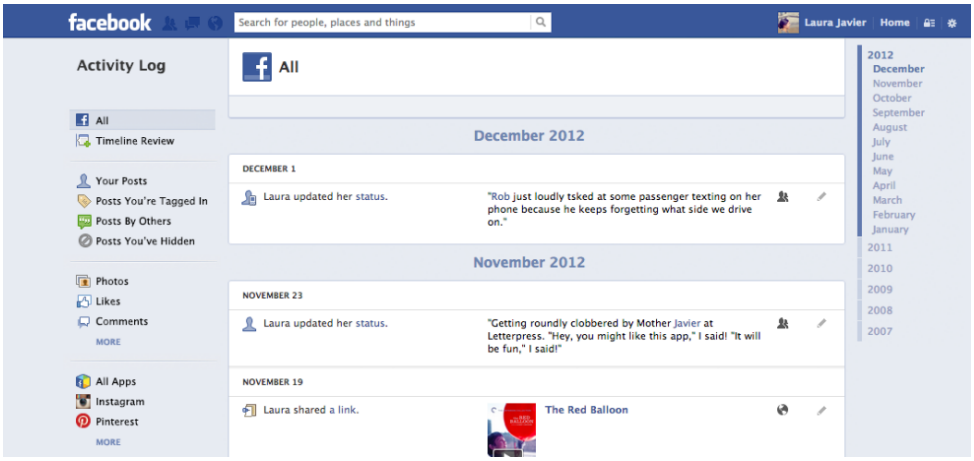

Figure 3.16: Example of an activity log on Facebook. On the left side you see types of content. If you want to view for example "Posts by others" you can do so by clicking on it. To the right you see a list of the years and months. You can click on which year or month you want, and review the activity from that year/month [54]

The introduction of timeline was not in itself a privacy breach since you had, and still have, the opportunity to decide what you want to be visible on it, and what you want to hide. On the other hand, there are people who are extra exposed when Facebook introduced new major changes, like the timeline. Lets refer back to section 2.3 in Chapter 2, where we highlighted some of the findings from the survey addressed in the paper "Facebook privacy settings; Who cares?" by danah boyd and Eszter Hargittai [21]. boyd and Hargittai concluded their paper, based on their survey and findings, that experience and Internet skill is important to take into account in regard to how people handle their privacy settings on Facebook. Since familiarity with technology plays a role in how people handle their Facebook privacy settings, one can

assume that the least skilled people get more exposed when Facebook changes the outline of the default privacy settings. This can be seen in the context with the introduction of the timeline. The least skilled users of Facebook that perhaps do not know how to change their privacy settings, probably was left extra exposed when the timeline was introduced and their timeline may have shown, and may still show, more than they actually would prefer.

There also exits privacy settings connected to you timeline under "Timeline and tagging" in your settings on Facebook. You can regulate who can add things to your timeline, and who can see things on your timeline. Under "Privacy" you can also regulate who can see your future posts.

3.3.7 Graph Search

Graph Search is a semantic search engine introduced in a beta version by Facebook in March 2013. During the summer 2013 the Graph Search became available for everyone using Facebook with US English language [55]. The old search bar at the top of the page is replaced with a larger search bar, Graph Search [56]. The Graph Search enables the users to search using natural language queries, and not just search using keywords. In addition to this the search results will be based on both relationships and content [55]. Two examples are "Photos of 'friend's name' are tagged in" and "Restaurants in Oslo, Norway visited by my friends". The basic idea is that the users are given the possibility to search Facebook for different stuff (photos, people, places etc.) in a specific subset, specifying the queries [57]. To emphasize how specific the search can be, we will provide you with an example. Let us say you met someone at a party and the only thing you know about the person is the name, where the person goes to school and you know that the person is a friend of one of your Facebook friends, you can write a query which reads as follows: *"People named 'name of the person' that are friends with 'name of the common acquaintance' and who go to 'name of schoool'"*. Off course this may not give the outcome you wanted, if the person for example have not given any information about where he/she goes to school on Facebook. Just having the opportunity to perform such queries gives the user more power, and makes it easier to connect to new people.

Zuckerberg says that Graph Search is centered around "making new connections", because the feature makes it easier to make new connections [57]. Facebook emphasizes that the purpose of Graph Search is not to replace traditional web search. The Graph Search concerns, on the other hand, the filtering of all photos and all connections on Facebook. Since Facebook is the largest online social network in the work, it is *not just a few* photos and connections available, but over 240 billion photos and over 1 trillion connections. The choices you have made in your settings determine what friends and others can see when they conduct a Graph Search [58]. If a photo is set to "Only me" no one else can find it in the search, it it is set to "Friends" friends can find it in their search, and if it is set to "Public" anyone who searches for it can find it. Graph Search is in other words a good tool for viewing

as many photos as you are allowed to view of people who are not your Facebook friends. The photos of you that are public will come up in a Graph Search regardless of how you have set your privacy settings. As long as someone has posted a photo of you as public, the entire Facebook can find and view this photo via Graph Search. So if you are interested in viewing pictures of a specific person who is not your friend on Facebook, it is not necessary to start digging through numerous albums and so on, but just do this with a quick search.

A limited group of people got access to Graph Search in January 2013. During a introductory press conference, Mark Zuckerberg stated that Graph Search was in it's early stages, and that it will take years to complete it. He said: "Graph Search is a really big project, and it's going to take years and years to index the whole map of the graph". After the introduction of Graph Search, many questions was brought up about the privacy issues regarding it. One of the issues brought up was that the tool makes it easier for people to retrieve information and photos about other people who do not want this content to be available and seen. The fact is that people only get to view content they already could view, but it makes it much easier to find this content. Facebook assured that Graph Search does not affect the privacy of minors. They stated that identifying information about those between the ages of 13 and 17 would only be shared with friends of friends of that minor [59].

Graph search is for the time being still only available for users using US English language on their Facebook, but is a work in progress like mentioned before. Facebook has stated that further work on the feature deals with searching across posts, comments and mobile [59].

3.3.8 Facebook Removes Search Privacy Setting

Facebook announced October 11 that they will remove the setting that has made it possible for Facebooks users to hide from the ability to be looked up on the Internet[60]. It was only the users that have not used the setting "who can look up my timeline by name" in December by last year that was affected by the change. Facebook explains the removal of the feature by it being outdated, and that there are several others ways to find a persons time line. They argue that it can be confusing for the user when they try to look up someone and do not find them. Mark Zuckerberg said that a users should do things they want to keep secret.

(sånn jeg ser det så er det jo fult mulig å søke opp hvem som helt på facebook sin egen søkefunksjon, det betyr jo ikke ta jeg ønsker å være søkbar på google.

3.4 Zuckerberg's Thoughts

Zuckerberg ones said this about Facebook in a one of his meetings: "I mean, one way to look at the goal of the site is to increase people's understanding of the world around them, to increase their information supply," he said. "The way you do that best is by having

people share as much information as they are comfortable with. The way you make people comfortable is by giving them control over exactly who can see what" [12].

This comment from Zuckerberg brings out his thoughts around the privacy issues. He wants the users of Facebook to be comfortable with sharing information, and give them this confidence by giving them control. In general the privacy settings and restrictions that Facebook has have protected the users. They can easily change the setting and decide who can see what. Zuckerburg firmly means that you should not post comments or pictures of things you do not want anybody else to see. And if a user does so, the user has to take the blame for it, not Facebook. Zuckerberg was once asked about pictures put on Facebook of students drinking at an East Coast college, which led to some students being expelled. His answer to this question was: "First of all, it's pretty stupid if you put up pictures of you doing drugs on Facebook. I think that that's just sort of the deviant behavior on the very far end of the distribution. I bet that those kids do not post pictures of them doing drugs on Facebook anymore." He added that he meant this was a "pretty shitty way to learn that" [12].

Mark Zuckerberg wrote this in a letter to possible investors [61]; *Facebook was not originally created to be a company. It was built to accomplish a social mission - to make the world more open and connected. People sharing more - even if just with their close friends or families - creates a more open culture and leads to a better understanding of the lives and perspectives of others. We believe that this creates a greater number of stronger relationships between people, and that it helps people get exposed to a greater number of diverse perspectives.*

Chapter 4
Survey

To be able to map to what extent people care and are aware of their Facebook settings, regarding privacy, security and interdependent privacy, we designed and distributed a survey. The survey addressed the different settings available on Facebook, and awareness regarding Facebook applications and knowledge about interdependent privacy. For the design of the survey, we utilized SurveyMonkey which provides web-based survey solutions (see section 2.6). We distributed the survey on two platforms, namely Amazon Mechanical Turk (AMT) and Facebook. Amazon Mechanical Turk is a Internet marketplace where human intelligence is utilized to perform various tasks [27]. For more information about Amazon Mechanical Turk, see section 2.5. To reach out to a even larger audience, we posted the survey-link on our Facebook pages. In this chapter we will describe how we designed the survey, how it is structured and how we distributed our survey. We will examine the results with focus on interdependent privacy.

4.1 Constructing the Survey

There is not much research on the area of interdependent privacy. To be able to bring forward information and contribute to new research, we created a survey. When making the questions, we wanted to create an image of peoples use of Facebook, how they set their settings and how they know and care about their privacy and to what extent their privacy is dependent on other users. We quickly chose to use AMT as a platform for distributing the survey, because we wanted to create an image of the average Facebook user as well as getting a high diversity among the respondents (different countries, age, education etc.). Previous research shows positive results with the use of AMT [11, 29].

We started implementing the survey inside the survey template provided by AMT. After some consideration, we found that AMT did fulfil our requirements for design, so we chose to implement the survey using SurveyMonkey instead. When creating the survey, we thought that it would be better to include some extra questions, than to leave some behind. When the survey first got distributed, we were not longer able to edit the questions. We therefore

chose to include questions not only regarding privacy and interdependent privacy, but also other aspects of Facebook usage. For example some questions about security settings, usage, personal experience in regard to photos and comment sharing.

4.1.1 Design

AMT offers a template for creating surveys. This template uses HTML. It is simple, but requires more work from the requester. We found the template to be little user friendly, and it did not give you many design options. Our survey consist of many questions, and some of them had follow-up questions requiring text answers. It was then desirable to have these on two different pages. We did not want the respondents to have their answers affected by the next question. It requires more of the respondent to write a text answer, so to avoid them answering based on the next question we separated the questions onto different pages. For example, we have one question asking whether or not the use of Facebook has lead to any uncomfortable situations. If the user answers "Yes", a follow-up question asking to describe the situation that occurred will appear. If the user answers "No" the follow-up question will be skipped. If the user had seen the follow-up question, he/she may not be bothered to answer yes even though this may have been the truthful answer. We did not find an easy solution to implement this design feature in AMT, so we looked for other options. Even though AMT provides their own "Survey"-template, they also provide a "Survey Link"-template. This means that you can create the survey somewhere else, and just link to it in AMT. We chose the latter, and used SurveyMonkey to create the survey. SurveyMonkey provided us with the tools and features necessary to design our survey as desired.

Features we used in SurveyMonkey. SurveyMonkey offers several features, and has a intuitive user interface. It was easy to implement the questions, and separate them on different pages which was of high value to us. SurveyMonkey offers the ability to customize the appearance (color/theme, layout, etc.) of the survey to a higher extent than AMT. We put in a picture of the university logo, to emphasize the seriousness of the survey, as shown in Figure 4.1. SurveyMonkey also offers many different question types (multiple choice, text box, matrix and drop-down menus, etc.), and restrictions on the questions. It was important to have some restrictions especially on the text boxes. Some of the restrictions that we used was to limit the amount of characters in the text boxes, to avoid too long answers. We also made almost all questions mandatory, meaning that the respondents had to answer them before being able to move to the next question. As mentioned we divided the questions onto several different pages. This gives the respondents the impression that the survey is shorter. Each page has a title on top, grouping the different areas the questions consider. A progress bar was added to show in percent how far into the survey the respondent was at any time. This gives a good overview, and the user get a feeling of how much is left. We chose to use these features to avoid overwhelming the respondents with too many questions at a time.

SurveyMonkey offers a great user interface also when it comes to reviewing the answers. It is possible to see graphs showing the distribution of answers to all of the questions, as well as individual answers. SurveyMonkey also offers a filter and comparing feature, which made the analysis a lot easier, especially when having a large number of respondents.

4.1.2 How the Survey is Structured

The first page seen when taking the survey, is a introduction page that shortly explains what the survey is about, and it's purpose. This page emphasizes the seriousness of the survey. When people see that it is a research survey carried out by master students at an university, we believe people will answer in a serious manner. The front page also includes the requirement for taking the survey, and a short explanation on where to find answers requested in some of the questions. This is shown in Figure 4.1. As mentioned before, we have divided the questions into different areas, and we will now go through each area and emphasize and elaborate the questions we consider as most relevant and important.

Figure 4.1: Front page of the survey. This figure shows the first page of our survey. It gives a short explanation about the purpose of the survey, and what it concerns. It also give some helping guidelines to where to find answers to some of the questions, and the requirement for taking the survey (that you need to be logged in to your main Facebook account).

Facebook usage

Following the first page, is one page about Facebook usage. This page includes questions about sign-up year, how often they check their Facebook page and number of friends.

Facebook privacy: settings

This is a part of the survey where the users need to be logged in to their main account on Facebook to check how their privacy settings look. The questions are taken directly from the "Privacy"-settings and "Timeline and tagging"-settings on Facebook. We divided these questions onto 4 different pages. Before we started asking about specific settings, we asked the users how often they have checked their Facebook privacy settings during the last year. One of the following pages ask for the privacy settings, and another for the timeline and tagging settings. These questions are straightforward for the user, since all they have to do is to render the settings they have set themselves. This will easily show us how many that actually have checked their settings, and to what extent they have made them more, or less, private than default. At the end we asked the users whether or not they consider changing their settings after having reviewed them. This can make for some interesting observations, and can also give an impression of whether or not the users care or are aware of the settings.

Facebook privacy: personal experience

This group of questions focus on the users personal experience with concern to both privacy and interdependent privacy. We ask whether or not the respondents have experienced that their use of Facebook has affected their professional life or led to any uncomfortable situations. Both of these questions have a follow-up question where the users are asked to describe the situation that occurred. You will only be sent to the page with the follow-up question if you answered yes. If you answered no, the page with the follow-up question will be skipped.

A big part of Facebook consists of sharing photos and comments with others, we therefore asked the respondents to indicate on a scale from 1 to 5 how much they care about what is published about themselves, and what they publish about others, see Figure 4.2. It was mandatory for the users to give an answer on the scale. We added a text box for the users to elaborate if desired, but this was not mandatory. We received a total of 250 responses on our survey, and 190 of them chose to elaborate.

Facebook privacy: apps

This is the part of the survey that concerns interdependent privacy (see section 2.4), and also the most important part of our suvey. As mentioned before this is a relatively unknown term, so we wanted to find out whether or not the respondents knew the meaning of interdependent privacy. Since the app platform on Facebook to a high extent relies on information about a user's friends, it is in this area interdependent privacy becomes more important to address. When you install an app on Facebook, it asks for your basic information, and often more information about you and your friends. For more detailed information about the app-platform, see subsection 3.3.2. Question 26, 27, 28 and 29 (see Figure 4.3 and Figure 4.4) asks about the users awareness regarding what kind of information the apps can retrieve. There exists settings directed towards apps on Facebook (see Figure 3.5). In question 30

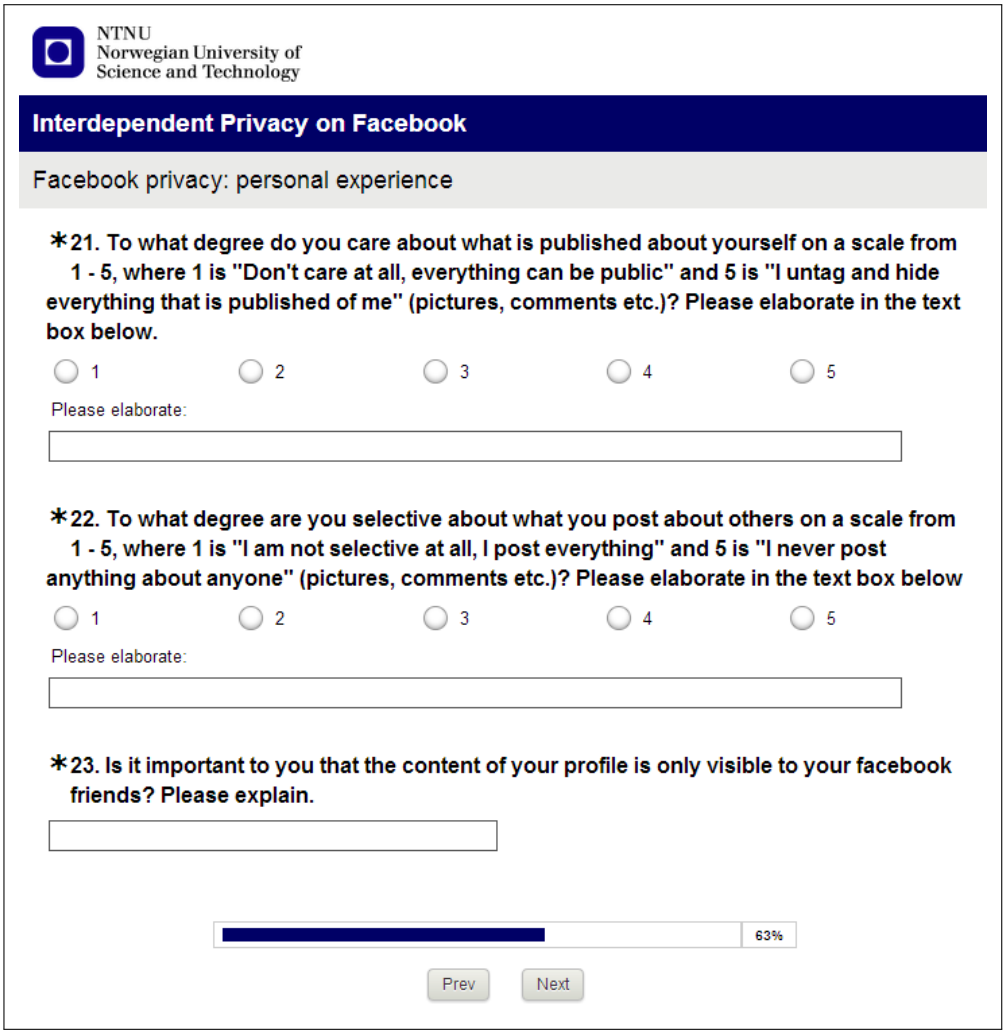

Figure 4.2: Question 21 and 22 in the survey. This figure shows question 21 and 22 in the survey. The questions concerns to what degree (on a scale from 1 to 5) the respondents care about what is published about themselves, and what they publish about others. After each of the two questions it is a text box where the respondents can elaborate.

(Figure 4.4) we ask the user to look at one of the app settings, "Apps others use". In this setting the user decides which information they make available to apps others use, in other words control the categories of information that people can bring with them when they use apps. We want to know if the user are aware of the existence of this setting. We did not ask for more specifics about what information they share, because this is not relevant. What is

relevant is whether or not they know it exists, and are aware of what kind of information they share. We finish this part of the survey with the same question we started it with, if they know the meaning of interdependent privacy. We wanted to ask again to see if they got a higher understanding of the term after answering questions about apps, and saw how it is all interconnected.

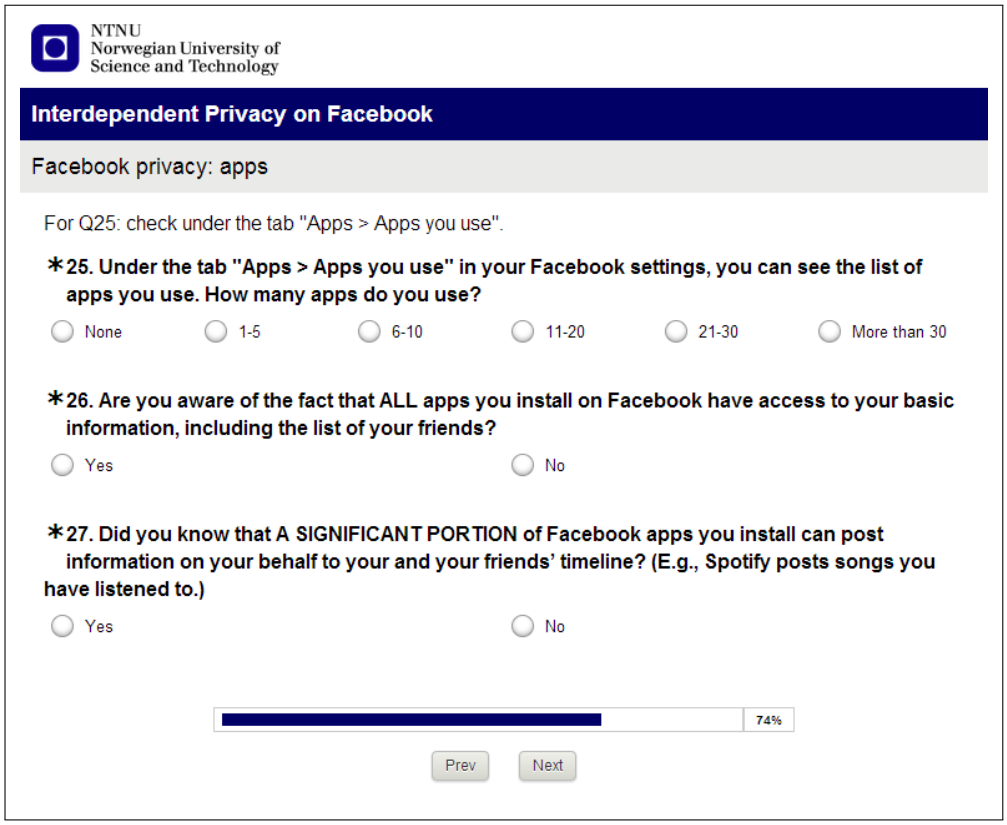

Figure 4.3: Question 25, 26 and 27 in the survey. This figure show question 25, 26 and 27 in our survey. Question 25 concern the number of apps the respondents use. Question 26 and 27 concerns the user's awareness connected to apps on Facebook.

Facebook security: settings

The main focus in this report is on privacy, not security. At the same time, we wanted to ask a few questions regarding Facebook security settings as well. The reason for this is because we wanted to see if there was a connection between strict security settings and strict privacy settings among the respondents of our survey. The questions concerns whether or not the respondents use secure browsing and login notification.

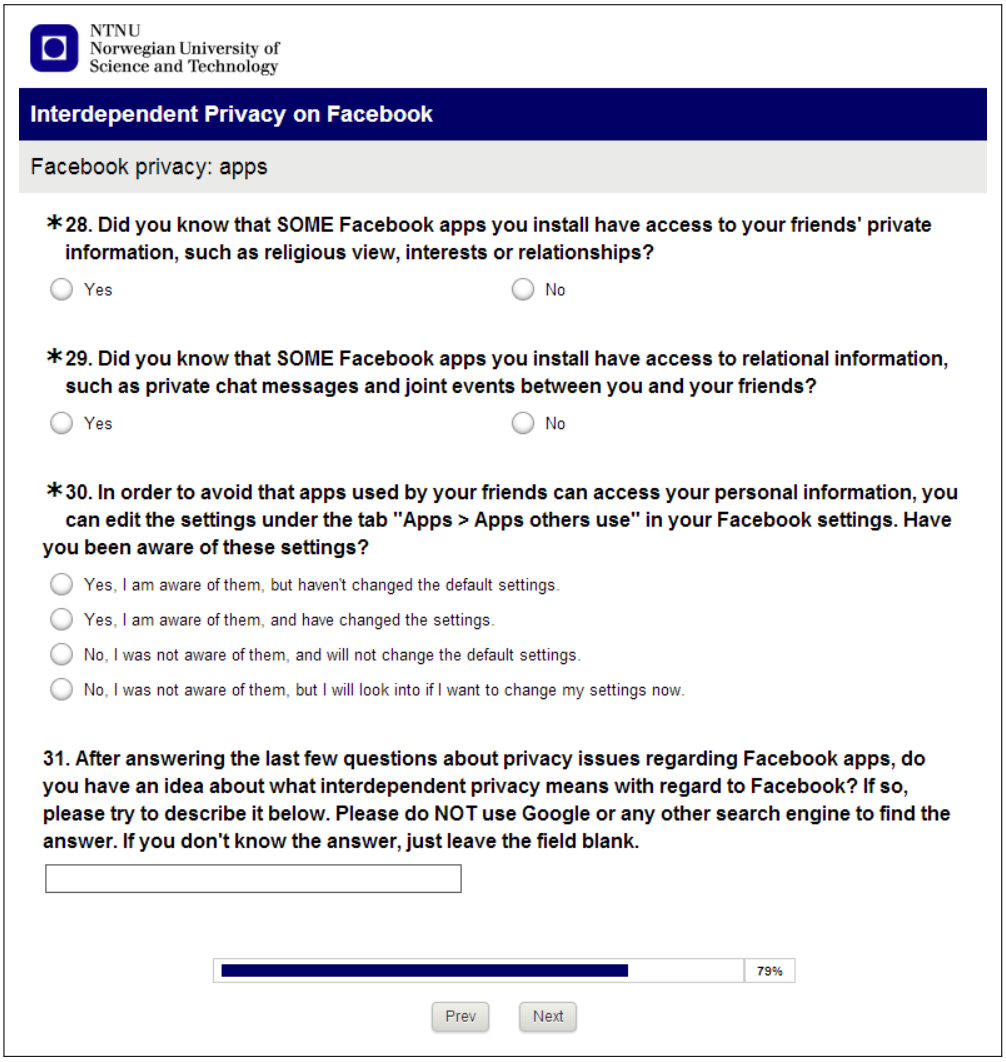

Figure 4.4: Question 28, 29, 30 and 31 in the survey. This figure show question 28, 29, 30 and 31 in our survey. Question 28, 29 and 30 concerns the user's awareness connected to apps on Facebook. Question 31 asks the respondents whether or not they know what the term interdependent privacy means after answering questions about apps.

Demographics

In the last part of our survey, we have asked for demographic information about the respondents, to get a hunch of what kind of people have taken the survey. We chose to put the demographics part at the end, rather than in the beginning. We assume that a respondents

attention span gets lower during the survey, we therefore wanted to put the "easy" questions at the end since they require less focus. These questions consists of: gender, age, country, family situation, highest qualification/degree, employment status and income. Although these questions are easy to answer, they are very important to include. When analysing, they are necessary in order to be able to draw comparisons between for example age and/or gender. An interesting factor is to see where the respondents using AMT come from.

4.1.3 Distributing the Survey

First we created a requester account on AMT. We did this using an already existing Amazon account. While creating the project (our project contained only one HIT) we filled out the properties shown in Figure 4.5. First we had to give a short title and description to describe our HIT to the workers. This is the information that is shown to the workers before they choose to either accept the HIT or skip the HIT. We also had to decide a reward for the workers. We had limited time, and wanted our HIT to be as attractive as possible, and therefore chose to have a higher reward than average. We sat the reward to be $1.5 per completed assignment. We estimated that it would take approximately 15 minutes to take the survey, this would give a hourly wage of $6. We were also asked to set a maximum number of assignments per HIT, this means number of unique answers. We sat this number to 250. We felt that 250 responses would give us a very good foundation to base our analysis on. AMT defines a feature that let the requester review the answers, and then choose to either approve or discard them. When discarding an answer, they worker will not get paid. If we did not manually approve the answers, they would automatically be approved after 3 days. We made the HIT available for only 21 days. To get a high quality on the responses, we were advised to use "Master Workers". This is users that have a good reputation from previous work done on AMT. See section 1.3 for more information about "Master Workers".

Next we filled in the "Survey-Link"-template provided by AMT, and the result of this is shown in Figure 4.6. It contains a title and a short description. In the description we linked to the homepage of the Norwegian University of Science and Technology, to emphasize the seriousness of the survey. In addition it contained the link to the survey on SurveyMonkey, as well as a field for the users to enter a survey code. This code was provided to them after they completed the survey. This was an assurance for us, so we only paid the people who actually took the survey. To avoid workers cheating with the code (for example getting the code from a fellow AMT-worker), we changed it several times during it's lifetime.

After editing the project as described above, the HIT was ready to be published. The published HIT is shown in Figure 4.7. After filtering on HITs requiring Master qualification, our HIT is shown at the top. Once our HIT was out, all we could do was to monitor it (approve or discard answers), and wait for people to respond.

We mainly wanted to distribute our survey on AMT, both to try it out as a research tool and because of it's high diversity. But in addition to distributing the survey on AMT, we

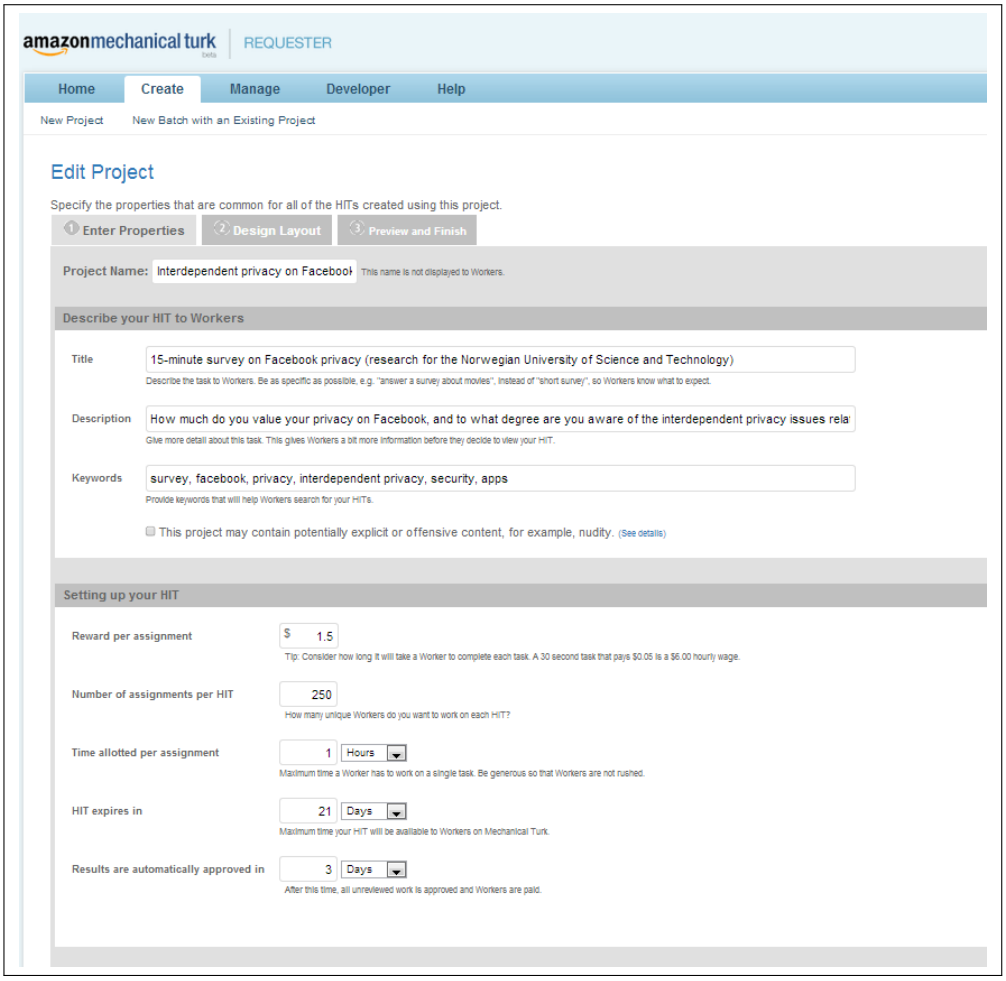

Figure 4.5: Creating an AMT project. This figure shows the layout for creating a new project in AMT. Here we stated the title, description, keywords, as well as defining the reward, number of unique workers and expiration date on the HIT.

decided to also share it with our friends on Facebook. We wanted to reach out to a even wider audience, as well as making our Facebook friends aware of their settings. Most of our Facebook friends mainly consist of fellow students, with a high technical knowledge. We were not depending on Facebook to give us many answers. We were hoping for at least 30 respondents from Facebook, but we got 77 respondents and were amazed of the outcome. We posted it and a few times during the 3 weeks the survey was out, we commented on it so it would appear on top of our friends' News Feeds. Three of our friends even chose to share it on their Facebook. This was probably one of the reasons we got so many answers. We

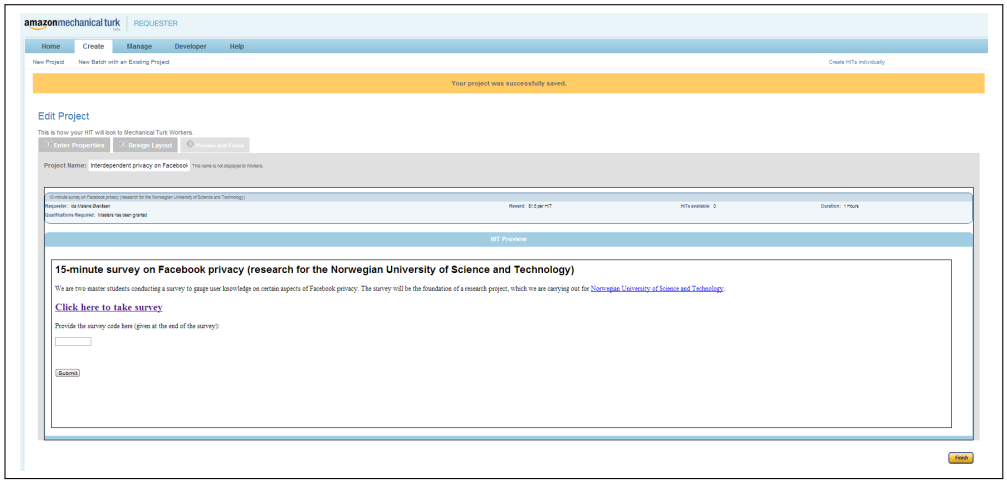

Figure 4.6: The design and layout of the survey on AMT. This figure shows the design and layout for the HIT. This is how it looks like for the workers.

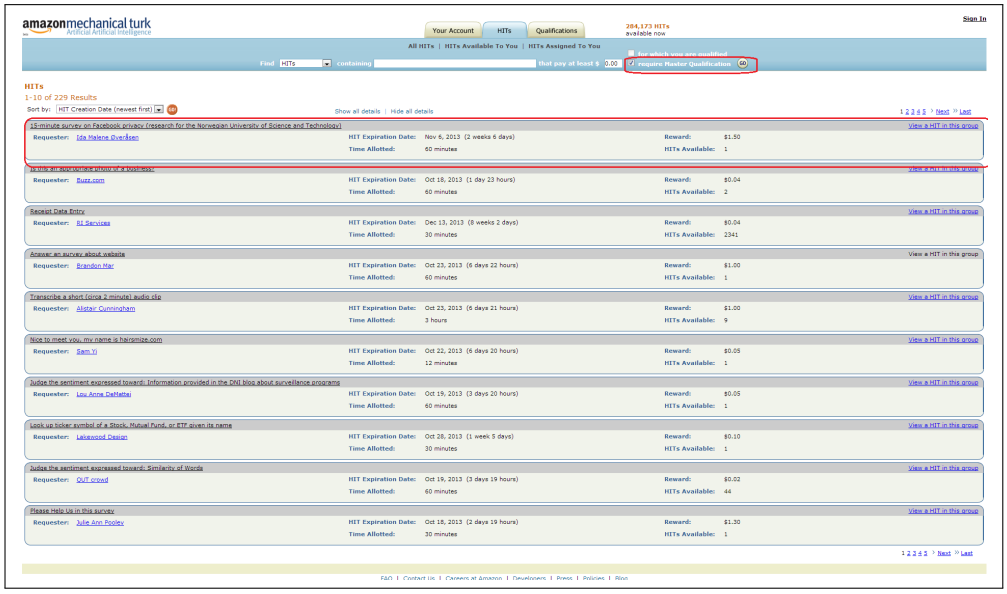

Figure 4.7: Our HIT is published. This figure shows our HIT in the list of all HITs available that requires "Master Workers".

posted it on Facebook a few days later than the HIT was published on AMT.

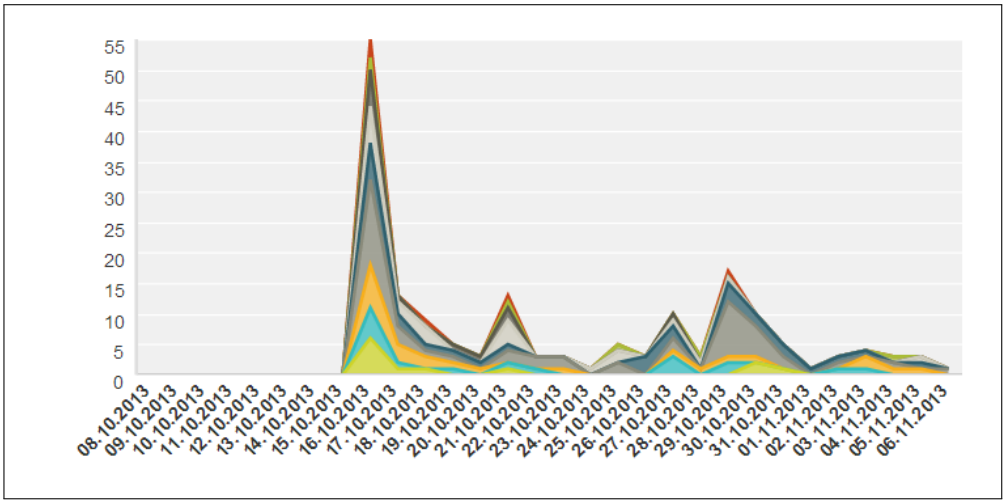

Figure 4.8: Daily distribution of number of answers from AMT.

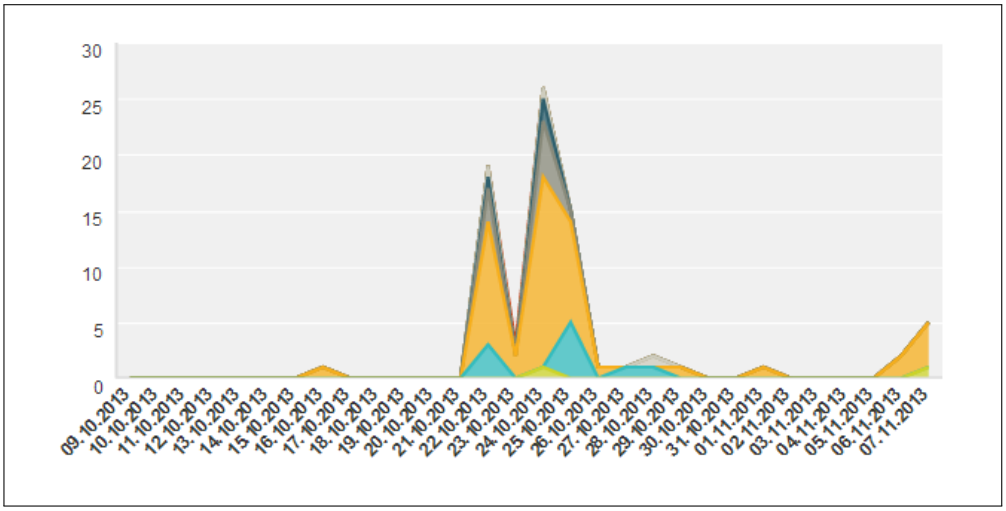

Figure 4.9: Daily distribution of number of answers from Facebook.

Figure 4.8 and Figure 4.9 shows the daily distribution of number of answers, respectively from AMT and Facebook. You can see from Figure 4.8 that we had the highest peak in responses the day it was published on AMT. The first day we had 55 unique answers, and the second day it dropped to 13 answers. The number of responses varied during the rest of the period, as the figure shows.

4.1.4 Feedback on the Survey

We got a lot of positive feedback on our survey from Facebook friends. Many have liked it, and many have commented on it. The comments focused mainly on the eye opening aspects of the survey and that it was informative. Some said the survey made them have a clean-up of their settings. Some mentioned that they though they had good control over their settings, but after taking the survey they realized that this was not the case. They became aware of something they did not know. Overall, the feedback was very positive. As mentioned above, 3 of our Facebook friends chose to share the survey further, and this suggests that they were pleased with it and thought it was good and informative.

Our survey has also been mentioned in forums on for example mturkform.com and mturkgrind.com. Most of the comments regarding our survey on these forums are about the time consumed taking the survey. The comments we got from mturkforum was: *"Time 5 min 35 sec - slow b/c I wanted to learn more about FB privacy..."* and *"Took 8 minutes, light writing but very simple."* The comments from mturkgrind was: *"About 5 minutes"* and *"Took 8 minutes, very simple and probably could do it in less time. Light writing"*

4.2 Survey Results

4.2.1 Demographics

As mentioned before, we distributed our survey on two platforms; Amazon Mechanical Turk (AMT) and Facebook. As you can see in Figure 4.10, the distribution of countries was mainly divided between two, the United States of America and Norway. Other countries were also represented; Canada, France, Germany, India, Indonesia, Ireland, Jamaica, Romania, Russia, Serbia and United Kingdom. 77 of the 250 responses were collected through the Facebook link, and out of these 77 people 96% (74 people) were from Norway. 173 of the 250 respondents took the survey via Amazon Mechanical Turk, and out of these people 85,5% (148 people) were from the United Stated of America.

The majority of the total respondents were female. They accounted for 56,80% of the responses, which is 142 responses. This means that 43,20% of the total respondents were male, with a 108 responses. We saw a difference in the gender distribution from the Facebook link and from AMT. On AMT 38,15% were men, and 56,80% were female. On Facebook 54,55% were male, and 45,55% were female. In other word the majority of respondents on AMT were females, in contrary to Facebook, were the majority of respondents were men. The different gender distributions are shown in the Figure 4.11.

Among the participants, the age ranged betweetn 19 and 76. The average age was 31. The average age of the AMT participants (33 years old) were higher than the average age of the Facebook participants (27 years old). When we looked at the total income of the

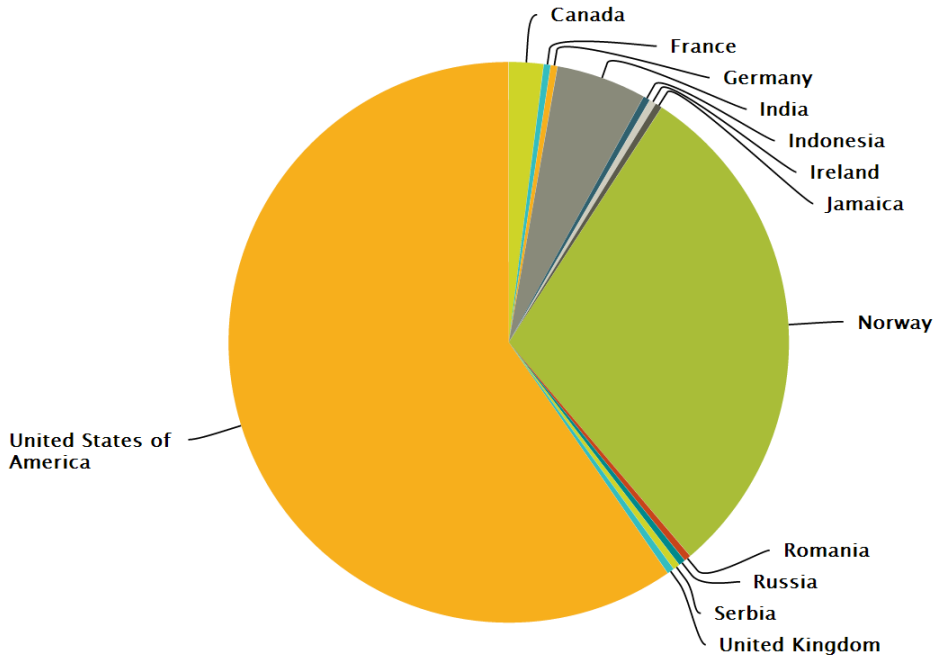

Figure 4.10: Distribution of the participant's country of origin. This graph shows the distribution of the participant's country of origin. Most of the participants are from the United Stated of America and Norway.

household per year and employment status, we found a wide range of variety among the participants. We had several participants in each group of income. Although the majority of the participants were employed for wages or students, all of the other employment status' was represented. This was consistent with former studies of AMT users [29].

4.2.2 Frequency in Checking Facebook Privacy Settings

Never Checked Facebook Privacy Settings During the Last Year

30 of the people who answered our survey stated that they have never checked their privacy settings during the last year. Even though they have not checked their privacy settings during the last year, most of them have done some changes to their settings before the previous year. The reason for this assumption is that their settings differ from the default settings. The average number of friends for the people who have never checked Facebook privacy settings during the last year is 162, and their average age is 39.

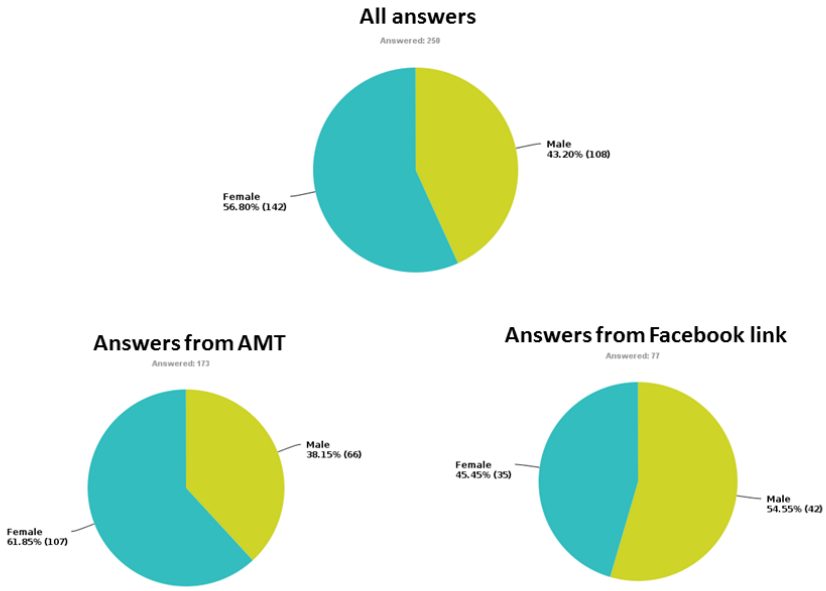

Figure 4.11: Gender distribution. This graph shows the overall gender distribution (on the top), gender distribution from AMT (to the left) and the gender distribution from the Facebook link (to the right).

In Figure 4.12 you can see a percentage distribution over Facebook settings among the people who have never checked their Facebook privacy settings during the last year. We have divided them into tree categories; "Default", "More secure", and "Less secure". You end up under the category "Default" if your setting is similar to the default setting anno 2013. See section 3.2.2 for more detailed description of the default settings on Facebook. You end up under the "More secure" category if you have changed the default setting to a more secure setting. The "Less secure" is for those who have made changes to their setting which is less secure than the default setting.

The majority of these users are active users, since 67% of them checks their Facebook page at least once a day.

60% of the people who had never checked their Facebook privacy settings during the last year *did not* consider changing their privacy settings after reviewing them. 40% of them wanted to make their privacy settings more private.

Never checked Facebook settings during the last year (30 of 250 people)			
	Default	More private/secure	Less private/secure
Q5. Who can see your future posts?	36,67 %	63,33 %	
Q6. Who can look you up using the email address or phone number provided?	76,67 %	23,33 %	
Q7. Do you want other search engines to link to your timeline?	73,33 %	26,67 %	
Q8. Who can post to your timeline?	96,67 %	3,33 %	
Q9. Review posts friends tag you in before they appear on your timeline.	76,67 %	23,33 %	
Q10. Who can see posts you've been tagged in on your timeline?	33,33 %	60,00 %	6,67 %
Q11. Who can see what others post on your timeline?	40,00 %	56,66 %	3,33 %
Q12. Review tags people add to your own posts before the tags appear on Facebook	86,67 %	13,33 %	
Q13. When you're tagged in a post, who do you want to add to the audience if they aren't already in it?	96,67 %	3,33 %	
Q33. Are you using secure browsing when using Facebook?	86,67 %		13,33 %
Q34. Are you using login notification?	63,33 %	36,67 %	

Figure 4.12: Never checked Facebook privacy settings during the last year. Forklare hva figuren viser.

We have a quote from a 67 year old woman that took our survey (with Ph.D and only 5 Facebook friends) that emphasised many user's unawareness when it comes to different Facebook settings: "Now you have scared me. I am alone and afraid".

Checks Facebook Privacy Settings "Once a month" or "Once a week or more"

48 of the people who answered our survey stated that they check their privacy settings "Once a month" or "Once a week or more". The average number of friends for these people is 416, and their average age is 28,5.

In Figure 4.13 you can see a percentage distribution of what kind of settings the people who check their privacy settings "Once a month" or "Once a week or more" have. We have divided them into the same categories as above; "Default", "More secure", and "Less secure".

85% of the people who checked their Facebook privacy settings "Once a month" or "Once a week or more" during the last year, has checked their Facebook page at least once a day during the last month. This indicates that the majority of those who check their settings frequently are also very active Facebook users.

70,83% of these people did not consider changing privacy settings after reviewing them. 27,08 % wanted to make their privacy settings more private, and 2,08% considered changing them to more public.

Checks Facebook settings "Once a month" or "Once a week or more" (48 of 250 people)			
	Default	More private/secure	Less private/secure
Q5. Who can see your future posts?	8,33 %	91,67 %	
Q6. Who can look you up using the email address or phone number provided?	31,25 %	68,75 %	
Q7. Do you want other search engines to link to your timeline?	18,75 %	81,25 %	
Q8. Who can post to your timeline?	81,25 %	18,75 %	
Q9. Review posts friends tag you in before they appear on your timeline.	33,33 %	66,67 %	
Q10. Who can see posts you've been tagged in on your timeline?	12,50 %	81,25 %	6,25 %
Q11. Who can see what others post on your timeline?	12,50 %	81,25 %	6,25 %
Q12. Review tags people add to your own posts before the tags appear on Facebook	43,75 %	56,25 %	
Q13. When you're tagged in a post, who do you want to add to the audience if they aren't already in it?	54,17 %	45,84 %	
Q33. Are you using secure browsing when using Facebook?	85,42 %		14,58 %
Q34. Are you using login notification?	33,33 %	66,67 %	

Figure 4.13: Checks Facebook privacy settings "Once a month" or "Once a week or more". Forklare figuren mer nøye her

Comparing the ones who have "Never checked their Facebook privacy settings during the last year" and the ones who checks "Once a month" or "Once a week or more"

Activity level. The majority of both groups checks their Facebook page at least once a day. The percentage is a little bit higher for the people who have checked their privacy settings "Once a month" or "Once a week or more" during the last year. 85% of them checks their Faceook page at least once a day, in contrast to the other group (who have never checked their settings during the last year) with 67% checking their Facebook page at least once a day. This indicates that the ones who have never checked their settings during the last year does not refrain from doing this because they are inactive users. One assumption for this may be that the users are unaware of the settings. 40% of them stated that they wanted to make their settings more private after taking the survey. This backs up the assumption about unawareness.

More secure settings for those who check their settings more often? If we compare Figure 4.12 and Figure 4.13, we see a clear difference in percentage that have changed from default to a more secure option. The percentage is much higher for all settings listed for those who checks frequently. Some of the settings shows a remarkable difference between the groups. We want to accentuate the settings that concern interdependent privacy. When we look at the setting "Review posts friends tag you in before they appear on your timeline" for the ones that never checked during the last year, only 23,33% have changed to a more

secure option. For the ones that check frequently, 66,67% have changed to a more secure option. Another example is the setting "Review tags people add to you own posts before the tags appear on Facebook" where 13,33% of the ones who never have checked their settings during the last year changed to a more secure option. On the contrary, as many as 56,25% of the frequent settings-checkers have changed to a more secure option.

Considered changing settings. The percentage of those wanting to make their settings more private is higher for those who have never checked settings during the last year with 40% of the group. Only 27% of the frequent setting-checkers wanted to make their settings more private. None of the people who have never checked their settings during the last year wanted to make their settings more public, unlike the other group (those who check "Once a month" or "Once a week or more") where 2% actually considered changing them to more public. Overall the frequent settings-checkers were more pleased with their settings than the once who had never checked them during the last year. 70% of the frequent settings-checkers did not consider changing their settings after reviewing them. Although the ones who have never checked their settings during the last year have far less secure settings than the other group, 60% of them did not consider changing their settings either.

4.2.3 Comparisons with Previous Surveys

In the article "Analyzing Facebook Privacy Settings: User Expectations vs. Reality" mentioned in section 2.3, they found that modified privacy settings match the users expectations only 39% of the time. In our case this number is much higher, 65,6% stated what they did not consider changing their privacy settings after reviewing them. This is an interesting observation. The previous research was done in 2011, and a lot has changed since then with regard to privacy settings. One assumption is the ongoing attention towards online security. With the media trying to make people aware of how easy it is to access ones information on the web.

In the other article mentioned in 2.3, "Facebook privacy settings; Who cares?" they found that among the majority both genders were equally confident in changing their Facebook privacy settings. Our survey backs up this finding to some extent. The majority of both females and males have changed their settings to a more private option, but our research shows that females focus more on who can see their posts and posts they have been tagged in and who can look them up. 81% of the females have changed the settings "Who can see posts you've been tagged in on your timeline?" and "Who can see what other's post on your timeline?" to a more private option. In both of these settings, this is almost 10% more than for males. In contrary, males have a larger focus on security, with more secure options on settings like "Login notification" and "Secure browsing".

4.2.4 Users' personal experience

Out of the 250 respondents 11 answered yes on the question "Have you ever experienced that your use of Facebook has affected your professional life?". 3 of these 11 have had their professional life affected in a negative way, and 8 was affected in a positive way. 50 of the 250 respondents stated that their use of Facebook had lead to uncomfortable situations, for example concerning unpleasant messages and/or inappropriate comments or pictures. The majority of the situations concerns unwanted pictures (where they do not look good) shared beyond their preferred audience and inappropriate comments on pictures of them. Some also mention cases of stalking. Some of the comments are shown below:

- I had a friend I parted ways with harass me on facebook by threatening messages, posts to photos about me, etc. I also had sexual harassment over facebook message by an ex boyfriend, inappropriate comments and propositions I was not interested in.
- Before I changed my settings, someone posted a picture of me that I did not want to share with everyone else.
- An ex girlfriend was using Facebook to get information about me and my friends.
- I shared (public) a photo from a friends timeline which he had posted to a limited set of friends, he got mad.
- I have many younger friends on facebook (underage), and I would like to be a good role model. So sometimes there have been pictures of me consuming alcohol, and I don´t want my younger friends to see that. I now have customized my settings, so they only se my personal posts which dosen´t include alcohol/smoking etc.
- Someone commented something on a photo I was tagged in that I don't want everyone to know about me
- I girl posted a naked photo of me.
- Just pictures of me not looking my best being posted by friends who then tag me and suddenly everyone - friends of friends, etc. can see the pics. It wasn't disasterous or inappropriate, but those weren't pictures I wanted old classmates from high school to look at (unless we are friended on FB)

39,6% of the total respondents have blocked one or more person due to uncomfortable situations or harassment.

To see how much a person values their privacy, we asked them to state on a scale from 1 to 5 to what degree they care about what is published about themselves. 1 is "I don't care at all. Everything can be public" and 5 is "I untag and hide everything that is published of me".

The majority (35,6%) answered 3 on the scale. When people were asked to elaborate on this topic, the comments ranged from "I don't trust the Internet" to "I don't untag everything, because the point of the site is to be social". Many says that they frequently untag photos they do not want others to see. One of the respondents said "It's a tricky dilemma, because when you untag you also loose control over what happens with the picture/post."

From our results, it seem like people care more about what they post of others, than what is posted about themselves. When we asked them to what degree they are selective about what they post about others on a scale from 1 to 5, where 1 is "I am not selective at all, I post everything" and 5 is "I never post anything about anyone", the majority answered 4. This shows that people are very selective when it comes to posting things about others.

4.2.5 Interdependent Privacy

A big part of our survey focus on apps and the issues related to apps which concerns interdependent privacy. When installing an app on Facebook, most apps ask for permission to access additional information in addition to your basic information (name, profile picture, cover photo, gender, networks, username, user ID, your list of friends, and any information you choose to make public). We wanted to map the awareness of the respondents when it came to apps, and to what degree they knew about the information apps access. We also wanted to find out whether or not the respondents had knowledge about the term interdependent privacy. We asked the question "Do you have any idea about what interdependent privacy can mean in regard to Facebook?" both before and after the app-related questions. We specified in the question that they were not allowed to use Google or any other search engine to find the answer, and if they did not know the answer it would be preferable for us if they skipped the question. It would not be of any value for us, if they searched for the "definition". We wanted to see if people could come up with their own idea of the term. It was 136 people that skipped or answered that they did not know what it was, both before and after the app-related questions. 69 of the respondents skipped the first question, but answered the second one. Even though everything was not entirely correct, a lot of people seemed to have gotten some idea of what the term evolves around after answering the question about apps. Table 4.1 shows some of the answers, both before and after the app-related questions.

Table 4.1: Peoples thoughts of what is meant by interdependent privacy before and after answering questions about privacy issues regarding the use of Facebook apps.

Q24. Do you have any idea about what interdependent privacy means?	**Q31. Do you have any idea about what interdependet privacy means after answering questions regarding privacy issues using Facebook apps?**

I have no idea what interdependent privacy means. It almost does not make sense to put those two words together. If you have privacy, it should not depend on another party to make it private. That defetes the whole purpose of "private".	Hmn. I guess it makes sense now, seeing that apps can do that to people who are friends.
I would image it relates to one person's privacy being compromised or supported by another user's privacy settings.	Yes, I understand what it means now. If a friend of mine permits an app to access their info then they have a certain amount of access to my info.
I think it's when my picture is visible to only friends but then a friend of mine reshares it, so I have to rely on that friend to keep my stuff private too.	I think I was close to right. Relying on others' settings to keep my privacy.
I think it means that people you allow to see things can also allow others to see it if they chose to, with or without your permission but I am not sure about this.	I think that it means if you give an app permission to use your information, the app can then use the information in any way it wants to. This is why I do not use any apps because I do not trust them period.
I think it has to do with other sites and apps allowing you to sign into or register for accounts using your facebook account. You would now have another set of privacy policies to review and how the two sites work together	Apps you use can disregard your privacy settings with facebook and play by tehir own rules - so I have to be much more diligent.
I think it means that people you allow to see things can also allow others to see it if they chose to, with or without your permission but I am not sure about this.	I think that it means if you give an app permission to use your information, the app can then use the information in any way it wants to. This is why I do not use any apps because I do not trust them period.
It's something about where someone else saying something (like Bob saying "Bob is at the restaurant with Mike") can reveal information about another person (in this case, that Mike is at the restaurant).	Maybe it's: Facebook taking other people's info based on something I do.
My privacy can be affected by those I share with. Just because I make something private does not mean that my friends won't pass it along, making it no longer private.	You are not the only person in control of your privacy. If you don't use the right settings, other people can share information you think is private.

I have no control over what info my friends share about me	(Skipped)
Nope. I will for sure google it now.	That it´s obv. not only facebook who can access my privacy settings, that this so called privacy is interdependet and I am in charge of setting those settings myself if I don´t want it to be that interdependent.
What others can do to your privacy if you "let them"?	Yes. what concerns your privacy that you dont know of, that your friends do to your privacy ish.
My privacy depends on others	The apps are allowing people to see things that are private. It's interdependent on FB.
I would say it means it depends on what others would post or say about you, or give out your private things.	You can control what you share, but not what others do or say that may infringe on your privacy.
No	Getting access through games and friends.
(Skipped)	My privacy setting depends also on other users, with the help of apps. I think this is what interdependent privacy means.
(Skipped)	Maybe other apps can take information from your friends without their knowing.
(Skipped)	It seems to be privacy independent from privacy settings. It appears apps can override general privacy settings.
(Skipped)	That apps I put on my FB page can access my friend's accounts, information and activities. I am always very careful to select "ONLY ME" when they ask whose wall they can post to - but I wasn't aware that apps were independently able to access the information of my friends without my consent.
(Skipped)	I think that it means that the apps that I use can have an effect on my friends privacy.

An issue discussed in the paper "Third-Party Apps on Facebook: Privacy and the Illusion of Control" [25] is the importance of user control of apps' data access, and that it should be made clear to the user what information they give the apps permission to access. In this paper, they conclude that it is often unclear for the users what information they agree to share, and that apps often ask for permissions that are in conflict with their privacy settings. We wanted to see if the users were aware of what information apps may ask for, and how much information they may agree on sharing (not just about themselves).

In the apps settings, one can see a list of all the apps the user have connected to Facebook. Figure 4.14 show the amount of apps the respondents have. The distribution is close to even for all the alternatives. 86,8% of the total respondents have at least one app connected to their Facebook. We can see that a higher percentage of the respondents have more than 30 apps in comparison to none.

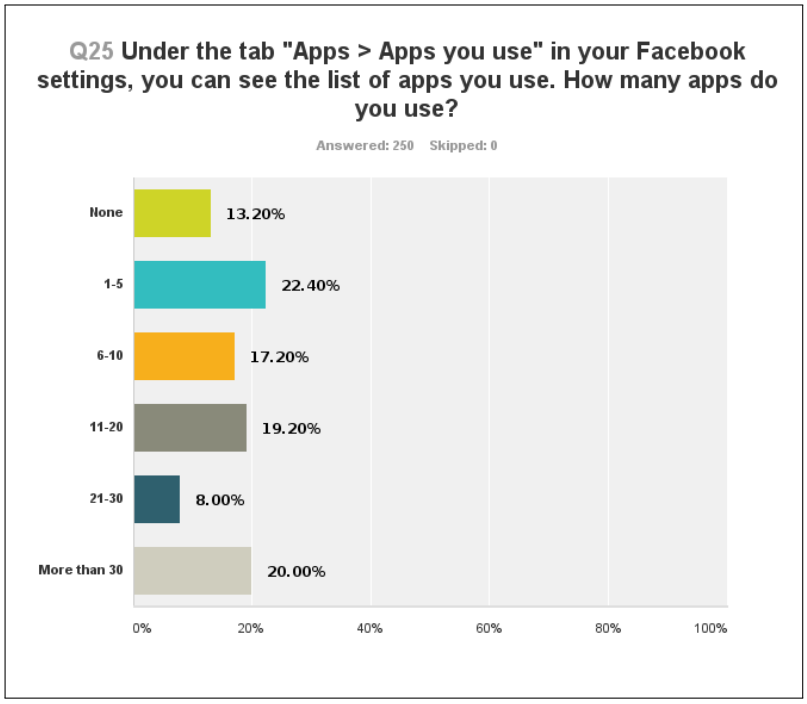

Figure 4.14: Question 25 - Displaying number of apps you use. After receiving 250 answers, this is the summary of the answers to question 25 asking for the number of apps the user use.

Figure 4.15, Figure 4.16, Figure 4.17 and Figure 4.18 shows the results from question 26, 27, 28 and 29, where we ask the respondents about their awareness regarding the information apps requests. The two first figures shows that the majority of the respondents were aware of the facts presented. The two last figures, on the other hand, shows that the majority were

unaware of the permission requests. The two first questions are more visible for the users, it is stated many times that all apps access your basic and public information, and the users experience apps posting both on their behalf and on friends' behalf (for example Spotify posting playlists or songs you have listened to). The two last questions is more hidden from the users, because nothing is posted or viewable etc. The users is not notified when the apps access this information, and therefore have no specific idea what is retrieved, when it is used, and for what purpose. We therefore think it is less knowledge about these permission requests.

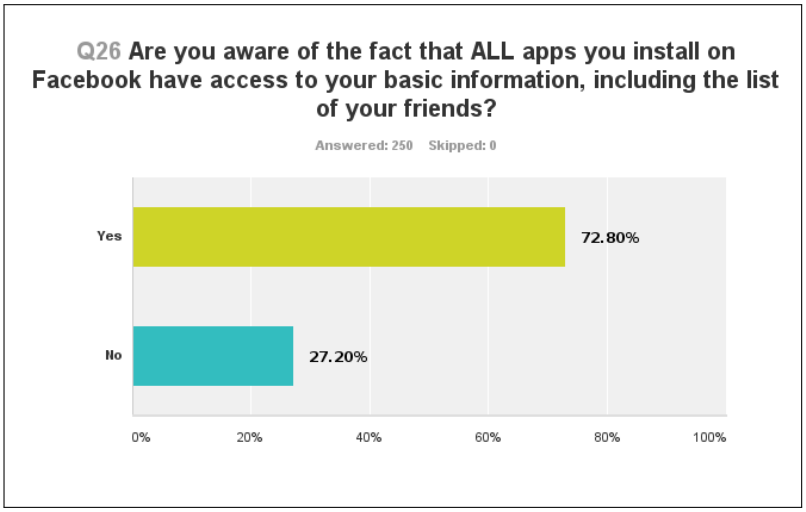

Figure 4.15: Question 26 - Displaying the awareness of the fact that all apps access your basic information. All apps you install on Facebook have access to your basic information, including the list of your friends. 72,80% of the respondents were aware of this.

We wanted to find out whether or not people using many apps had more or less knowledge when it came to the app-related questions, than people using few apps. *Our hypothesis were that the ones with many apps have less knowledge about the privacy issues related to apps*. The reason for this assumption is that we thought if these people were aware of all the permissions they agree/agreed on, they would not have had that many apps to begin with (because of the privacy breach apps cause). On the other hand, we thought that those with few apps had more knowledge about the privacy issues related to apps, and therefore chose to refrain for installing apps and/or are frequently deleting the apps not in use. Figure 4.20 shows the results of this comparison. On question 26 the distribution is close to equal for those with many apps (21 apps or more) and those with few (5 apps or less). This is a relatively common known fact, because information about this is stated on the top of the app settings, as well as always on top of the list when installing an app. Question 27 shows that the people with many apps were more aware of the fact that a significant portion of apps post on your behalf. We think the reason for this is that the people who frequently use apps have

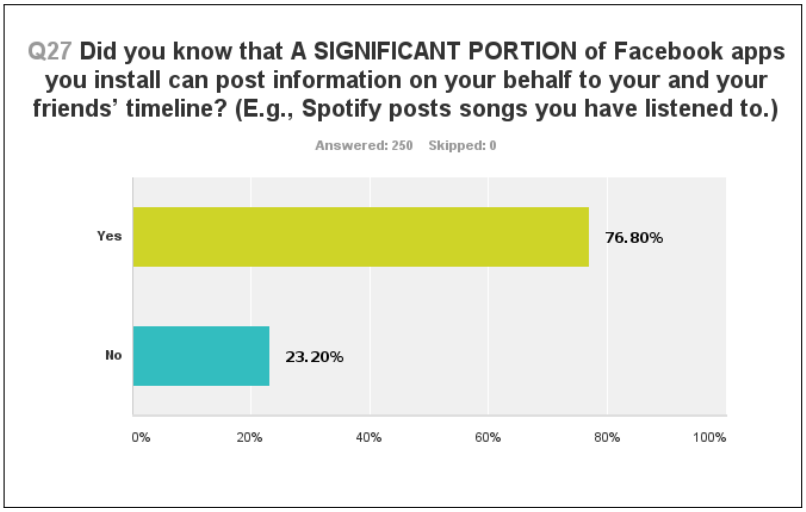

Figure 4.16: Question 27 - Displaying the awareness of the fact that a significant portion of apps post on your behalf. A significant portion of apps you use on Facebook post to your timeline and your friends' timeline on your behalf, for example Spotify posting songs you have listened to. 76,8% of the respondents were aware of this.

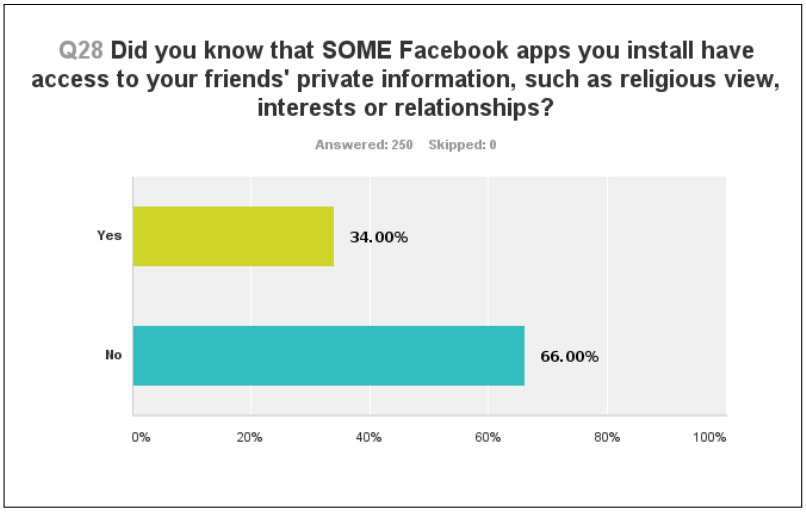

Figure 4.17: Question 28 - Displaying the awareness of the fact that some apps access your friends' private information. Some apps you use on Facebook access your friends' private information, such as religious view, interests and relationships. 34% of the respondents were aware of this.

more experience when it comes to apps posting on their behalf, and this makes them more

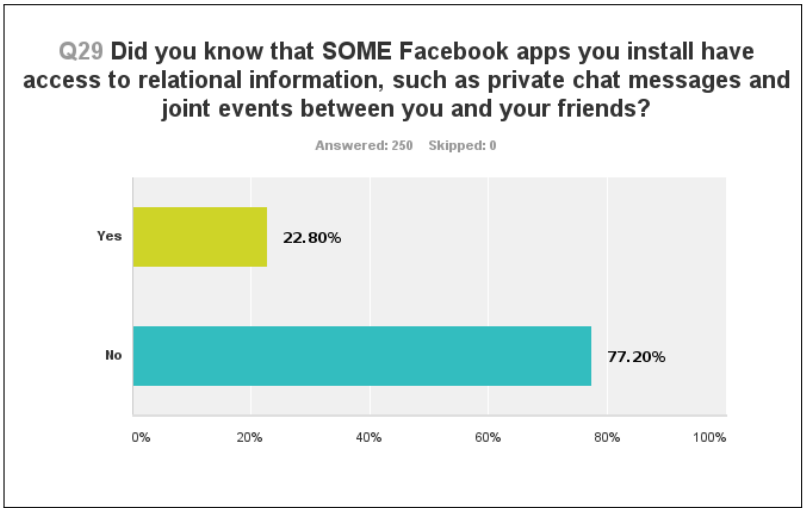

Figure 4.18: Question 29 - Displaying the awareness of the fact that some apps access relational information. Some apps you use on Facebook access relational information, such as private chat messages and joint events between you and your friends. 22,8% of the respondents were aware of this.

aware of this fact. When apps post on behalf of a user, it is shown on your timeline. This is something the user experiences hands on. In addition to this, people who use many apps sees the permission requests from Facebook more frequently. Question 28 and question 29 on the other hand, are not visible for the naked eye. Although, this is stated in the permission request, it is never visible for the user what information is accessed and retrieved by the apps. The percentage of people aware of the facts presented in question 28 and question 29 is higher for those with few apps than for those with many apps. This backs up our hypothesis. The last question (30) concerns the setting "Apps others use" found under the App tab in your Facebook settings. Here you can choose which information your friends' apps can access. From our results you see that 37,08% of those with few apps were aware of the existence of this setting. Almost 10% less of the ones with many apps were aware of it. This also backs up our hypothesis that the ones with few apps are to a larger extent aware of the privacy issues related to apps and the settings that exist.

Question 30 asks not only for a simple "Yes" or "No" answer to whether or not they are aware of the setting "Apps others use". The possible answers for the question is "Yes, I am aware of them, but I haven't changed the default settings", "Yes, I am aware of them, and have changed the settings", "No, I was not aware of them, and will not change the default settings" and "No, I was not aware of them, but will look into if I want to change my settings now". The latter option was significantly higher for those with many apps, which means a higher portion of those with many apps were unaware of this setting and dissatisfied with the

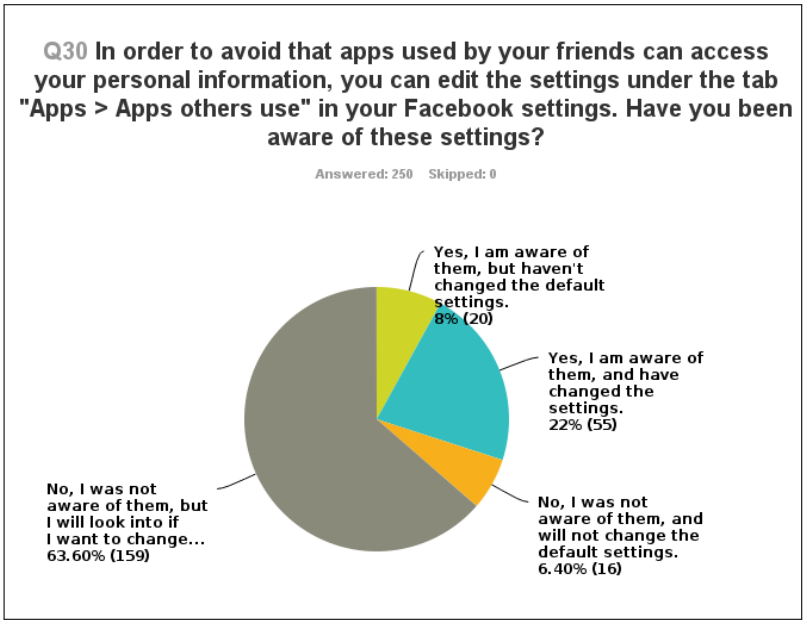

Figure 4.19: Question 30 - Displaying the awareness of the setting "Apps others use". Under the setting "Apps others use" the user can edit what information about you apps used by your friends can access. 70% of the respondents were NOT aware of this setting.

configuration of this setting, compared to the ones with few apps. Another observation is that the alternative "Yes, I was aware of them, and have changed the settings" is higher for those with few apps. These results are shown in Figure 4.21. These results also back up our hypothesis.

	Many apps		Few apps	
	Yes	No	Yes	No
Q26. Are you aware that ALL apps access basic information?	75,71 %	24,29 %	74,16 %	25,84 %
Q27. Do you know that a significant portion of apps post on your behalf?	81,43 %	18,57 %	74,16 %	25,84 %
Q28. Do you know that some apps access friends' private information?	27,14 %	72,86 %	35,96 %	64,04 %
Q29. Do you know that some apps access relational information?	17,14 %	82,86 %	29,21 %	70,79 %
Q30. Are you aware of the setting "Apps others use"?	28,57 %	71,43 %	37,08 %	62,92 %

Figure 4.20: App awareness - Comparing those with many app and those with few apps. Percentage distribution of the answers to all of the app questions differentiating the 70 people with many apps (21 apps or more) and the 89 people with few apps (5 or less).

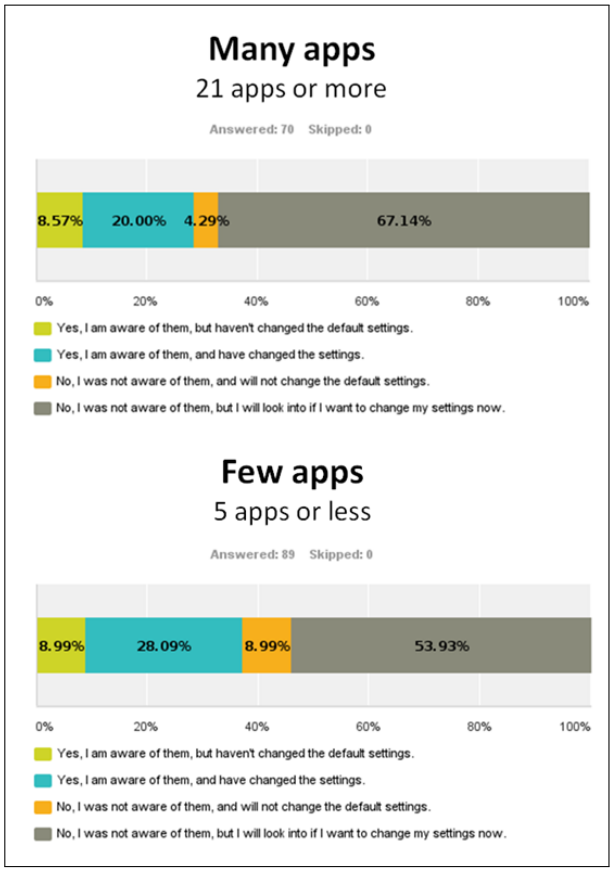

Figure 4.21: Awareness of the setting "Apps others use" - Comparing those with many app and those with few apps.

Discussion

Conclusion

References

[1] Facebook, "Facebook settings," 2013. https://www.facebook.com/settings, accessed 14.11.2013.

[2] M. McKeon, "The evolution of privacy on facebook," 2010. http://www.mattmckeon.com/facebook-privacy, accessed 26.09.2013.

[3] K. Opsahl, "Facebook's eroding privacy policy: A timeline," 2010. https://www.eff.org/deeplinks/2010/04/facebook-timeline, accessed 02.10.2013.

[4] Corvida, "Facebook answers myspace data availability with facebook connect," May 09, 2008. http://readwrite.com/2008/05/09/facebook_answers_myspace_with_facebook_connect#awesm=~onbBzdw2DxSyoW, accessed 14.11.2013.

[5] CrunchBase, "Facebook connect," 2008. http://www.crunchbase.com/product/facebook-connect, accessed 14.11.2013.

[6] A. Bhattacherjee, *Social Science Research: Principles, Methods, and Practices*, ch. Survey Research, pp. 73–82. Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License, 2012.

[7] GSMArena.com, "Social network service." http://www.gsmarena.com/glossary.php3?term=sns, accessed 15.10.2013.

[8] M. Faloutsos, T. Karagiannis, and S. Moon, "Online social networks." http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5578911&tag=1, accessed 15.10.2013.

[9] A. Acquisti, S. Gritzalis, C. Lambrinoudakis, and S. D. C. di Vimercati, eds., *Digital Privacy: Theory, Technologies, and Practices*, ch. Privacy Perceptions among Members of Online Communities, pp. 253–266. Auerbach Publications, 2008.

[10] A. Mislove, M. Marcon, K. P. Gummadi, P. Druschel, and B. Bhattacharjee, "Measurement and analysis of online social networks," 2007. Published in Proceeding IMC '07 Proceedings of the 7th ACM SIGCOMM conference on Internet measurement. Pages 29-42.

[11] Y. Liu, K. P. Gummadi, B. Krishnamurthy, and A. Mislove, "Analyzing facebook privacy settings: User expectations vs. reality," 2011.

[12] J. Cassidy, “The online life; me media,” May 2006. http://www.newyorker.com/archive/2006/05/15/060515fa_fact_cassidy, accessed 04.10.2013.

[13] S. Musli, “Winklevoss twins drop facebook lawsuit.” http://www.ivygateblog.com/2011/06/winklevoss-twins-finally-end-facebook-lawsuit-%E2%80%A6-psyche/, accessed 23.10.2013.

[14] Wikipedia, “History of facebook,” Last edited: September 2013. http://en.wikipedia.org/wiki/History_of_Facebook, accessed 02.10.201.

[15] T. Houston, “The facebook story: from inception to ipo,” 2012. Published in the Verge.

[16] IMDB, “The social network.” http://www.imdb.com/title/tt1285016/, accessed 24.10.2013.

[17] T. Houston, “Facebook to buy instagram for 1 billion.” http://www.theverge.com/2012/4/9/2936375/facebook-buys-instagram, accessed 28.10.2013.

[18] BBC News Technology, “Facebook timeline: the social network’s life story,” May 18, 2012. http://www.bbc.co.uk/news/technology-16832799, accessed 05.11.2013.

[19] The New York Times Business Day Technology, “The evolution of facebook.” http://www.nytimes.com/interactive/technology/facebook-timeline.html?_r=0#/#time189_6062, Last edited 24.07.2013, accessed 28.10.2013.

[20] Facebook, “Key facts,” September 2013. https://newsroom.fb.com/Key-Facts, accessed 14.11.2013.

[21] danah boyd and E. Hargittai, “Facebook privacy settings; who cares?,” 2010.

[22] G. Biczók and P. H. Chia, “Interdependet privaqcy: Let me share your data,” 2013.

[23] R. Clarke, “Introduction to dataveillance and information privacy, and definitions of terms,” Last edited: October 2013. http://www.rogerclarke.com/DV/Intro.html#Priv, accessed 30.10.2013.

[24] F. Gottheil, “Principles of economics.” Power Point, 2013. Chapter 14: Externalities, Market, Failure and Public Choise.

[25] N. Wang, H. Xu, and J. Grossklags, “Third-party apps on facebook: Privacy and the illusion of control,” December 2011.

[26] W. Mason and S. Suri, “Conducting behavioral research on amazon’s mechanical turk,” 2011.

[27] Amazon, “Amazon mechanical turk.” http://aws.amazon.com/mturk/, accessed 23.10.2013.

[28] Wikipedia, “The turk,” Last edited: October 2013. http://en.wikipedia.org/wiki/The_Turk, accessed 23.10.2013.

[29] W. Mason and D. J. Watts, “Financial incentives and the "performance of crowds",”

[30] J. J. Horton and L. B. Chilton, “The labor economics of paid crowdsourcing,” 2010.

[31] P. G. Ipeirotis, “Analyzing the amazon mechanical turk marketplace,” 2010.

[32] Wikipedia, “Anchoring,” Last edited: October 2013. http://en.wikipedia.org/wiki/Anchoring_effect, accessed 28.10.2013.

[33] SurveyMonkey, “Surveymonkey - about us,” 2013. https://www.surveymonkey.com/mp/aboutus/, accessed 30.10.2013.

[34] Wikipedia, “Surveymonkey,” Last edited: October 2013. http://en.wikipedia.org/wiki/SurveyMonkey, accessed 30.10.2013.

[35] SurveyMonkey, “Surveymonkey - how it works,” 2013. https://www.surveymonkey.com/mp/take-a-tour/, accessed 30.10.2013.

[36] M. Gardner, “Facebook privacy settings are changing again,” October 30, 2013. http://guardianlv.com/2013/10/facebook-privacy-settings-are-changing-again/, accessed 14.11.2013.

[37] Michael C., “The evolution of privacy on facebook,” 2011. http://www.yalelawtech.org/control-privacy-technology/evolution-of-facebook-privacy, accessed 30.09.2013.

[38] J. Kirk, “Facebook turns on secure browsing by default,” August 1, 2013. http://www.computerworld.com/s/article/9241277Facebook_turns_on_secure_browsing_by_default, accessed 12.11.2013.

[39] Facebook, “Teens now start with "friends" privacy for new accounts; adding the option to share publicly,” Octover 16, 2013. http://newsroom.fb.com/News/737/Teens-Now-Start-With-Friends-Privacy-for-New-Accounts-Adding-the-Option-to-Share-Publicly#downloads, accessed 04.11.2013.

[40] Facebook, “How news feed works.” https://www.facebook.com/help/327131014036297, accessed 15.11.2013.

[41] D. Schwartz for CBC News, “8 facebook privacy flaps,” September 25, 2012.

[42] H. MCKENZIE, “Move fast, break things: The sad story of platform, facebook’s gigantic missed opportunity,” July 23, 2013. http://pandodaily.com/2013/07/23/move-fast-break-things-the-sad-story-of-platform-facebooks-gigantic-missed-opportunity/, accessed 15.11.2013.

[43] Facebook, “Facebook newsroom - platform.” http://newsroom.fb.com/Platform, accessed 15.11.2013.

[44] Facebook Help Center - App Basics, “Facebook.” https://www.facebook.com/help/493707223977442/, accessed 14.11.2013.

[45] Facebook Developers - Login Reference, “Facebook.” https://developers.facebook.com/docs/reference/login/, accessed 14.11.2013.

[46] S. Me, “Tripadvisor.” https://apps.secure.me/a/tripadvisor, accessed 15.11.2013.

[47] Facebook, “Leading websites offer facebook beacon for social distribution.” https://newsroom.fb.com/News/234/Leading-Websites-Offer-Facebook-Beacon-for-Social-Distribution, accessed 24.10.2013.

[48] M. Dickman, “Inside//out: Facebook beacon,” Last edit December 5, 2007. http://technomarketer.typepad.com/technomarketer/2007/11/insideout-faceb.html, accessed 06.11.2013.

[49] C. Li, “Close encounter with facebook beacon,” November 21, 2007. http://forrester.typepad.com/groundswell/2007/11/close-encounter.html, accessed 14.11.2013.

[50] M. Zuckerberg, “Thoughts on beacon.” https://www.facebook.com/notes/facebook/thoughts-on-beacon/7584397130, accessed 24.10.2013.

[51] J. Brodkin, “Facebook halts beacon, gives $9.5m to settle lawsuit,” December 8, 2009. http://www.pcworld.com/article/184029/facebook_halts_beacon_gives_9_5_million_to_settle_lawsuit.html, accessed 14.11.2013.

[52] M. E. Sharon, “Who, what, when, and now... where,” August 19, 2010. https://www.facebook.com/notes/facebook/who-what-when-and-nowwhere/418175202130, accessed 14.11.2013.

[53] S. W. Lessin, “Tell your story with timeline,” September 22, 2011. https://www.facebook.com/notes/facebook/tell-your-story-with-timeline/10150289612087131, accessed 04.11.2013.

[54] Facebook, “Explore your activity log.” https://www.facebook.com/help/437430672945092, accessed 05.11.2013.

[55] Z. Zorz, “Facebook rolls out graph search for english speaking users,” October 08, 2013. http://www.net-security.org/secworld.php?id=15377, accessed 14.11.2013.

[56] Facebook, “Graph search now fully launched in us english,” August 07, 2013. http://newsroom.fb.com/News/684/Graph-Search-Now-Fully-Launched-in-US-English, accessed 14.11.2013.

[57] T. Craver, “Facebook introduces graph search,” January 15, 2013. http://searchenginewatch.com/article/2236618/Facebook-Introduces-Graph-Search, accessed 14.11.2013.

[58] Facebook, “3 tips about search privacy,” 2013. https://www.facebook.com/about/graphsearch/privacy, accessed 14.11.2013.

[59] Z. Miners, “Facebook launches graph search, acknowledges privacy concerns,” August 7, 2013. http://www.computerworld.com/s/article/9241453/Facebook_launches_Graph_Search_acknowledges_privacy_concerns, accessed 14.11.2013.

[60] G. Wallace, “Facebook kills search privacy setting,” October 11, 2013. http://money.cnn.com/2013/10/11/technology/social/facebook-search-privacy/index.html?iid=EL, accessed 30.10.2013.

[61] J. Topolsky, “Mark zuckerberg’s letter to investors on facebook’s ’social mission’.” http://www.theverge.com/2012/2/1/2764840/mark-zuckerbergs-letter-to-investors-on-facebooks-social-mission/in/2528910, accessed 28.10.2013.