SOCIAL MEDIA ADDICTION -
THE PARADOX OF VISIBILITY &
VULNERABILITY

Master’s (one year) thesis in Informatics (15 credits)
Ewelina Paula Kempa

Spring 2015:MAGI01
Title: Social media addiction - The paradox of visibility & vulnerability

Year: 2015

Author: Ewelina Paula Kempa

Supervisor: Rikard Lindgren

Abstract: We currently post a large amount of personal information about ourselves on social media sites. Many times though, users of these services are poorly aware of what kind of terms and conditions they agree to. There are in fact many techniques available that ensure users privacy, yet not many organizations make the effort to have those in place. Making a profit is what matters for companies and information on users is highly valued. It is the lack of regulations regarding data collection that enable organizations not to consider their users privacy. The data that can be collected is vast, it is important to understand that everything we do online, every search, click, shop and view is stored and the information is many times sold along to third-parties. Using information on users, companies can make profit by for example making predictions on the users, figuring out what they are interested in buying. It is nevertheless very difficult to make long-lasting regulations as the web constantly changes and grows. A qualitative research was conducted to observe to what extent social media addiction and its consequences is being discussed and researched. Interviews with social media users were also conducted. After an analysis on the findings it is clear that many users in fact would like to have more privacy online yet they feel the need to accept the term and conditions any way. Many users also state that they happily would like to read the terms and conditions, had they been written in a different way.

Keywords: Online privacy, Internet addiction, Big Data, Regulations, Social media
# Table of Contents

1 INTRODUCTION ......................................................................................................................... 1
  1.1 BACKGROUND ........................................................................................................... 1
  1.2 RELATED RESEARCH .............................................................................................. 3
  1.3 RESEARCH QUESTION .......................................................................................... 5
  1.4 PURPOSE OF THE RESEARCH ............................................................................ 5
  1.5 TARGET GROUP ...................................................................................................... 5

2 METHOD ........................................................................................................................................... 6
  2.1 DEDUCTION ............................................................................................................. 6
  2.2 QUALITATIVE RESEARCH ...................................................................................... 6
  2.3 INTERVIEWS – PROCEDURE ............................................................................... 6
  2.4 OBSERVATIONS – PROCEDURE ............................................................................ 7
  2.5 SAMPLING ............................................................................................................... 7
  2.6 DATA COLLECTION ................................................................................................ 7
  2.7 CRITERIA FOR THEORETICAL STUDY ................................................................. 8
  2.8 QUALITATIVE ANALYSIS METHOD ..................................................................... 8
  2.9 POSITIVISM ............................................................................................................ 8
  2.10 VALIDITY ................................................................................................................ 8

3 THEORETICAL STUDY ...................................................................................................................... 9
  3.1 PARADOXES ............................................................................................................. 9
  3.2 BIG DATA .................................................................................................................. 11
  3.3 WEB MINING ........................................................................................................... 13
  3.4 REGULATIONS .......................................................................................................... 14
  3.5 INTERNET ADDICTION .......................................................................................... 17
  3.6 ONLINE PRIVACY .................................................................................................. 19

4 HYPOTHESES .................................................................................................................................. 21

5 EMPIRICAL STUDY .......................................................................................................................... 23
  5.1 OBSERVATIONS – POPULAR MEDIA ........................................................................ 23
     5.1.1 Internet addiction .............................................................................................. 23
     5.1.2 Privacy aspects ................................................................................................. 25
     5.1.3 Social Media ..................................................................................................... 29
     5.1.4 Terms and Conditions .................................................................................... 30
     5.1.5 Example ............................................................................................................ 31
  5.2 INTERVIEWS ............................................................................................................... 34
  5.3 QUESTIONS ............................................................................................................... 34
  5.4 POSITIVE OUTCOMES ............................................................................................ 34
  5.5 NEGATIVE OUTCOMES ............................................................................................ 35

6 ANALYSIS ......................................................................................................................................... 36
  6.1 DOES THE USE OF SOCIAL MEDIA HAVE A NEGATIVE IMPACT ON INDIVIDUALS’ DESIRE FOR ONLINE PRIVACY? ................................................. 36
  6.2 WHAT HAZARDS DOES THE LACK OF REGULATIONS ON BIG DATA HAVE ON ONLINE PRIVACY? .......................................................... 40

7 DISCUSSION ..................................................................................................................................... 42
  7.1 SOCIAL MEDIA ADDICTION ..................................................................................... 42
  7.2 TERMS AND CONDITIONS ..................................................................................... 45
  7.3 BIG DATA REGULATIONS ....................................................................................... 47

8 CONCLUSION .................................................................................................................................... 50
  8.1 CONCLUSION ............................................................................................................. 50
  8.2 RESEARCH CONTRIBUTION ..................................................................................... 51
8.3 METHOD EVALUATION .......................................................................................................................... 51
8.4 SUGGESTIONS ON FURTHER RESEARCH ....................................................................................... 51
9 REFERENCES.......................................................................................................................................... 52
1 Introduction

In this chapter a background and related research to this paper is presented alongside the research main- and sub question. Furthermore, the target group and purpose of the research is presented.

1.1 Background

In recent years there has been brought much attention to the privacy requirements of data, i.e. whenever private information is stored, managed, or communicated to third-parties. Currently encryption techniques are used only in such circumstances where data protection is essential or whenever the organization finds it to be essential. These types of techniques do indeed provide some defense against the exposè of personal information; however these types of techniques are far from sufficient enough. People have different views of what counts as sensitive information and what needs to be protected. Current guidelines and regulations are nevertheless not adequate enough in declaring what needs to be done to protect personal and sensitive information. Both private and governmental organizations are progressively gathering more and more data, information has by all means become one of the most highly valued resources and it is therefore it needs to be more properly protected (Cirani et al. 2010).

Cárdenas et al. (2013) states that today’s organizations collectively gather terabytes of data for analysis, and that the amount will only keep on growing when more personnel will get hired and more software will be run. It is nonetheless always important to understand that even with regulations in place; an extensive collection of data is attractive to numerous parties and hackers as well. The recent progresses made in the area of Big Data, has provided organizations with the ability to extract and analyze larger amounts of data, making privacy violations easier. It is thus important that Big Data applications are developed with a great understanding of privacy principles.

Our current world is a digital one and as such everything is able to be measured as data. Big Data as a phenomenon is not the issue; in fact it can be considered a huge possibility, especially for organizations who seek to make profit. A vast amount of data is stored and the numbers are only growing. It is the ethical aspect of Big Data that is of concern, as are the regulations surrounding it; it is also this that has been less researched. By all means, it is also the subject of Big Data that is commonly unknown by the common individual, which is a problem as well, since we spend a lot of time online and provide online companies with a lot of information. We see the advances and results of the usage of data every time we are online. An example of this is when we shop for something at an online store; as we choose an item we would like to purchase we receive a message back that states: 'Customers who purchased this item also purchased these items' and we are provided with a list of several other products we did not consider of in the first place, but that the company wants us to buy, based on information they have gained about us (Ackerman 2012).

An important question to raise is how many of us actually stop and think about how much information about us is stored online, how it is used or misused and who is handling the data. Lots of companies are today choosing to move their data to cloud storage, and with that our data included. The main reasons are to be able to cut costs and make more profit. Online privacy issues have in recent years become a much bigger problem than just a few years past,
though all suppliers of cloud services are not equally trustworthy, nor are the online companies and organizations. The common individual browsing, shopping or writing information online has today very little to no control over what happens with his personal information. Mostly due to the reason that the data is now being stored by a third-party (Li & Guo 2014).

Diesburg & Wang (2010) determine that there is an increasing need to support people in regards to privacy aspects online and to provide them with more opportunities to store and delete their personal data on individual terms. There is an existing distress concerning personal information and the fact that it has the possibility to at any moment in time be hacked, misused or accidentally leaked to third-parties, depending on the person handling the data.

The term Big Data has become a worldwide phenomenon in the past years as more and more data is stored. The term refers simply to the vast and complex amount of data that is available. We create the data ourselves every time we are online, writing, chatting, reading and searching for information. This data is often measured in Exabyte’s. The data is stored, analyzed and managed by large-scaled companies; the purposes are many, for example to advertise the “right” products and services back to you or to sell the information to third-parties. The data is highly beneficial to companies that want to make a large profit. The data consist of textual, image, video, geolocation and audio data (Pope 2014).

It is said that Internet and social media addiction has become a common disorder in today’s society. Thought of as a worldwide problem, it is nevertheless most commonly accepted as a term and most known of, in countries where computer access is general. The disorder has been associated with both neurological and psychological characteristics like depression, anxiety and poor impulse control. It is said that we become so addicted to the usage of the Internet that we disregard the given terms of condition and thus ignore all security threats. Researchers do nevertheless state themselves that more research is needed on the matter, and that all research has to be considered with respect to the amount of respondent that were tested, along with factors like age, gender and location (Shaw & Black 2008).
1.2 Related research

In an article on Internet Addiction Disorder, aka. IAD, Yuan et.al (2011) discusses IAD being associated with structural abnormalities in the brains gray matter. Using a voxel-based morphometric technique, the researchers were able to find multiple structural changes of the brain in IAD subjects. They were able to confirm that long-term Internet addiction would result in brain structural alterations. There were also images captured of the brain matter of IAD subject with a 3T Siemens scanner, capturing reduced gray matter volumes. In the article the researchers refer to IAD as a now common mental health problem, stating that though not being commonly used as a term, IAD indeed has attracted the attention of psychiatrists and the public. Data from the China Youth Internet Association demonstrated that the incidence rate of Internet addiction among Chinese urban youths is about 14%. It is worth noting that the total number of that percentage is 24 million.

Yuan et.al (2011) also discusses the hazards of a strong Internet addiction, talking about its dangers of negatively affecting an individual’s psychological well-being, contributing to academic failure and making way for reduced work performance. The article also refers to other similar researchers like Dong et al. (2010) whose research also has proven that IAD subjects show less efficiency in information processing and have lower cognitive control.

The problem that lays in IAD not yet being fully accepted as a term and a disorder is that there unfortunately, currently is no standardized treatment for IAD and that the longer an individual doesn’t get treatment the worse off he can get, in the context of the disorder becoming more aggressive with time. There are nevertheless possibilities of studying IAD further on and at a higher level than before, as advances in neuroimaging techniques have been made, that provide researchers’ with ideal methods to investigate brain activity and its changes. There is an importance of IAD still being in need to be researched in much greater detail (Dong et al. 2010).

Dong, et al. (2010) discusses the past studies made on Internet Addiction Disorder, IAD, saying that many researchers view this specific disorder to be an impulse disorder that eventually can have a negative impact on an individual’s psychology and social life. The authors also talk about the fact that many other researchers share the view that Internet addicts share similar neuropsychological and personality characteristics with other addicts, like for example drug and alcohol addicts.

Nevertheless, the authors point out the fact that few electrophysiological studies about the relationship between IAD and impulse control have in fact been done. Fortunately though, present studies do aim to find a neural index, underlying the response inhibition difference between Internet addicted people and “normal” people, by using an ERP technique, pointing out to the study of Young et al. (2011). Using trials called Go/NoGo, where one looks at the relation between brain activity and impulse control, where a Go stimulus is requiring response (using a button press) and a NoGo stimulus that requires the inhibition of the response, Dong et al. (2010) were able to provide evidence for the assumption that inhibitory ability is impaired in IAD troubled subjects, that impulse control in IAD individuals differs from that in “normal” people and can be detected.
The authors do however point out weaknesses in their own study, pointing to the fact that all the participants were right-handed students and that all the participants were male students, because few females are in fact addicted to the Internet.

Bhimani (2015) determines that a growing number of organizations exploit the common individuals wanting to be online and their writing large volumes of private information online, that contribute to the Big Data and that they do so simply to make profit and to create more value for themselves. It is the volume of data and the many possibility and ways in which one can use the data that is attractive. The lack of proper regulations is another factor. The common individual either does not know of Big Data or is poorly aware of it and of the terms and conditions one accepts online, which lets companies to exploit the data in many different ways. As more and more people have access to the Internet the volumes of data grow as well. The personalized ads we see each time we are online is only one of many examples of how the data has been exploited. Mining knowledge from the data is the main purpose, since with the power of knowledge one can create many opportunities; this has become part of the strategic work of companies. It is with methods like web mining and techniques like profiling that makes this a possibility. The developments in digitalization and software are also factors that create new possibilities for organizations.
1.3 Research question

Main question:

Does the use of social media have a negative impact on individuals’ desire for online privacy?

Sub question:

What hazards does the lack of regulations on Big Data have on online privacy?

1.4 Purpose of the research

The purpose of this research is to highlight the importance of online privacy and users’ knowledge of data exploitation. The research paper is of educational nature. Furthermore, the purpose of the research paper is to bring insight to the large volumes of data collection, storage and distribution that occur in today’s society as well as to individuals’ social media addiction.

1.5 Target group

As the research paper is of educational nature, the main target group is students in the field of Informatics that wish to gain more knowledge in the subjects of online privacy, Big Data, social media and regulations. The secondary target group is the common individual who wishes to expand his or her views on social media addiction and regulations regarding online privacy. A third target group is researchers in the field of Informatics who wish to read more papers on the subjects of data regulations, online privacy and social media addiction.
2 Method

In this chapter, the chosen method of research is presented and motivated.

2.1 Deduction

The research is based on the deductive theory. The process of deduction is created of six steps. The steps are followed in a logical sequence.

1 – Finding theory
2 – Creating a hypothesis
3 – Collecting appropriate data
4 – Making findings
5 – Confirming or rejecting the hypothesis
6 – Making a revision of the theory

Taking upon a deductive theory, one aims to find a relationship between theory and research. The theory is supposed to form a basis for the empirical study (Bryman & Bell 2011). The theory that is found in this research paper forms a basis for the empirical study and the hypothesis. The empirical study and findings within it, form a basis for the discussion in which the hypothesis is either accepted or rejected.

The hypothesis that is examined in this research is that there is a negative relationship between an individual’s alleged addictive social media usage and the need for online privacy.

2.2 Qualitative research

The chosen research strategy is of the qualitative nature.

Qualitative research enables the ‘right’ information to surface. Unlike the choice of a quantitative method, the qualitative research strategy is a very powerful one, in the sense that it has potentials to generate in a great understanding of the respondents, due to the reason of the researcher meeting the respondents in person (Bryman & Bell 2011). The quantitative method is based on numerical measurements in the data collection and statistical processing methods. (Patel & Davidson 2011) In this research paper I was keen on finding an understanding in the mindset of social media users, finding the reasons of their usage of social media and their understandings of the potential hazards. It is therefore I chose the qualitative method of interviewing the respondents, not only to be able to hear them answer the question but also to see their body language as they were answering.

2.3 Interviews – procedure

Structured interviews were conducted in which sixty two respondents were asked two questions regarding their usage of social media. (Social media is in this context not narrowed to one specific platform, though Facebook, Instagram, Twitter etc. are all included)
The respondents were given the option of answering either yes or no to the questions. The respondents were nevertheless given the opportunity’s to comment on their choices which lead to very interesting findings in regards to their views on social media in general, online privacy, hackers and the storage of their private data. The respondents were of the ages between twenty four and fifty two and consisted of forty percent males and sixty percent females. It is important to note the variety in ages among the respondents since there is no intention in this research of making the point of there existing a divide in generations. Precaution was taken as to ask all respondents the questions in the exact same way.

Structured interviews use pre-determined and identical questions for all respondents. It is important to read out the questions in the same way to each respondent and note the answers without comment; otherwise you might indicate your own views to the respondent (Oates 2006).

As mentioned, the interviews also opened up for the possibility for the respondents to comment on their answers, stating why they answered the way they did. The purpose of the interviews was to gain insight into the respondents’ knowledge of online privacy. The qualitative research was based on objectivism. Being objective is important as it is the respondents’ views that are of interest and not the interviewers. (Bryman & Bell 2011)

2.4 Observations – procedure

Furthermore, a qualitative observation study was conducted. Current popular media and literature was observed and analyzed. The purpose for this research was to find out the current status on which Internet addiction, social media, online privacy and Big Data is discussed, to what extent and which researchers and authors were advocates and which were critics. Oates (2006) states that observation as a data generation method can be used within any research study. Observations can generate in gaining rich insight, leading to holistic explanations. It is nevertheless difficult to generalize from observations and they can lack in reliability as the research can be difficult to replicate.

2.5 Sampling

Convenience sampling was used in the qualitative research. A convenience sample is one that is simply available to the researcher by virtue of its accessibility. The problem of such a sampling strategy is that it becomes very difficult to generalize the findings. (Bryman & Bell 2011) The purpose of this sampling strategy was nevertheless of the point to not to generalize the finding that could possibly create a problem of letting the respondents to be put in to categories which could generate a generation question, which was not the purpose of the study. The respondents were therefore in this case of the ages between twenty four and fifty two and consisted of forty percent males and sixty percent females.

2.6 Data collection

I collected the data mainly using the schools online library search, i.e. http://www hb.se/Biblioteket/ and various databases including the ACM Digital Library and IEEExplore. The search words I used included Big Data ethics, Web mining strategies, Social Media paradox, Internet addiction and Big Data regulations. I also looked to books, Informatics course literature and journals.
Furthermore, in the observational study on popular media I was looking at articles, books, YouTube clips and documentary films, always evaluating the most valid research that could be used.

2.7 Criteria for theoretical study

Oates (2006) states that textbooks can be useful as introductory sources, as they explain the main approaches or theories and due to the fact that they give guidance. They are nevertheless limited and research must be conducted using journals, reports and databases as well. The author also highlights the importance of assessing the credibility of any text that one finds.


Essential researchers have in recent years had the possibilities of not only looking at journals for their theoretical framework, but also magazines and other media on the Internet. (Oates 2006)

2.8 Qualitative analysis method

The advantages of a qualitative data analysis include that the data and its analysis can be rich and detailed, including words, images, video and websites, which are all very useful to IS research. The possibility of alternative explanations is also an advantage. A disadvantage is that interpretation of the data is more closely tied to the researchers’ identity, background and assumptions (Oates 2006).

A typical set of analytic moves include going through the material at hand and finding similarities and differences in opinion and patterns, while adding comments and making elaborations. (Robson 2011)

2.9 Positivism

Positivist research aims to prove or disprove a hypothesis. Using the positivism strategy, the researcher aims to be objective. The researcher creates hypotheses and tests them. The other aim in positivism is validity where the researcher focuses on high generalizability. Though often considered to be related to quantitative research, positivism can be applied to other forms of research as well. (Oates 2006) I chose the positivism method approach due to the fact that I chose deduction as my research theory. Using deduction the researcher aims to create and accept or reject a hypothesis, which is related to the positivism strategy.

2.10 Validity

Validity is commonly seen as the most important criteria in research. The collection of data has to be relevant for the research question. The observer must be bias in the research strategy; the researcher must also be objective (Robson 2011). I seek for validity as I have made a great effort as to staying objective throughout the entire research.
3 Theoretical Study

In this chapter the applied theory for the research is presented. This theory forms a basis for the hypothesis created in chapter 4.

3.1 Paradoxes

Farjoun (2010) states that commercial companies whose aim is to make as much profit as possible, need to acclimatize a sense of stability in their business in order to keep customers trust and to have customers returning. Those types of companies should also seek change in their business, as the market is constantly changing and new competitors come out with similar or innovative services and products. This however, brings along a paradox with itself, as stability and change are two clear opposites of each other. By both technological and economical preferences, efficiency and specialization do not coexist with the dynamic efficiency required for innovation. It is nevertheless in a profitable company’s nature to adapt itself to the current environment or at least, so should it be, as without adaptation a company simply cannot survive in a competitive market. The author nevertheless conceptualizes that change and stability should not be a question of dualism but rather of duality. Conceptually viewed as a duality, stability and change, though theoretically separate, do have the potential to be compatible. The author also concludes that change in fact by all means can enable stability rather than be its opposite. A shared concern in organizations is the concern of system reliability. To some, reliability means loyalty to a particular service; to others it means the security of core methods. The author does conversely claim that several studies have shown that most managers do in fact use much discipline and rules in their organizations, though not always in the sense of the good of the customer but rather in order to protect the business itself.

It can be concluded that the longer a system is sustained without failure, the more reliable it becomes. Organizations nonetheless also need to be efficient and efficiency is first and foremost associated with short-term reliability. This short-term reliability makes systems unstable, less efficient and makes them vulnerable to many options of failure alongside system meltdown. This is also a clear paradox. Organization to often focus on avoiding problems rather than repeating what seemed to work or reacting fast after failure. They experiment with ways to avoid problems in ways that can not only inhabit their users’ security but also cause more long-term problems to the systems themselves. In order to increase long-term stability in systems, organizations need to understand the importance of combining rules, discipline and routines, with variety.

Lewis (2000) talks about paradoxes appearing increasingly in organizations today. There is a conflict happening in many organizations as they need to provide some form of security in their systems as they need to be highly competitive as well. The increasing changes in technology, global rivalry and personnel variety expose and strengthen paradoxes. Paradoxes are contradictory yet connected to each other at the same time. As the two sides of a paradox can seem logical in separation they seem absurd and unreasonable when discussed together. Unlike a dilemma, a paradox signifies two sides of the same coin. The author determines that today’s complex organizations need to be acknowledging and managing paradoxes rather than
suppressing them and believing that they do not exist. That is nevertheless something that takes time and something that not many managers are prepared to do.

As well as managers in competitive organizations, many researchers are equally conflicted on how organizations should best handle paradoxes. Some propose that managers should simply and only accept paradoxes as that can lead to a sense of freedom and helps managers to avoid debates and tension; others on the other hand, propose that managers need to confront paradoxes in order to better understand their organizations and make way for better and more reliable systems that offer a high security.

Having a negative outlook on the Internet and its rise, Kraut et al. (1998) made the point that the Internet has lots of potentials in altering our day-to-day lives, however not necessarily for the better. The authors discuss that much research has shown that the usage of Internet can in fact harm the common individual in various psychological ways as they can become more detached from real life social happenings. The authors also make the point that there occurs a paradox in the sense that while the Internet has many capability’s to enhance our social lives, with for example social communities that makes it easier for us to connect with old friends and family in real time, it has at the same time been shown that we in fact become less social as we depend on the computer to the extent that we start to connect less in real life, generating a negative effect on social involvement which is in many ways key in our evolution. The authors conclude that until technology evolves to become more beneficial, people need to moderate their use of the Internet, if only for their own well-being. All things are good in moderation and an excessive use of any product or service can have a negative effect on an individual’s well-being in any case.

While the new generations spend more time online, they create a wealth of opportunities for marketing companies. These companies use social media as a platform for finding information about their current and potential customers. There often nevertheless occurs a misunderstanding of how people actually use social media, which in turn could lead to inadequate predictions. One could be a critic or advocate of social media, yet the matter is that there are nonetheless both positive consequences of social media consumption and negative ones. The impact of social media on the welfare of the common individual nevertheless remains a matter of debate. For some researchers, social media is contributing in the development and keep of social relationships, allowing people to meet and stay connected with families, friends and colleagues at geographically distant locations (Barcelos et al. 2014).

Moreover, as the Internet offers anonymity at times when one want it, people start to feel less introverted and start to express themselves in ways that they would normally not be comfortable doing in person. The adolescent’s brain is particularly vulnerable and if not supervised one might start making risky and impulsive actions. It is therefore many social media sites state that one must be a certain age before logging in to the site, that can unfortunately not be confirmed in any way other than a person accepting the given terms and conditions. It is therefore very important that the younger users are monitored. There exists nevertheless a conflict between young people’s desire to protect their privacy and their actual behavior on social media. Barcelos et al. (2014) conducted a study in which they were able to show that adolescents report contradictory opinions on the option to block private information and photos on social media. It was concluded that although they did not appreciate the existence of privacy settings, they were undoubtedly afraid of the possibility of strangers or people “from outside the group” gaining access to their data.
3.2 Big Data

The advocates of Big Data claim it to be a sophisticated analytics system, which allows the mining of vastly large data sets in purpose of gaining insight, in order to come up with solutions to many of society’s problems. The advocates also state that the collection of data can in the future help organizations of all sorts to not only improve their business but also to improve our lives and make them safer. Some advocates like the authors of the book *The human face of Big Data* (Smolan & Erwitt 2012) go as far as to claim Big Data to be an "extraordinary knowledge revolution" (Richards & King 2013).

Not disagreeing on the many potentials of Big Data, yet rather looking at it from a more critical point of view Richards & King (2013) make the point of that there is no denying the fact that the data that is collected is most often very private and the collection and storage of peoples private data is in fact shrouded in legal secrecy. The data that is collected is vast, not only in the sense of how much data is stored but also what type of data is stored i.e. everything from, click patterns to places, shopping history, posts on social network and mobile traffic. The truth is that we are already influenced by Big Data every time we are online and visit sites like for example Yahoo or Google where we are getting tailored search results and ads. This collection happens invisibly and most likely without the common individual’s knowledge. The authors state that Big Data now has the power to shape our identities and our views of the world. Big Data undoubtedly also benefits large governments and corporations at the expense of ordinary individuals. That is a paradox of Big Data. The authors concludes that Big Data is indeed revolutionary but that we need to figure out a way to better control Big Data and to figure out a way to take more advantage of the good things that it can do, while trying to avoid the bad.

Zwitter (2014) talks about there now occurring a change in the way we should talk and handle aspects of ethics in regards to Big Data or rather the lack of ethics. The needed ethics are concerning particularly the individual’s privacy and the moral that there currently is a lack of regulations, when it comes to what type of data is collected and for how long. The questions on ethics definitely came to surface along with the ‘Snowden case’ and were starting to be discussed in the media. That is nevertheless a problem on its own, the fact that we are not talking about the moral and ethical questions regarding Big Data, without such an event. The problem of Big Data lays also in the fact that much of its work is done secretly. More transparency is absolutely needed, for example in regards to social media, where the information on what we “like” is sold to third-parties, such as marketing companies. This is nevertheless much of a political question. It is in politics where new and better regulations need to come in to place, in order for transparency of Big Data to become better. The problem of setting good regulations is that Big Data is global, and that what might be legal or what might be considered as ethical in one country might not be considered as such in another.

Lafuente (2015) also talk about the challenges of Big Data, stating that with Big Data come many challenges. In terms of marketing, companies and organizations of various sorts have much to gain. There is however a fine line in when it comes to breaking the common individual’s privacy. The ordinary individuals are not taken into consideration as they should, though there might come a day when a data breach could be catastrophic and lead to legal repercussions. Personal data is in need to be handled with more care. What can be done is that organizations that use Big Data, try and isolate sensitive information, such as for example, health records, and with that try and ensure more security. Another option is encrypting the
data or anonymizing the data. The data that is collected and stored need also to become more structured as it today is much unstructured.

Hsinchun (2012) concludes that we are currently living in a Big Data era. Big Data is grounded in data mining, statistical analytics, and text, web, mobile and network analytics. The amount of data that is collected and stored comes at a terabyte scale and that new science, knowledge and discovery’s can be obtained with Big Data which any organization can take advantage of. The author also states that there is significant proof in that Big Data has a BIG impact on large-scaled organizations and companies like Google, Facebook and Amazon, that all are leading actors in the use of web analytics and social media platforms. Big Data is also able to support government decision making at both a macroscopic level and a microscopic level. This publicity however, comes at a cost of concerns in regard to users’ and customers’ privacy and data security. Security issues are costly for organizations and it is said to be a billion dollar business. It is therefore undoubtedly important to set proper regulations on Big Data.

There are several ethical aspects and issues with Big Data. As researched by Li & Guo (2014) there are in fact algorithms that can be used to obtain more security of the data. An example of this is ReadandRemove, as the name hints; it is about reading the provided information in the cloud and then directly removing it from storage. It becomes an important aspect for today's companies to write contracts with cloud services to obtain as much security as possible, to reduce risks of social ethics and sustainability. It seems as though companies either focus on social or economic aspects in which the economic ones tends to be more interesting and more important for the companies. There is also an issue of environmental aspects and how those affect the common individual and how one looks upon a company, though many people today are greatly affected by and interested in the environmental problems. That too however seem to be taking a backseat in companies’ interest for the benefit of the economic aspects, i.e. making profit (Li & Guo 2014).

The high value of online information was spoken of already in the 1980's by Durieux (1989). The author discusses information to be a valuable resource for managers and economists that seek out competitive advantage, to cut costs and gain profit. Economists as well as managers rely heavily on information. The value of information is growing in price and the information that can be obtained free of charge is priceless. The information can nevertheless become a problem in law, as the volume of information grows and its methods of delivery change. Durieux predicted that the usage of computers and the volumes of information being stored on technological platforms would keep on growing, as would the value and importance of information. In the US alone, the market of computer based information was in 1984 valued to around 15 billion. Durieux refers to the term online information as direct access.

In the year 2006, humans produced an astonishing 161 Exabyte’s of digital information; this number has since grown tremendously. The number becomes even more astonishing, knowing that in 2006 only 18 % of the world’s population had access to the Internet (Conti 2009).
3.3 Web mining

Web mining is often discussed as the future of computer-based research. The method has the excessive potentials to scan through vast origins of digital information in order to find relevant data and to reveal patterns that can tell a company almost everything there is to know about its customers, for example what they are most interested in buying, where and at what point in time. The main purpose of web mining is discovering meaningful knowledge from data, this includes blogs, and social media and includes analysis of structure, usage, and content in order to extract and analyze the information. Web mining makes way for gaining understanding into customers’ behavior. Many large organizations such as Google and Yahoo are using this method and are able to scuttle across large-scale content online in order to store it and use it for commercial gain. The focus of web mining as mentioned before lies on discovering meaningful patterns in the data. The entire web is mined including all texts, videos, audios, images and hyperlinks. When the data has been mined it becomes easier to endorse content to users (Van Norden 2013).

Linoff (2011) states that forecasting customer behavior is a valued business goal. There are many techniques one can use in order to create such forecasting; two examples are predictions and profiling. Questions that can be answered when making predictions are for example: what is the best offer for the given customer and when will the customer make his next purchase?

Historical factors of a customer’s behavior are also very important, as by looking at intervals between a customer’s purchases one can make further predictions of the future. Profiling is a technique based on variables like, age, gender and location etc. A company can make a big increase in sales by using the profiling technique. Questions that can be answered using this technique are among others: Who is the customer and what items are bought together? By then analyzing the data, managers of a store can put items that sell best together and make other item categorization decisions in order to increase sale (Linoff 2011).

Knowledge about customers is central in the establishment of viable e-commerce solutions. The web mining method and the associated web mining techniques make way for acquiring knowledge for improved e-commerce. The benefits are many, the biggest thought is that companies can improve their sells, cut costs and make a huge profit. The addition of clickstream collection permits exceptional measurement of site activities and provides companies managers with more knowledge. Clickstream data is over 95 % of all data collected in most e-commerce environments and holds a fortune of knowledge rooted in it (Kohavi 2002).
3.4 Regulations

Social media and the web can on one hand be argued as a platform for freedom of expression and freedom of thought. It is important to note that the platforms that do offer the possibility of free expression and anonymity are most often formed on political decisions and are subject of censorship, influence of media ownership and editorial control. In many ways, social media enables freedom of expression in its purest form. On the other hand, by accepting terms and conditions online, you put yourself in a very vulnerable position as you accept that the organization that controls the platform is able to control your data in any way shape or form. The common individual is not always prepared for the responsibility that comes with its use or its consequences. The web is much like the Wild West when it comes to laws and regulations. As politics change, so do opinions on regulations online, this enables many organizations to rewrite their terms and conditions in ways unimaginable to the common individual. Loopholes will always be sought after in law as an organizations first aim is to make profit and not to protect you. New politicians in government also mean new point of views on what should or should not be written in law in regards to the Internet. As regulations change frequently it becomes an easy task for programmers and mangers to find loopholes (Coe 2015).

What begins as casual acts of expression, for example a conversation on politics with friends or colleagues, sharing pictures, articles and thoughts, become permanent data sets that can be used in making predictions on the individuals as to whom they are, what they stand for and what they are likely to buy. Storing and analyzing individual’s data for the purpose of profit give rise to many concerns regarding individual’s rights to privacy. The simple being online also give way for concerns on protection from harassment, bullying and threatening, as we clearly can see in today’s society, everyone are potential subjects of harassment. The lack of regulations online enables this. It is no easy task nevertheless to apply the same rules and legislations online as in real life. Though information is stored and processed in a very different matter on the web (Coe 2015).

Throughout the years many cases on online harassment, stalking and bullying have seen their days in court, so have cases on companies collections on individual’s data. In May 2014 it was announced that Snapchat had settled with the US Federal Trade Commission for misleading its users over data collection, and failing to inform them that their photos could be saved, thus raising concerns over the durableness of pictures taken using its mobile phone application. The big issue was that all photos were in October 2014 hacked, when www.snapsaved.com a third-party ‘add-on’ site to Snapchat, was hacked by an unknown group. Thus, pictures stored on Snapchat were made available online to everybody. Though no law could make sure no hacker could get hold of the pictures, a regulation could have been in place that would not have allowed for the organization to store the photos for a longer period of time in the first place (Coe 2015).
(Conti 2009) states that websites and services like for example Google can in fact be too usable, tempting people to reveal information without concern, including extremely sensitive and personal information. Each search query on Google provides a new piece of information that makes up a profile of each user and delivers the means to uniquely identify the individual. In fact Google has the power to form public opinions, expose sensitive information to third parties and blackmail individual people from the certain websites. They have the means to do so, due to the lack of regulations.

Web based information exposé is a battlefield. Programmers, lawyers, policy makers, web users, privacy advocates and companies all have different thought on the subject. Conti (2009) also stresses the importance of knowledge of what is regulated online and what isn’t as well as what the consequences of being online are, stating that the common individual needs to become more aware of what he is giving away in terms of personal information and know the long-term impact of that type of exposé. Becoming an informed user is the most effective countermeasure.

Online regulations and ethics are at the heart of the debate surrounding web-based information disclosure. They include usage and privacy policies. Today’s policies are generally insufficient and flexible. At the stroke of a pen, they can change, based on corporate needs and current politics. The matter of fact is that most terms and conditions and regulations online are written by lawyers for lawyers and they are written to protect the company, not you. A well written policy is a key factor to success in an organization, as writing in that the organization owns all information posted, they hold all the power and gain much competitive advantage. Conti (2009) concludes nevertheless that there is a very effective way to make people wake up and recognize the dangers online. By showing people queries from the AOL dataset they get to see with their own eyes what and how much sensitive information is stored. When people are directly confronted with information like that, it is very hard to argue that the problem doesn’t exist. With that, it is fairly easy to state that a little paranoia is healthy when it comes to security and privacy online.

Chadwick (2003) expresses the hope that public services if exposed to the same kind of threats as the common individual will become more sensitive and thoughtful to the demands of their users in regards to online privacy. As we see today it is no longer only the common individual whose data is hacked, but the entire organizations data, which include not only their customers’ data but also companies’ passwords, security routines and other sensitive information. This type of threats should make organizations managers and lawyers rethink their security and start to adapt to changes in operational policy’s, making sure threats like hacking and fraud would minimize. E-government is a way of bringing governments and organizations “closer to the people”, by meeting their expectations on regulations. Some advocates of high online security and E-government go as far as to stating that E-government should include people entirely into the regular policy-making processes.
The author continues on the subject of E-government saying that it needs to become a “learning organization,” able to respond to the needs of its citizens. There are currently and unquestionably many political, economic, and technical barriers to the development of E-government. Data today flows freely on the web, and is exposed to many security issues due to the lack of regulations. E-government is as all things also met by resistance in many cases, especially as citizens become more aware of the new techniques of surveillance that are being established in answer to electronic communication. Private sector organizations nevertheless rarely face political opposition, unlike the public sector. Another political problem, is the fear among senior managers who are afraid of change in their organizations and the dramatic increases in requests for information from citizens i.e. customers and users (Chadwick 2003).

The challenges towards E-democracy, through the electronic change of political systems, have become progressively obvious within developed economies and commercial organizations. Even though it is many times regarded as a way for increased and better quality in regards to citizen participation in the democratic processes, there are still many critics of E-government. E-democracy forms a factor of overall E-government initiatives, where technology adoption and diffusion, to develop broader access to, and the delivery of, government services, are obvious. Fear of change is not restricted to managers in big profitable organizations nonetheless; there exists a fear in politicians as well, a fear that inhabits the further evolution of E-democracy. E-democracy is generally regarded as an instrument for deserting the representative systems for ones with more direct citizen engagement (Mahrer & Krimmer 2005).
3.5 Internet addiction

An article on BBC News discusses the findings in China by Yuan et al. Stating in the article that it has now been confirmed that individuals addicted to the web, do in fact show brain changes in similar ways to those hooked on drugs. The article states that Internet addiction is in fact a clinical disorder marked by out-of-control Internet use and that the study conducted in China showed evidence using a specialized MRI brain scan, that there was in fact a disruption in the connections in nerve fibers linking brain areas in emotions and self-control. In the article a statement on the study had also been given by psychiatrist Dr. Henrietta Boden-Jones, stating that “The research was groundbreaking” (Briggs 2012).

Shaw & Black (2008) discuss the problem of the fact that despite the attention Internet addiction has received; scientific understanding has not been very high, in part because of the lack of a common definition and consistent terminology. The authors also discuss Internet addiction and in particular social media usage, as having the possibility to be linked to other disorders, such as OCD aka. Obsessive-compulsive disorder, and ICD aka. Impulse control disorder. The authors likewise discuss the ‘National Institute on Drug Abuses’ view on Internet addiction, labeling it as a “pure behavioral addiction” because it is not tainted by the presence of an “exogenous substance”. The authors also discuss the matter of there being those researchers and authors whom in fact do criticize the attempts to categorize Internet addiction as a disorder stating that critics question the existence of Internet addiction due to the many alleged weakness in confirming its existence. Shaw & Black (2008) however, state that that type of criticism only trivializes and minimizes the attempts to understand or treat Internet addiction.

Habits in the brain and the brains reward system is nevertheless heavily discussed in media and research. Fredholm (2007) talks about the reward system not being concentrated to just one area of the brain but rather that it is connected to the entire communication system and that that is what makes the reward system so very powerful. When an individual for example eats or drinks something, there occurs an extract of dopamine in the brain that affects the reward system in a positive way and makes the individual want to eat or drink again. This event occurs in exactly the same way when one takes drugs or alcohol, this is why it is so very easy for people to become addicted. The more the individual then becomes addicted the more dopamine release there occurs in the brain, this has also been proved in an independent study on addiction in the US using a PET-camera.

Hu (2014) concludes that social media services allow users many different benefits, such as for example building and maintaining a networks of friends, that support the users in creating lasting powerful relationships that the users might not want to lose. That is why social media addiction is powerful. There is nevertheless an evident exposure to many hazards as the users in a way give away their own privacy to the service providers, for the maintenance of these relationships. The author state that with social media comes two essential and overlapping benefits, that is: relational and informational. Users gain benefits psychologically when creating groups online, maintain them, keeping contact and when they post information as they receive positive feedback. In the context of informational gain, users are provided with advertisement and information from their peers.
An additional reward in the context of using social media is based on how a symbolic online system can create a surrealistic environment, where users treat in interactive, gratifying and pleasant experiences and with that gain the benefits of enjoyment and curiosity fulfillment. These benefits are gained when the users for example play a game with their friends.

Nevertheless, the many benefits of social media do come at a cost of informational risks and privacy violations. Informational risk is defined as “individuals’ loss of control over information about personal traits, actions, and attributes”. While value can be assessed as positive or negative given trade-offs, a sensible user of a service such as social media, should continue to use a service as long as value is evaluated positively. Trust in these service providers is key, as is trust in organizations and brand reputation. These are reasons to why users spend time on social media (Hu 2014).
3.6 **Online privacy**

Concerns on privacy, especially in commercial use, have been present ever since the 1990’s. The problem of how personal data can be used and is used for marketing purposes is one of great concern both for organizations and their customers. Organizations today have only guidelines when it comes to how information can be gathered and how that information later on can be used, which in turn can lead to a misuse. Customers on the other hand can have their own concerns regarding how their personal information was used for marketing, why and how much (Nunan & Domenico 2013). Furthermore George et al. (2014) states that Big Data-sharing agreements continue to be informal and poorly structured and that these agreements do need to be linked to a greater extent to data privacy aspects.

The issue of Big Data privacy is that many companies tend to trade-off the privacy aspects of individuals for statistic results. Ensuring privacy has become a big problem and should not become easily looked upon. Not only is it of great importance to provide individuals with information on what is being done with their personal information but also for companies to understand which third-parties they are trading information with. A problem within the problem of privacy is what kind of information is to be considered as sensitive. This differs from person to person and it is therefore the privacy aspects of Big Data has a long way to go before being understood and perfected by companies and third-parties. Users should nonetheless be able to themselves specify what counts as sensitive information, which needs to be protected (He et al. 2014).

As the technology has grown so has the many concerns people have over privacy, we tend to believe that the web should be a sort of an open space, for everyone to share their information, yet we do want to protect our own privacy. Many people do not know however, that by logging on to for example a social media site, they accept terms of letting their personal information to be stored and sold. For market researchers and analysts this type of information about people is of great importance and benefit companies greatly (Nunana & Domenico 2013).

Collecting and analyzing data is an important factor in today’s commercialized world where much of the profit a company makes comes from the possibilities of offering the right product for customers, something that is obtained by a wide collection of personal data. A recent challenge of Big Data though, is that the data is increasingly being collected independent of humans, i.e. autonomously (Nunana & Domenico 2013).

Conti (2009) explains that when one takes in to consideration the volume of digital information and the resources that only a company like Google has at its disposal, one can easily imagine the power the company possesses. In 2009 alone, Google’s revenue was 13 billion dollars. It is important to understand that it is a business and that what companies like Google or Twitter are providing to their customers is part of their business strategy. It is a business strategy that enables the companies to make huge profit, often on the common individual’s expense.
The desired skills that an employee at Google should possess are skills in among others: algorithms, data mining, information retrieval, profiling, machine learning and text processing. This reveals a lot of information on what type of a business Google in fact is. Many times though, the common individuals focus is only that he is provided with a service that enables information search and communication for free. There is nevertheless no such thing as a free offer online. One does pay for the service in one way or another and if the payment is not handled with money, one might be certain of the fact that the payment is personal information. Every single search word on Google is stored and analyzed. If not for the purpose of providing individuals with personalized advertisement, then for the purpose of the information being sold to a third-party (Conti 2009).

The author also discusses that there is some data that is in fact reasonable for companies to retain. However, the issue lays in the lack of regulations surrounding data preservation. To date, companies are able to store the information on all of an individual’s online activities for an indeterminate time. Some companies do nevertheless make a gesture of anonymizing the data after a certain amount of time, far too few companies are making that gesture though. Companies should by all means ensure their customers and users protection, in regards to their private information; it is the ethical thing to do. When data is stored on a company’s server, like for example Google, the data has to date only the possibility of being protected by the Electronic Communications Privacy Act, which is far from good enough. It is also important to know that in fact, by law, companies’ obligation is to work in the best interest of their shareholders, not essentially their users.

Rossnagel et al. (2013) state that service providers of for example social media demand user interaction and authentication. Nevertheless even the use of passwords leads to several problems, such as inconvenient password management issues password reuse and other security problems. Rossnagel continues stating that numerous authors have identified hazards of information privacy of services like social media and have also identified many ways to ensure more privacy. For example, ‘User-centric identity management’, which provides users full control over their personal information. These authors also argue that improving privacy will address the problem of there existing a lack of trust. Perceived benefits of information nonetheless disclosure negatively influence perceived risk, which in turn negatively influences perceived privacy. Users most often do not nevertheless value such features as extensive. It is evident that users often prefer systems in which an intermediary takes responsibility for data, which is viewed as a problem in itself. This enables organizations to save lots of data on the users and make much profit.

The lack of regulations online bring with them many hazard, among others cybercriminals, or as they are more commonly known: hackers. These people are most often not the people we imagine them to be. They aren’t drug addicts who browse the web and hack information for fun. This is an important aspect to have in mind when talking about privacy issues. Though the information is always vulnerable online and if hacked, have the possibility to be used or misused in a numerous different ways depending on the hacker. It is important nevertheless to note that hackers most often are very intelligent; they have a lot of money, connections and are really good at what they do. They are also represented all around the world, and they know that their chances of getting caught are very low (Jakobsson 2012).
4 Hypotheses

Based on the theoretical study, three separate yet related to each other hypotheses, are presented. These hypotheses are later on explored and discussed in chapter 7. The hypotheses are also in chapter 7 either accepted or rejected. Furthermore, the hypotheses are connected to chapter 5.3 in which the interview questions to the respondents are presented. The questions were created taking in to consideration the hypotheses. The given answers from the respondents could later on, along with theory and the empirical study form a basis for the discussion.

1. If an individual becomes addicted to social media, he does not question online privacy regulations.

As it is stated in chapter 3.5 the brains reward system is a strong one. Research conducted on the brains abnormalities by Fredholm (2007) and Briggs (2012) as well as Hu (2014) clearly shows that an individual can become addicted to the Internet and particularly to social media. The supposed rewards one receives visiting social media sites are similar to those rewards an alcohol or drug abuser receives. The reward is in this context the dopamine extraction in the brain. As more dopamine is released the more an individual wants to continue that habit that enables it to happen. In this context that is staying online on social media sites, chatting and writing posts about one’s personal life. Though Internet addiction has not to date yet become fully accepted as a condition by all scientists it has by all means caught the attention of scientists, psychologists and researchers. It is therefore vital to keep on looking at the consequences of a strong Internet abuse.

A raised question is if whether or not an individual in fact questions privacy regulations at any time or if the reward system is so powerful that it makes an individual to disregard the regulations completely, not considering the hazards.

In chapter 3.6 online privacy is questioned, in particular by Conti (2009). There is a supposed online privacy regulation, yet organizations have to date only guidelines to follow when creating online privacy regulations. An individual’s disregard of what kind of privacy one actually possesses online is therefore very hazards as one can give out to much sensitive information thinking it is protected when it actually is not.

2. If a website offers its online services for free, we do not care to read the given terms and conditions.

This hypothesis is also connected to chapter 3.5 and Internet addiction, as when an individual becomes addicted to the Internet one simply does not care to read any given terms and conditions though they are not of concern for the individual. All that matters is that the individual gets to be on the given social media site and keep receiving the dopamine jolt that follows by writing information about ones day to day activities and receiving positive feedback on those posts from one’s peers.
In chapter 3.1 it becomes nevertheless evident by Barcelos et al. (2014) that individuals commonly do to appreciate the fact that they have to sign any privacy statement, yet that they are concerned that anyone from the “outside” would gain access to their information. A question that can be raised is whether or not the aspect of the online service being free of charge plays an important factor or not and if it is simply the matter of the dopamine jolt that makes people disregard the given terms and conditions or if there are other factors.

3. The lack of regulations on Big Data, enable managers to exploit the data in a ways that harms online privacy and security.

As expressed in chapters 3.3 and 3.4 there are many ways in which an organization can find and exploit information online. For example by using webbots or by making prediction on customers or by making profiles.

As uttered by Conti (2009) Big Data has in many ways become a question of ethics rather than regulation, this due to the fact that it simply is very difficult to create good and long lasting online regulations. If Big Data then now has become a question of ethics, managers of large organizations are faced with a big dilemma on whether or not to store data for longer periods of time and what type of data is to be considered as sensitive. Coe (2015) states that the lack of regulations allow managers to store as much information as they wish on their users and that not many managers are keen on changing there ways. Storing information for large periods of time enable hackers to gain access to the information at any given moment. It is to be considered what kind of change must occur in order for the organizations managers to change their ways and if perhaps a change in the common individuals Internet usage could result in a change as well. It is also important to try and understand just why it is difficult to create good regulations online and what can be done about it.

Access to information is nevertheless highly valued today as it enables organizations at any scale to make large profits. It is many times the customer’s themselves that provide organizations with a lot of information about them, while disregarding privacy concerns. This is nonetheless connected to the first and second hypothesis and Internet addiction and as these are later on explored so is this final hypothesis.
5 Empirical study

The empirical study in this chapter consists of two parts. The first being observations of popular media and the second being interviews. The research strategy for this study is presented in chapter 2. Discussion on the finding is found in chapter 7. The analysis is found in chapter 6.

5.1 Observations – Popular Media

Internet and social media addiction is discussed widely in popular media and by several different researchers. The opinions aren’t always similar; however, this however provides the research with a good discussion, not only on the subject of whether or not social media addiction is a real phenomenon but also on human behavior in the context of the growth of the IT society in general.

5.1.1 Internet addiction

The society has in recent years come to the point where we now are discussing the terms of social media addiction. Using the Internet is no longer only a simple matter of logging in once or twice a week to check e-mails or just using the computer for work purposes. The behavior has shifted to the point where people act obsessively as they aren’t able to stop themselves from constantly checking their e-mail account, shopping online or writing post about their own lives on social media (Financial Times 2013).

Prof. Kristen Lindquist at the University of North Carolina, (a professor in psychology) talks about there occurring a dopamine jolt that is the effect on the reward center in the brain while being active on social media. This jolt occurs when someone makes a positive comment on what we have written on the web. This type of dopamine jolt can be compared to the way a drug addict feels the need to go back for more drugs, where the social media addict goes back to write more information on himself on the web. The addict develops an association between goodness and social media. Research has nevertheless been conducted that prove that long-term Internet addiction could in fact result in brain structural alterations (Financial Times 2013).

An article in Huffington Post discusses social media addiction referring to research that demonstrated the reality of addictive qualities of social media. A research conducted by psychologists in Albany – USA, concluded the fact that those people that are heavy social media users are at risk for impulse-control issues like substance abuse. This research was conducted on 253 undergraduate students and the questions asked where the same as for people suffering from alcohol abuse. These questions were among others: “How good does Facebook make you feel?” and "Do you check Facebook first thing when you wake up in the morning?" One of the leading psychologists of the study, Julia Hormes, reported Facebook as having especially addictive properties, talking about notifications and “likes” acting as reward for the users. Hormes also states that a disorderly social media use is very likely a symptom of deprived emotional skills, which intensifies the exposure to several different types of addiction (Gregoire 2014).
It is nevertheless pointed out in the article, that nor Hormse’s nor other researchers studies on the matter of social media addiction can be taken as conclusive evidence, that it is a difficult subject and that it depends on ones definition of the word addiction. (Gregoire 2014)

Yet another Huffington Post article discusses whether or not we actually are addicted to social media, or rather if we are addicted to ourselves. (Brewer 2013) asks the question of what it is exactly that we are addicted to. Looking at studies in neuroscience by researchers at Harvard University, one might actually conclude that is ourselves we are addicted to and not the Internet or social media per say. The research was done in the way that test subjects were put under an fMRI scanner and given three choices to choose from, each associated to a monetary payoff. The results showed that participant on an average lost seventeen percent of potential earnings, in order to talk and think about themselves. They were essentially willing to give up money in order to talk about themselves. The part of the brain that is associated to addiction also light up as the participants were speaking of themselves.

Social media addiction is discussed in a similar way in an article by Stone (2012) where addiction is defined as a “persistent, compulsive use in the face of increasingly negative life consequences”. The article discusses the problem of defining the term social media addict and the fact that it is nevertheless difficult to conclude who might be one or become one. There is a big difference between liking something and constantly wanting something. Thus, the fact that an individual simply enjoys being online and being active on social media does not make him an addict per say. It is when the individual feels a strong need to be on social media, a need so strong that he cannot control, is when one can start talking about the individual as an addict. The author provides the reader with an example of a man checking his cellphone every three minutes over the span of two hours, all the while forgetting each time that his phone in fact was out of batteries. The author also discusses dopamine, saying that there occurs a dopamine jolt in our brains when we receive an email or Facebook notification and that is something that an individual most absolutely can become addictive to, that is the dopamine jolt itself.

The author concludes nevertheless that unlike addiction of substances like drugs, tobacco and alcohol, social media addiction can usually be managed, without an intervention, as long as the individual is aware of the addiction. It is all about setting limits and sticking to them, moderation is the key to a happy and balanced life.

Griffiths (2000) criticizes Internet addiction, saying that there has been conducted very little to prove the fact and addiction and that there is very little empirical evidence to support those claims. Griffith claims addiction to be categorized in to two categories, either passive or active and that the addictive tendencies toward technology can be explained as a form of a behavioral addiction, yet not that it can be defined as an Internet addiction on its own. Nevertheless the author does in fact conclude that usage of the Internet will inevitably grow in the coming years and that if social pathologies do actually exist, that it will be the psychologists who will have to deal with the aftermath of the growth of online activity's such as gambling or even checking messages more obsessively and that that might perhaps result in some form of addiction further along the road.

Davis (2001) refers to Internet addiction as Pathological Internet Use aka. PIU. Davis much like Griffiths (2000) states that PIU is a cognitive-behavioral disorder. The symptoms of PIU are describes as an individual having obsessive thought about being online, a loss of impulse
control and tolerance. Davis (2001) does not use the term addiction due to the fact that the word addiction does not describe a pathological use or abuse of a substance. Davis also states that more research needs to be conducted in order to distinguish between real cases of PIU and those that are only artifacts of questionable experimental design. Davis also points to the fact that there is such a thing as healthy Internet usage and that many researchers tend to focus only on the negative aspects of the Internet, that some researchers might be too quick on defining Internet users as addictive, not looking at its potentials and that the Internet should not be seen as a negative resource in the first place. There exists a healthy usage of the Internet; a healthy Internet usage is when the user can separate Internet communications with real life communications.

5.1.2 Privacy aspects

Popular quote by Jonathan Zittrain: “As they say if something online is free, you’re not the customer you’re the product” Demonstrated in a cartoon by IT blogger. Widder (2014):

![Cartoon demonstrating Facebook as a business.](image-url)
At TED talks in May 2011, Eli Pariser talks about there ones exiting an idea of the Internet as being a platform for democracy and a broader worldview, but that it in recent years has shifted. Pariser says that a social media platform such as Facebook and other sites on the web like Google, is a big contributor to that shift. Looking at a person’s previous clicks, it determines what else you might be interested in hearing or reading about and provides you with links to those pages, at the same time though, it filters out the rest of the information you possibly would be interested in as well. And that narrows your world view.

Pariser takes his own Facebook page as an example saying that he likes to read about both liberal and conservative political parties but since he had clicked more on links to liberal pages, Facebook had removed the conservative ones from his page, only advertising the liberal ones. And that it had done so without his knowledge and consultancy. This, he talks about as a large problem. The problem lays in the fact that individuals now have less control over what they get to hear and read online and that there is an issue of the privacy aspect as well. Google for example looks at 57 different points when determining what to advertise for you. These points include your location, what browser you are using and what computer you are using. The tailored advertisement is a bad thing due to the fact that we only are provided with information on what we might be interested in hearing about and not necessarily what we are in need of hearing about (Pariser 2011).

Schneier (2015) says he believes that eventually much of what the NSA is doing today, i.e. surveillance on the data, will be stopped by the courts as new legislations come, those legislations need nevertheless to be implemented first. The NSA collects do date a lot of data, with emphasis on the words a lot. There is a fitting quote here “When something online is free, you’re not the customer, you’re the product” although the source of the quote is unknown, it was made popular by Jonathan Zittrain.

Nevertheless as data is to date collected, stored and sold along to third-parties by many corporations, not just the NSA, the US State Department does in fact fund a large amount of programs worldwide that work on countering censorship, promote encryption and enable anonymity. The critique made on enabling anonymity however, is that it would be harder to then identify criminals, spammers and stalkers online, and that that is an important aspect of national security anywhere in the world. It is today quite easy to find people that are “anonymized” online, looking at their IP address (Schneier 2015).

The author goes on saying that transparency is nevertheless a vital factor in any open and free society. The author also says that why surveillance online has become a business model and that it has become that due to the fact that it is in fact one of the easiest things that makes money, because of it not having proper regulations. There is a lot of money invested in the value of Big Data. For it to become a change we first need to want that change and for people to want a change they first need to become aware of the issue at hand (Schneier 2015).

The reality is that most social media users do not read the terms of conditions they agree to, nor do they want to or would want to, even if the long and complicated terms of conditions would get shorter. There is nevertheless no doubt that users should read the terms of conditions due to what one can find in them. However companies like Facebook have themselves agreed on the fact that their users do not read them and feel that they can put any form of agreement they want in that text, which can be alarming. The goal with companies like Facebook is simply to sell as much advertisement as possible, since the users themselves
do not pay any money for the service. In this case, your personal data becomes very valuable to the company and the company does exploit that. The idea is also to track the location of the users in order to target them with localized adverts; this is something that than can attract more companies to advertise. This however can seem intrusive, though you are targeted personally. This however just makes the company more powerful. The company does however have the permission to do so, since the users have agreed to the terms of conditions (Grothaus 2014).

A photo posted on Twitter remains the intellectual property of the user but Twitter's terms give the company a "worldwide, non-exclusive, royalty-free license (with the right to sublicense)". In practice, that gives Twitter almost total control over the text and images and the ability to do just about anything with it. The company claims the right to "use, modify or transmit" your photo any way. A lot of the time it really isn't transparent what these agreements mean. People haven't really understood what they have entered into. Often companies will over-egg what they need, and it's a land grab for users' rights and content (Smith 2013).

The most striking example of such a “land grab” can be seen on professional networking site LinkedIn. LinkedIn makes broad claims over users' content, giving it the ability to "copy, improve, distribute, publish, remove, retain, add, process, analyze, use and commercialize content, in any way" LinkedIn applies this claim not only to users content, but also all data, concepts or even ideas passed through their service (Smith 2013).

Facebook can transfer or sub-license its rights over a user’s content to another company or organization if needed. Facebook’s license does not end upon the deactivation or deletion of a user’s account, content is only released from this license once all other users that have interacted with the content have also broken their ties with it for example, a photo or video shared or tagged with a group of friends (Smith 2013).

Conti (2009) states that the simple fact is that knowledge can be harvested from even the most improbable pieces of information. By simply ordering a pizza online we disclose sensitive information about ourselves and our friends and family. Information is often captured by webspider. With the help of such webspiders, companies get to find out a great deal about your private life.

The author makes the point that it all comes down to trust. If an individual fells like he can trust a web page then the individual will without concern give out information. What one might not know of though, is that the trust one gives a web page, is also trust put to the personnel working behind the web pages. It is also important to understand that accidents do happen and that a company at any time can lose your personal information for an unknown reason and to an unknown location. Attacks from hackers do happen and they happen regularly. This results in the fact that we always are vulnerable online. No one is immune.

The fact is that there are many companies who deliberately share information on individuals with third-parties. It is many times part of their strategic business model. If an individual would take the time to read the terms and conditions, one would discover that there are in fact wordings that allow it to take place (Conti 2009).
The truth is that your personal information can at any point in time be hacked. There are many hackers out there, who know how to get to the information and how to use it in the best way. These are intelligent people with many connections who have the means to hack large volumes of data. It also has no meaning whether the information is stored on your personal computer or whether it’s stored on a company’s web-based system. The matter of fact is that hackers most often do not get caught and even at the times that they do, the punishment is very low. A hacker in Romania in 2011 was for example only convicted to a total of 3 years in prison after making a big fraud on eBay. To catch more hackers’ better security policies need to come in to place as well as better risk-based detections in systems (Jakobsson 2012).

It is nevertheless commonly the users themselves who are the biggest security risk enablers. The common individual posts a lot of personal information online that most likely should never have been posted. One puts himself in risk even by simply browsing the web. It is highly important for users to understand that, so that no surprises occur if one gets any data hacked. The users most often put too much trust in the organization online that provide services for them. However, by policies these companies are first and foremost supposed to protect themselves and not their users. It is our social nature that makes us vulnerable. We need to become more educated on the subject. Online companies and social media sites want people to use their services and create many exciting offers to draw people in. Social media sites have nonetheless always been exposed to several problematic risk factors, like spammers, phishing and hackers. It therefore becomes our responsibility to think twice about what we do and what we write on these sites and to what extent we can trust the service providers. It is important to always question the security aspects and not give out sensitive information. If we start to question the providers more, they will have to start providing us with better ways of keeping our data safe (Jakobsson 2012).
5.1.3 Social Media

Facebook is here taken as an example of the growth of social media throughout the years.

Though there is an obvious growth in the number of active user, the peak at which the numbers of active users grew the most was in the year between 2010-2011, with a growth of 150 million users. The number of active users in 2013 was an astonishing 1.11 billion. Nevertheless the growth of active users between the years 2012-2013 was only 50 million. That is a decrease of 100 million active users in growth (The Associated Press 2013).

Active users:

500 million — July 2010
608 million — End of 2010
750 million — July 2011
1.06 billion — December 2012
1.11 billion — March 2013

The international growth of Facebook is astonishing as well. The growth is nevertheless associated with when and where Facebook became available to the public. As it became more available, the growth of active users increased. As an example, a large growth occurred in the year 2008; this is nevertheless associated to the fact that it was that year that Facebook launches translated versions of the site in Spanish, French, and German.(Social Times 2008).

![Figure 2: Growth of active users on Facebook.](image-url)
5.1.4 Terms and Conditions

The following is an observation and summary of the documentary film “Terms and conditions may apply”.

In the documentary film "Terms and Conditions May Apply" by Hyrax Films (2013) the many terms and conditions we daily accept online are discussed. The movie makes a point on just how important it is for everyone to understand what exactly they are agreeing on and what the terms and conditions we agree on really mean and their consequences. In the movie we get to see various scenes from courts in the US where the terms and conditions are questioned by court, we also see management from different companies such as Apple defending their online terms and conditions. The court asks a lot of questions, for example how many people actually read the terms and conditions and how the managers can know that people are fully aware on what they sign up for or agree to, we also get to see that when the managers aren't avoiding the questions all together the answers are very skeptical, for example that people need to click that they have agreed to them, nevertheless the court is not satisfied with those type of answers, claiming that the managers have no way of knowing if someone has actually read them before clicking the agree button.

The managers also state that they try and make the text short and in plain English, however the reality is quite different as the terms and conditions are written in small font and in all caps, that is a very uninviting text to read says typographer Brian Lawler. The truth is that it would take a person a full month of work, every year, to read through all the terms and condition that one normally agrees to. This type of language is found almost everywhere online, i.e. on LinkedIn, Google, Facebook, YouTube etc. And what most of them in the end say, simplified, is that they can take everything you post online and all information about you forever. In fact it was brought to light one day on a news report in the US that the terms and conditions on Instagram also stated that one agrees to the fact that Instagram may and can sell and post your photos without any compensation to you. The different committees also state that it is clearly a growing problem.

It is perhaps the idea of the general public that it is a sort of a standard form, that does not really apply in real life, yet the terms and conditions are very real and they do by all means apply says Harvey Anderson, vice president at Business Affairs and General Counsel, he states that it is a valid contract.

In the movie we also find out that the company Game Station one day as a joke put in their terms and conditions the right to claim ones immortal soul and though that was just a joke, it should make you think what other more serious terms and conditions are stating.

Further along in the video we find out that the AT&T Privacy Policy states that they can use your data to investigate, prevent or take action regarding illegal activity. Though it sounds as a good condition over all, it is important to understand what it really means and that is not only that your safety is taken in to consideration but that you can be monitored as well. As an example we get to find out that a person on AOL that online searched for words such as, murder, wife killer and decapitated photos, got suspected on planning a murder on his wife. It later turned out that this person was a writer for a crime TV show, and his wife is to date doing very well indeed. This was shown to point out the fact that you truly cannot actually
ever feel safe online and that a harmless individual can become a suspect and that this in no way is right. Thought we like to feel secure and know that the police can prevent crimes, one can not only look at a person's search records online, due to the mistakes that can occur, that in a negative way affect innocent people.

Eric Schmidt, CEO at Google points out the fact that it many times is not the decisions of the managers of different companies, what to put in the terms and conditions, but that is many times are political decisions. In the video the growth of Big Data is also discussed and companies like Acxiom are mentioned as examples of companies that people aren't aware of but that hold personal data on a very large amount of individuals, information such as, what political stand you have to what kind of a dog you have. At the end of the video Sherry Turkle, Prof. In Social Studies of Science and Technology at MIT, points out that the general public is waking up slowly and realizing the problems of online privacy, but that it probably is a couple of years too late. At the very end of the video we also find out that there are no good regulations to date on the various terms and conditions.

5.1.5 Example

As an example of how Terms and Conditions actually looks like online, the following example is presented:

Twitters Terms and Conditions:

- Is 7145 words long
- There are also Terms of Conditions within the Terms of Conditions
- The Privacy Policy, is on its own conducted of 5976 words more

Terms and conditions:

“Basic Account Information: When you create or reconfigure a Twitter account, you provide some personal information, such as your name, username, password, and email address. In some cases, you may be required to provide your phone number, for example, to use Twitter via SMS or to help us prevent spam, fraud, or abuse. Your name and username are listed publicly on our Services, including on your profile page and in search results. Some Services, such as search and public user profiles, do not require registration.”

“Additional Information: You may provide us with profile information to make public, such as a short biography, your location, your website, or a picture. You may provide information to customize your account, such as a cell phone number for the delivery of SMS messages. We may use your contact information to send you information about our Services or to market to you. You may use your account settings to unsubscribe from notifications from Twitter. You may also unsubscribe by following the instructions contained within the notification or the instructions on our website. We may use your contact information to help others find your Twitter account, including through third-party services and client applications. Your privacy settings control whether others can find you by your email address or cell phone number. You may choose to upload your address book so that we can help you find Twitter users you know or help other Twitter users find you. We may later make suggestions to you and other users on Twitter based on imported address book contacts. You can delete your imported address book
contacts from Twitter at any time. If you email us, we may keep your message, email address and contact information to respond to your request. If you connect your Twitter account to your account on another service in order to cross-post between Twitter and that service, the other service may send us your registration or profile information on that service and other information that you authorize. This information enables cross-posting, helps us improve the Services, and is deleted from Twitter within a few weeks of your disconnecting from Twitter your account on the other service. Learn more here. Providing the additional information described in this section is entirely optional.”

“Tweets, Following, Lists and other Public Information: Our Services are primarily designed to help you share information with the world. Most of the information you provide us is information you are asking us to make public. This includes not only the messages you Tweet and the metadata provided with Tweets, such as when you Tweeted, but also the lists you create, the people you follow, the Tweets you mark as favorites or Retweet, and many other bits of information that result from your use of the Services. We may use this information to customize the content we show you, including ads. Our default is almost always to make the information you provide public for as long as you do not delete it from Twitter, but we generally give you settings to make the information more private if you want. Our Services broadly and instantly disseminate your public information to a wide range of users, customers, and services. For instance, your public user profile information and public Tweets are immediately delivered via SMS and our APIs to our partners and other third parties, including search engines, developers, and publishers that integrate Twitter content into their services, and institutions such as universities and public health agencies that analyze the information for trends and insights. When you share information or content like photos, videos, and links via the Services, you should think carefully about what you are making public.”

“Location Information: You may choose to publish your location in your Tweets and in your Twitter profile. You may also tell us your location when you set your trend location on Twitter.com or your computer or mobile device sends us location information. We may also use other data from your device to determine location, for example, information about wireless networks or cell towers near your mobile device, or your IP address. We may use and store information about your location to provide features of our Services, such as Tweeting with your location, and to improve and customize the Services, for example, with more relevant content like local trends, stories, ads, and suggestions for people to follow. Learn more about Twitter’s use of location here, and how to set your location preferences here.

Links: Twitter may keep track of how you interact with links across our Services, including our email notifications, third-party services, and client applications, by redirecting clicks or through other means. We do this to help improve our Services, to provide more relevant advertising, and to be able to share aggregate click statistics such as how many times a particular link was clicked on.”

“Cookies: Like many websites, we use cookies and similar technologies to collect additional website usage data and to improve our Services, but we do not require cookies for many parts of our Services such as searching and looking at public user profiles. A cookie is a small data file that is transferred to your computer’s hard disk. Twitter may use both session cookies and persistent cookies to better understand how you interact with our Services, to monitor aggregate usage by our users and web traffic routing on our Services, and to customize and improve our Services. Most Internet browsers automatically accept cookies. You can instruct your browser, by changing its settings, to stop accepting cookies or to prompt you before
accepting a cookie from the websites you visit. However, some Services may not function properly if you disable cookies. Learn more about how we use cookies and similar technologies here.”

“Log Data: When you use our Services, we may receive information (“Log Data”) such as your IP address, browser type, operating system, the referring web page, pages visited, location, your mobile carrier, device information (including device and application IDs), search terms, and cookie information. We receive Log Data when you interact with our Services, for example, when you visit our websites, sign into our Services, interact with our email notifications, use your Twitter account to authenticate to a third-party website or application, or visit a third-party website that includes a Twitter button or widget. We may also receive Log Data when you click on, view or interact with a link on our Services to a third-party application, such as when you choose to install another application through Twitter. Twitter uses Log Data to provide, understand, and improve our Services. If not already done earlier, for example, as provided below for Widget Data, we will either delete Log Data or remove any common account identifiers, such as your username, full IP address, or email address, after 18 months” (Twitter 2015).
5.2 Interviews

The results generated from the questions focuses on the respondent insight in what happens with their data once posted and on their knowledge and understanding of regulations online as well as their potential obsession with social media and therefore potential lack of interest in privacy aspects.

The interviews were conducted continuously during a period of two weeks, were sixty two respondents were asked two questions regarding their Internet usage and online privacy. As explained in chapter 2.5 the sampling of the respondents was a convenience sampling. That is that the chosen respondents were available by virtue of accessibility. The interviews were conducted on site where the respondents were found, that is, in school, at work and on spare time. The interviews took place one on one as it also was important for the respondents not to be influence by anybody else’s thoughts or responses. The respondents consisted of forty percent males and sixty percent females. As stated in chapter 2.3 the respondent were in the ages between twenty four and fifty two in regards to not making a point of there existing a potential divide in generations. For this thesis it was empirical not to make a conclusion on whether or not there is a divide between generations in regards to Internet usage, but rather to understand the mindset of Internet users per say and their understanding of online threats.

The importance of asking the questions in the same way to all respondents is stressed in chapter 2.3 as is the importance of objectivism so that one does not reflect one’s own views and thought about the subject at hand. The respondent were also given the opportunity to freely comment on their answers to the questions which gave way for interesting observations. The respondents’ body language and attitude toward the questions was also noted in the analysis.

5.3 Questions

The questions were as following:

- Have you ever read the Terms and Conditions?
- Are you ok with having your personal information stored and sold to third-parties?

5.4 Positive Outcomes

80 % of the respondents answered that they in fact are not ok with having their personal information stored and sold to third-parties.

52 % of the respondents stated that they had in fact read the terms and condition the first time the logged on to the page.
65 % stated that they would happily read the terms and conditions if in fact they were much shorter and written in a more “friendly” font and size.

80 % would happily obtain more privacy online.

5.5  **Negative Outcomes**

48 % of the respondents answered that they have in fact never read any terms and conditions before accepting them.

60 % made the comparison of their information being stored by the organization providing the service, similar to the experience of a hacker getting hold of their information and using it in a harmful and unknown way.

32 % of the respondents stated that if you are heard online you exist. Commenting on the importance of being active on social media as one otherwise would not be part of the “important community”.

20 % stated that they had no interest in privacy issues and did not care to know what happens with their information or what type of data was collected and how it was used or whom it was sold to.
6 Analysis

An analysis is conducted looking back at the theoretical framework and the empirical study. The headlines for this chapter represent the two research questions of this paper presented in chapter 1, as they are here examined in detail alongside the results from the empirical study. This analysis forms a basis for a discussion on the hypotheses presented in chapter 4.

6.1 Does the use of social media have a negative impact on individuals’ desire for online privacy?

Concluding whether or not social media has a negative effect on individuals’ desire for online privacy; one must take into consideration many factors. Research on Internet Addiction Disorder aka. IAD, presented in chapter 1.2 and 3.5 reveals that a long-term Internet addiction has negative effects on an individual in both psychological and neurological matters. The research proves that the disorder contributes to the brains structural abnormalities and reduced grey matter in the brain. These abnormalities are prominent factors in several side effects, for example reduced impulse control. The research on structural brain abnormalities is nevertheless still very new and the researchers themselves admit many factors that need to be taken with consideration in the analysis of the study. As all participants have been male and were young at age. In the early stages of adulthood many changes occur in the brain as it is developing, as such one must note that the abnormalities in the brain might change over time, whether they become more or less prominent.

The psychological abnormalities show themselves in matters of the individual becoming less social outside the cyberspace, as the individual becomes disassociated with people around him. The disorder has been compared to the abuse of drugs or alcohol as it is a strong abuse of a substance. Researchers speak of individuals addicted to the internet to be unable to quit, due to the Internet’s power of “hooking” the user. In chapter 5.1.1 a dopamine jolt in the brain is examined as researchers claim that the response we receive from others online, as we post a picture or write a blog post, is as powerful as taking another line of cocaine or a fourth glass of wine. In a similar way to a drug, alcohol, or tobacco addiction, we receive a jolt of dopamine as we receive a nice comment online.

The dopamine jolt is supposedly so dominant that we lose control and stop considering the hazards of taking more drugs or in this case writing more information online and spending much more time online than normal. The dopamine jolt lest the brain know that what we just did was a good thing, that it was nice and worth doing again. As with drug abuse, it is said that online activities such as gambling, chatting or even posting text on social media becomes more addictive the more we do it, which makes it all that more difficult to quit or to stop and consider the negative effects. It is of course nonetheless not applicable to all individuals as some are more prompt to take a drug substance and some are not. It does nevertheless take a lot of self-restraint not to continue to be online and post information on ones personal life, equal to the restraint of not taking another line of cocaine as you have taken the first one. One can of course never generalize people claiming that what one person does another one will do as well, when put it the same situation. The dopamine jolt is nevertheless a proven fact and we do feel a sense of self accomplishment and joy as we receive positive responses on the things we do online.
As one nonetheless is prompt to become addicted to the Internet and to posting personal information on social media, one also does not care to consider the hazards. As such, the online privacy matter takes a backseat to the joy of being online and posting information and pictures.

It is nevertheless not because the individual does not care about the privacy matter. Though some do, as presented in chapter 5.5 there are those who simply do not care to know of what they sign up for as the simple being online is of great importance to them and they are prepared to accept any given terms and conditions.

Looking back at the results in chapter 5.5 of the empirical study, thirty two percent of the sixty two respondents had answered that it is highly important for them to be seen online and to be active online as that is an undoubtedly important factor in their day-to day life. The respondents showed no interest in finding out what terms and conditions they were accepting online. Shrugging their shoulder when answering the question on whether or not they were ok with having their information online stored and sold by the company to a third-party, it became evident that the importance of accepting the terms and conditions in order to be able to post the information and share it with others, was so very important to the respondents that they nor wanted to read the given to them terms and conditions, nor would they not have accepted them if they had read them.

These results are well fitted with the research presented in chapter 5.1.1 as they show that the dopamine jolt is so strong, that the hazards of the addiction aren’t taken in to consideration as the individuals receive good feedback online and become happier individuals as they post information about themselves. It is the psychology of wanting to belong to a community and following the group regardless of the consequences.

Mankind is by nature prompt to want to belong to a group or a community as it strengthens our own being and makes us feel as we are part of something bigger. Social media sites have many great offers, the biggest being that it is free. As illustrated in chapter 5.1.2 though, nothing online is ever as free as it seems, though we are paying for the services as we pay the companies with the information we provide about ourselves. As presented in chapter 3.6 information is today valued as a high commodity and it has potentials of being exploited in a numerous different ways, depending on who is handling the information and the end-purpose. The common individual’s knowledge is restricted when it comes to knowing what happens with the information. It is nonetheless currently impossible to make someone read the given terms and conditions unless the individual has the need to do so himself. The only way in which it can be assumed that the individual has read the terms and conditions or not, is if he accepts them. As presented in chapter 5.1.4 the providers and managers of these social media sites are fully aware of the fact that there aren’t many people who read the given terms and conditions and are able to put in a lot of potentially hazards policies in them that may have negative consequences on the individuals’ online privacy.
The common individuals behavior on social media can thus have a negative effect on the privacy matters, as we deliberately are prompt to give our privacy away, not taking in to consideration what might be written in the given terms and conditions.

Though thirty two percent is a high percentage, the empirical study of the qualitative interviews presented in chapter 5.2 has its weakness. All of the respondents were located in the same geographical location. It is thereby difficult to make a claim that respondents in a different geographical location would have the same answers. The strengths of the research is nevertheless the fact that the respondents did not only represent one single age or gender group, as both genders and different generations were presented.

The geographical location plays a substantial contribution to the analysis. In chapter 5.1.3 we can note that the growth of social media is based on the fact that the service providers each year had launched and translated the social media site in different countries. The amount of active users differentiates nevertheless depending on the geographical location. It is therefore important to note that as individuals located at one geographical point have been socializing more on social media, the number of active users is far fewer at another location. This has of course to do with our life styles and of historical factors on how much we use the Internet in our day-to-day lives, as some countries provide very young student with personal computers early in their education and others do not.

As negative as the outcome of the thirty two percent of individuals not taking the terms and conditions online in to consideration is, equally positive are the results of the research presented in chapter 5.4, as eighty percent of the respondents had answered that they had not been ok with having their personal information stored and sold to third-parties. Fifty two percent had also answered that they in fact had read the terms and conditions online at one point in time. Thought the respondent had commented on the fact that they had not perhaps read all of the information provided to them, they had in fact browsed through them, reading one or two sentences on what kind of terms they were accepting. This is a positive outcome in the sense that some individuals make some precautions online. Knowing is half the battle won when it comes to reading the terms and conditions as some of the things that are written in to the terms and conditions are in fact hazards to our personal life as presented in chapter 5.1.2 and 5.1.4. The reality is also that those terms and conditions are written by lawyers for lawyers and are there to protect the company and not you.

Unfortunately the terms and conditions are often very difficult to read as explained in chapter 5.1.4 and presented in chapter 5.1.5. As they are written in “unfriendly” to read fonts and sizes. Often written in all caps and being very long, users are not willing to take the time to read them. As presented in chapter 5.4, sixty five percent of the users would in fact be very happy to read the given terms and conditions if they were written in a different way. Many times companies also rely on cloud services when it comes to the storage of data, this data includes all of the users’ data and the cloud services are run by third-parties. It is due to factors like these that make the social media sites themselves hazards to the common individuals online privacy, as that privacy is sold to third-parties.
There is nonetheless a prominent paradox in place in the results of the empirical study, as the same individuals that have stated that they were not ok with having their personal information stored and sold to third-parties were the same respondents that nevertheless were active online on social media sites and that compared the social media sites usage and misuse of their personal information to hackers.

One has to remember that thought social media sites are lucrative services, the programmers of these sites, the managers and third-party companies are viewing these sites as a business. A commercial company will always want to make more profit and cut costs. Obtaining information on potential customers from social media sites is an easy and cheap task, and it is thereby the question of profit that is of concern for companies and not the common individuals’ privacy.
6.2 What hazards does the lack of regulations on Big Data have on online privacy?

As stated in chapter 3.4, online terms and conditions are written by lawyers for lawyers. As then presented in chapter 5.1.4 we find out that anything is possible in regards to the terms and conditions we find online, as the company Game Station for a limited time, once wrote in that they would gain access to your immortal soul. Though this might seem funny and not at all serious, it does show just what companies are able to write in to their terms and conditions, completely legally. Privacy policy often states that they can use your data to investigate, prevent or take action regarding illegal activity. As mentioned in chapter 5.1.4, one might think that these policies are there to protect us and indeed in one way they are, as we do seek to have privacy online. As shown in chapter 5.4 eighty percent of the responds had said that they happily would like to obtain more security, this is also evident in the theoretical framework and empirical study as much research have shown that we might not read the given terms and condition but that we nevertheless want to be secure online, protected mainly from hackers. The privacy policies nonetheless also oppose threats to our privacy online, as all data online is stored and analyzed by either the service providers themselves or buy external third-parties.

It is not only the IP address that is saved, though much information can be obtained searching only for an individual’s IP address. Information such as what kind of computer one uses, what sites one visits and one’s geographical location. The information stored is much greater than that of an IP address though. Every search query, post, like, comment, image, video and click is saved, stored, managed and if necessary the information gained from these activities, is also sold. It is the lack of regulations that enable organizations to obtain this kind of information and store it for an indefinite period of time.

The hazard of information being stored for a longer period of time is big, since it provides hackers to obtain large volumes of sensitive data at any point in time. What is not realized yet by many large-scaled companies is that their own data consisted of all online transaction; contracts and password are in danger alongside their customers data. As stated in chapter 3.6, hackers are very intelligent people. Weather they operate alone or in groups they have many connections, often a lot of money and the capacities to come over large volumes of data from virtually any organization or individual.

As clarified in chapter 3.2, the data collection happens invisibly and most likely without the common individual’s knowledge or understanding. In the chapter there also occurs a discussion by researchers on the fact that Big Data in many ways has become a question of ethics. Though the lack of regulation bring with them many ethical aspects. As there in fact are many encryption techniques and methods that protect data, for example the method of ReadandRemove that removes the data from storage after being read, not many organizations and companies are adapting these methods. It is the ethical aspect of right and wrong that is the main issue.
The question of regulations will always be a problematic factor. A passed law and regulation can change fairly quickly depending on the government at hand. As stated in chapter 1.5.4 the matter of data collection is by all means necessary, a political question. Organizations have no say in what becomes regulated and in what becomes legal or illegal. All political parties have nevertheless different view, and what might be regulated at one point in time can be change four years later. Creating laws that withstand the time is also no easy task as the digital world is constantly changing and new online companies and services emerge. The difficulties of creating proper and time lasting regulations do nevertheless affect online privacy in a very negative way, since organizations are left standing with no clear structure on what to do. It is due to this reason that data collection and storage becomes a matter of moral and ethics instead. To date organizations managers are very unwilling in making any changes. Change is in many ways scary and if one method of data collection and storage has worked, it is difficult to change or to make the effort to change it.

It is when the organizations managers themselves become target to hackers that change start to happen, as the realization of how much personal data is out there and that hackers are intelligent individuals who know how to best use that obtained information, is scary. There needs to occur a shift in the minds of large-scaled companies managers as the web is expanding and programming knowledge is increasing as much education today is done technologically.

The naivety of what happens with our information online is still very much occurring, a shift in the matter of knowledge is nevertheless happening as we are introduced to technology at a much higher rate than before and since much information is available for us online. A pessimistic approach to this fact in presented in chapter 5.1.4 though, as it is discussed that we in fact are starting to wake up and realize the hazards online but that it might already be too late. The collected amount of data that is available on us online and that is currently stored is in an undetermined large scale. Today’s current regulations are as mentioned previously, there to protect the organizations and the common individual, this poses a very large hazard to online privacy. We have no control over what happens to our information. Organizations are able to use the gained data to make predictions on their customers, profile them, sell their information to external third-parties for commercial gain. It does however not stop there. In fact large-scaled organization have possibilities to form public opinions, show sensitive information to third parties and blackmail individual people from the certain websites, and they have the means to do so, due to the lack of regulations.

As stated in chapter 5.1.2 different individuals are provided with different types of information online. Not only does this have to do with the advertisement provided for us, those are generated by usage of such method like web mining. An individual’s search on Google can be very different from another individual. This also depends on the information that organizations have about us. The hazard lays in the fact that this has the possibility to change our political view and our outlook on life. The information is supposed to be personalized under the assumption that we want to have personalized information, yet if able to shift our way of thinking it is no good deed. People need to be able to form their own political views in a democracy and therefore personalized information is very much a hazards’ factor.
7 Discussion

In this chapter a discussion on the three hypotheses stated in chapter 4 is brought forward. Each headline is related to each individual hypothesis and is discussed in the same chronological order as the hypotheses are presented in chapter 4. The discussion has its basis in the theoretical framework, empirical study and analysis. The hypotheses are then either accepted or rejected.

7.1 Social media addiction

As there has been much research conducted on the matter of Internet addiction and social media addiction, it is undoubtedly difficult to reason its non-existence. Accepting Internet addiction as a real disorder, gives way to accepting that the disorder has the potentials to have very negative consequences on both our psychology and our neurological factors like reduced impulse control.

Both the neurological and psychological consequences are contributory in the discussion on online privacy.

The neurological consequences are many, yet reduced grey matter in the brain and abnormalities in the brains structure are the most prominent ones. These consequences should not be taken lightly as brain structural changes is a very serious medical condition and have many consequences on our actions. These types of changes can have psychological consequences as different parts in our brain control different factors. One is for example how impulsive we act and how much restraint we have. A highly impulsive individual with little to non-restraint, will most likely not have any inhibitions of posting personal information online and not considering the hazards that come with it.

Looking back at chapter 3.6 Nunana & Domenico (2013) state that not many people are aware of what kind of terms and conditions they accept online. This also became evident in the empirical study in chapter 5 as 48 % of the respondents had answered they had never read any given terms and conditions online. Looking at the brighter side of the empirical study, a larger percentage of individuals had nonetheless stated that they in fact had read at least once, the given terms and conditions online. However it also became evident that many do in fact disregard the hazards online for the benefits of what the social media sites offer to their customers i.e. staying in touch with old friends and distant family and perhaps most importantly, the ability to post information on yourself and receiving positive feedback with 32 % of the respondents stating the high importance of being visible online and therefore ”existing” and being part of ”an important community”. This is closely related to the research of Hu (2014) who concludes that there are many psychological benefits gained from social media sites. Such as, creating groups, posting information and receiving positive feedback. It is therefore it becomes so very easy to become addicted to the Internet. These benefits act as reward for the individuals making them want to continue their actions.

Whether or not these individuals were stating this due to the fact that they were addicted to the Internet, is difficult to say without making further research with the particular individuals,
one would for example have to use a PET-camera, (looking to Fredholm (2007)), which
would allow the researcher to see the dopamine release in the brain. It nevertheless become
evident that these individuals clearly are hooked on the advantages of the social media sites
and that they do not take in to consideration any hazards that follow.

The psychological consequences are among other that the individual becomes disassociated
with real life as the cyberspace becomes the individuals “real life”. Getting hooked on the
many advantages that services of social media does provide one with, are also hazards as we
get a dopamine jolt each time we win a game on for example Farmville, get a “like” on a post
we made or get a nice comment on a picture we posted. This dopamine jolt is directly related
to our psychology as we are prompt to continue our actions and reject any potential hazards.
This works in a similar way to an alcohol abuse as we feel happier after drinking a couple
glasses of wine, we then want to feel happier and drink more and we do not stop to think
about whether or not the alcohol is good for us.

Social media sites are by all means very tempting. They provide us with the option to stay in
touch with old friends and family, to receive good feedback on the things that we post and it is
free of charge. Though we do want privacy and we do want to be secure, posting information
on ourselves online and disregarding the terms and conditions that we have to accept do
unfortunately not go hand in hand, as many terms and conditions deprive us of any privacy.

The neurological consequences of long-term Internet addiction and the psychological factors
of a dopamine jolt are factors that contribute to us accepting any given terms and conditions,
in order to be able to stay online and continue to post information on ourselves on a frequent
basis and getting positive feedback from our peers.

The matter of whether we might be addicted to the Internet and to social media versus us
being addicted to ourselves is one that has been researched more and more over the past years.
There are nonetheless conclusive evidence in many research studies that show the fact that
there indeed occurs a change in the brain when we are online, gaming, chatting or writing
about ourselves.

Perhaps it could be a combination of the both, we might in a sense be addicted to the Internet
and be addicted to ourselves at the same time. Looking at social media, as we write about
ourselves, we do spend a lot of time online waiting for that positive response and the more
time we spend online the more addictive we can get. Certainly that is similar to other
addictions such as drug addiction where the more of a substance you take, the more addicted
you can get. It is also then that it gets more difficult to stop the addiction.

The matter of there occurring a dopamine jolt, in a way similar to drugs and alcohol, in
regards to the Internet is heavily discussed in both science and popular media. There are
advocates of the idea and there are critiques. Reports do nevertheless show that it is very
much a real matter and that we do get addicted to being on social media due to the dopamine
and that we do disregard the hazard.

Once again looking back at the results from the empirical study in chapter 5 it is clear that
there is a certain percentage of people who clearly have very little to no interest in becoming
informed on the hazard that follow staying connected online. With 20 % of the respondents in
chapter 5.2 stating they simply do not care, (while shrugging their shoulders and smiling).
With the existence of there occurring a dopamine jolt, looking to the findings in chapter 5.1.1
of Prof. Kristen Lindquist (Financial Times 2013), one can conclude that there indeed exists a percentage of individuals who do get hooked on that jolt and that they will continue to stay online and disregard the hazard because it makes them happy.

The hypothesis of if an individual becomes addicted to social media, he does not question online privacy regulation is thereby accepted.

The emphasis is nonetheless on the word if. It is if an individual becomes addicted to social media as he is prompt to disregard any hazards of it and not question any regulations. The question is whether or not we all are in danger of becoming addicted to social media or not? The consequences of a dopamine jolt and long-term Internet abuse are nonetheless two issues that both need to be further examined. People are nevertheless different and as one individual might in fact become addicted to the Internet, another individual might not. There is such a thing as a healthy usage of the Internet and all things are good in moderation.
7.2 Terms and Conditions

The common feel among the respondents from the empirical study is that when information is being stored and sold to third-parties, it feels as if the information is hacked. The feeling is the same of that, that a hacker has hacked all the private and sensitive information and is selling it along to unknown companies and individuals for profit. It is the unknowing of to whom the information was sold to and what type of data, that is the most disturbing one. It also came to light in the empirical study that most of the respondents have in fact read the terms and conditions the first time they signed up but then have neglected to read them ever again. As it is seen in popular media though, the terms and conditions do change and expand from time to time. In fact, the entire terms and conditions can change. Making the comparing of a company like Facebook or Twitter to a hacker is perhaps not what the companies are out for, yet it is very likely that if there is one person who feels that way there might be many more who feel just the same. This should be of concern to companies, though a company cannot grow without the trust of its customers, at least not in the long run.

As has become evident, the growth of a company like Facebook is largely based on the fact that the site is launched continually in new countries. Where it has been active for a longer period of time, we can nevertheless see that the amount of users decline. We can also see that the number of active users (though there are 1.1 billion of the) actually decline in growth over the years. At a peak in the year between 2010 and 2011 with the growth of active users by 142 million in one year to a growth in only 50 million in another year in 2012-2013, it can perhaps be concluded that Facebook reached its peak a long time ago. These numbers are however clearly looking the way they are as Facebook had continued to launch its site in new countries as the time has passed.

Though the empirical study did show that there are those individuals who do in fact not care to read any given terms and conditions, this percentage of people was very low in comparison to the percentage of people wanting to have more privacy online and the respondents expressing that they in fact would read the terms and conditions if they had been written in a different way.

Terms and condition are often written in all caps, they are written in long and complicated sentences and are written in what many users find as an “unfriendly” font. The question is why the service providers do write these terms and conditions in that way? Though the answer has potentials to be very complex as the managers and programmers’ data is equally vulnerable as a common individual’s is in regards to hackers, a more simple answer could perhaps be presented: It is the economy that will perhaps always be a front runner in the issues explored by companies and taken care of first, a company cannot survive without a strong economy, and though it is always important to think of quality and responsibility over quantity and profit, the mindsets of many managers do not work in that way, as many times profit and self-protection is written in to the companies policies.
Much more information is needed for the common individuals who are storing information and shopping on the web. People aren’t nevertheless not as naive as one might think. Most individuals do care about their privacy and would like to know what is written in the terms and conditions. By making the terms and conditions unfriendly to read though, companies deliberately try to make sure that people do not read them.

Similar to the research of Barcelos et al. (2014) in chapter 3.1 it has become evident that individuals’ desire for online privacy and actual behavior online differs. With the respondents comparing large scaled organizations like Google and Facebook’s collection of data to the acts of hackers, many respondents at the same time state not to have read the given terms and conditions online at any point in time. This is also a clear paradox as one cannot seek for privacy when not reading what kind of privacy one actually is entitled to. Building upon the research of Lewis (2000) in chapter 3.1, it is also evident that there is an ongoing power struggle and paradox in large scaled companies as they have obligations to provide some form of security for their customers they need to at the same time make a lot of profit in this competitive market. At is was made evident in the empirical study of chapter 5 making the terms and conditions unfriendly to read is a business strategy that generates profit, due to the fact that it inhibits people to read the given terms and conditions and therefore generates in many active users, though what is actually said in the terms and conditions may not be approved by many of the users.

In chapter 5.1.4 it becomes clear that terms and conditions are written by lawyers for lawyers and not for the users. Looking back at the results in chapter 5.4 it 65 % of the respondents had stated that they in fact would be happy to read the terms and conditions had they been written differently. This does nevertheless differ a bit from the research of Barcelos et al. (2014) as there are those users, and there is a large percentage of them, that would like to have more privacy online and that at the same time are interested in the hazards and the terms and conditions, yet they are prevented to take part of them due to the way that they are written.

As the empirical study has shown people are starting to wake up and see the hazards of posting information on social media sites. Though there are many lucrative factors associated with social media, one being that it is free of charge, we are slowly but safely becoming more and more suspicious of what happens with our data. The question is whether we are waking up to late?

The hypothesis of if a website offers its online services for free, we do not care to read the given terms and conditions, can nevertheless be rejected.

The matter of fact is that most individuals do care; but the complexity and the fact that regulations are often written by lawyers for lawyers make the terms and conditions very difficult to comprehend.
7.3 Big Data regulations

Big Data is undoubtedly something that the society has had to adjust to. A company that is in need to make a high profit is in need to use the services that Big Data is offering. Knowing what potential and existing customers like, what they are talking about, what they dislike, what products they are buying and at what occasions, is highly valued information and undoubtedly important. It is this knowledge that allows companies to sell the “right” products to the right customers. The power of Big Data doesn't however stop there. Along with data mining tools, predictions on what type of products a customer is most likely keen on buying on what day and hour of the day is possible. Predictions that say that a customer is prompt to buy a soda alongside chocolate on a Tuesday afternoon or that a customer is keen on buying more items the day before Christmas are predictions that are now possible to make.

There is also the matter of online organizations like Google, having the power to change people’s opinions and removing people from search engines, as explained in the analysis, which poses many hazards to the privacy and online security of the common individual.

The way that these types of predictions are able to be made is actually very simple. All a store needs is for you to use your credit card or you're store card, and just like that they have all the information about you that they need. Every single search query made on the web is also stored and analyzed. With this knowledge the stores managers are able to among other, send out customized offers to their customers and place products at strategic positions in the store. Online, companies are able to send you customized advertisement and make you feel as though you in fact do want to purchase a product you did not consider of at first. Scary? perhaps, it is nevertheless a very personal matter. There are of course those people who don't mind at all that their information is stored, there are those that are bothered but that continue on shopping with their credit cards any way and there are those that might stop using their credit cards. The issue of the matter is that there are people who have absolutely no idea of the fact that the store is storing and using their credit card information and purchase history for their own benefit, the benefit being a large profit.

There is much that can be done in the sense of informing customers about what happens to their information. An example is to send out a short notification to the customers with clear examples, in plain English, explaining what happens to the data, what data is stored and how it's used. The second problem that this issue faces is the matter of some people not wanting to read the information that is provided to them. This is also the issue with the terms of conditions online as clarified in the previous section of the discussion. The accept button is provided to the users alongside a text stating that it is necessary for the user to read through the text, before accepting the terms and that of course is a good thing. The terms and conditions are nevertheless very complex to actually read. Thought if someone chooses to ignore the terms of conditions and click on the accept button right away, does this individual then not have himself to blame? There are undoubtedly those people that would answer yes to that question. Since the individual chose not to read he has to accept the consequences. In this case the consequences are those that all data of the individual, such as the IP address, name, date of birth, likes and dislikes, comments and photos are stored, used and sold to third-parties.
Then there are those who state that it is exactly this type of sensitive and private information that creates the problem and that whether or not an individual chose to read the terms of conditions before accepting them or not, is not the issue. The issue rather lays in the fact that the information is stored and that it is able to be stored for an undetermined period of time along with the issue of what type of information is stored and that it is that that should not be allowed. The lack of regulations on Big Data, nevertheless enable this.

The issue of security online is clearly a problem as well. Data is never one hundred percent safe. There are hackers out there, and they are very intelligent. If an online hacker attack happens, your information will be lost, no matter who you are. Figuring out what type of information an individual is ok with giving up and what information might seem as too sensitive, is a key factor for creating good regulations. Regulations are nevertheless difficult to create as the web constantly changes and the issue of Big Data becomes an ethical one instead.

With 80% of the respondents from chapter 5.4 stating they would happily obtain more privacy online, one can conclude that the matter of online privacy is nonetheless an important one to many common individuals. The form of privacy that people are receiving online today is obviously not enough for many; nevertheless obtaining personal information on the common individual is highly valued. Expanding on the thoughts of Zwitter (2014) chapter 3.2, it is evident that the collection of data today has become a question of ethics rather than standard regulations. As discussed, the matter of creating long-lasting regulations is no easy task and it is very much a political question.

Looking back at the empirical study of chapter 5.1.4 one can agree on the research of Lafuente (2015), chapter 3.2, on the subject of there existing a fine line when it comes to breaching a common individual’s privacy online. Data is definitely in need of being handled with more care as the amount of possibilities of exploiting the data are growing.

One possible solution to the issue of online privacy though, might be that this type of information should be taught in schools from an early age. Perhaps reading through terms of conditions on different web sites and communities, alongside discussions on the matter, is something that should be mandatory in schools. This is perhaps a solution that would solve at least the knowledge issue in the long run. As student would learn what the terms of conditions actually state and by discussing whether or not the terms of conditions are good and what effect that has on the common individual, student would become very educated in that matter. Knowledge is half the battle won.

This doesn't however change what is actually stated in the terms of conditions nor does it changes managers’ views on exploiting the given data for the purpose of higher profit. Nevertheless, as more education would be provided on the subject, perhaps the attitude towards companies that use long and complicated term of conditions would shift and maybe those companies would lose some of its customers, which in turn would be a sign for them that a change in the terms of conditions is in fact needed.
This is nevertheless a clear paradox, in the sense that the common individual wants to be online, share information and get good offers, yet want to feel secure online and have privacy. These things currently do not go hand in hand, as we give away our privacy by accepting terms and conditions.

**Nonetheless, the hypothesis of the lack of regulations on Big Data, enabling managers to exploit the data in a way that harms online privacy and security, is accepted.**
8 Conclusion

In this chapter a final conclusion is presented alongside the research contribution, method evaluation and suggestions on further research.

8.1 Conclusion

There is a clear paradox in the matter of visibility and vulnerability in regards to social media. We do want to feel secure and private online, yet we do want to share information about ourselves with our friends, post comments, search for offers and information, post pictures and make purchases. Provided for us terms and conditions are nevertheless very complex and difficult to comprehend. A shift in the way that these are written would by all means necessary be very beneficial to the users, and the choice of whether or not to post sensitive information online would become easier.

Social media is nevertheless a business, and the matter of companies making profit is currently the only thing that matters for managers, thus the common individuals’ privacy is not taken in to consideration. Techniques that provide managers with the ability to create more security for their customers are available. The lack of regulations nevertheless enables managers to disregard them. What is stated in terms and conditions need to perhaps be taught from an early age as knowledge is the most important tool in with users are able to protect themselves. A weak online security enables hackers to get hold of large volumes of sensitive information. There is also undoubtedly a risk in becoming addicted to social media; this addiction has shown to make us more impulsive and less prompt to think about the hazards. With Internet addiction being that powerful, the importance of proper regulations in place is that much more important, as the common individual is not able to control his own actions online.
8.2 Research contribution

This research paper aims to be of educational nature for those active on social media. Much current research is made on the risks of social media yet is written in journals with complex examples and methods of research. This research paper aims to have simplified some of that research.

Adding the views of social media users themselves in the research, the research aims to bring forward the importance of the users’ comments. As much of current literature state that users should be examined and taken in to consideration, not much research follows through on that.

8.3 Method evaluation

The method I have chosen has been developed to best suit the purpose of the research. I believe that the qualitative method was the most appropriate for me, in order to be able to get the research questions answered. I do not think that a quantitative method could have brought the depth needed. A negative aspect with the qualitative method is that it can be difficult to replicate and that it can become subjective. I have nevertheless made an effort as to stay objective throughout the entire research.

In the qualitative method, the interviewer also gets to see to the respondents’ body language during the interviews while listening to the tone they speak in, and thus be able to make a deeper reflection of what has been said in the interviews.

The observational analysis on popular media and literature also provided the possibility to make a careful discussion. Through a deep dive in to a subject an opportunity is created to carry out a more detailed analysis.

8.4 Suggestions on further research

The following is a list of points of what could be further explored:

- Would active users on social media continue to use the services if having to pay for it with money?
- Creating a technique making sure the users would have to read the entire terms and conditions, would they still accept them?
- With regulations on Big Data in place, would we see a drop in active users on social media?
9 References


Brewer, J (2013) Are We Addicted to Facebook, or Are We Just Addicted to Ourselves? [http://www.huffingtonpost.com/dr-judson-brewer/social-media-addiction_b_4079697.html](http://www.huffingtonpost.com/dr-judson-brewer/social-media-addiction_b_4079697.html) [06-05/15]


Durieux, B (1989) *Online information in Europe*, EUSIDIC

Facebook, [https://www.facebook.com/legal/terms](https://www.facebook.com/legal/terms) [05-05/15]


Hu, T et al. (2014) The effect of online social value on satisfaction and continued use of social media, *European Journal of Information Systems*


Li, P & Guo, S (2014) Load balancing for privacy-preserving access to big data in cloud, *IEEE Conference on Computer Communications Workshops*

Linoff, G & Berry, M (2011) *Data minig techniques*, Wiley Publications


Pariser, E (2011) *Beware Online “filter bubbles”*, TED Talks, [https://www.youtube.com/watch?v=B8ofWFx525s](https://www.youtube.com/watch?v=B8ofWFx525s) [02-05/15]


Robson, C (2011) *Real world research*, Wiley publication, Third edition


Smith, O (2013) Facebook terms and conditions, why you don’t own your online life, [http://www.telegraph.co.uk/technology/social-media/9780565/Facebook-terms-and-conditions-why-you-dont-own-your-online-life.html](http://www.telegraph.co.uk/technology/social-media/9780565/Facebook-terms-and-conditions-why-you-dont-own-your-online-life.html) [08-05/15]


"Terms and Conditions May Apply" by Hyrax Films (2013) [http://freedocumentaries.org/documentary/terms-and-conditions-may-apply#watch-film](http://freedocumentaries.org/documentary/terms-and-conditions-may-apply#watch-film) [27-04/15]

The Associated Press (2013) Number of active users at Facebook over the years, [http://news.yahoo.com/number-active-users-facebook-over-230449748.html](http://news.yahoo.com/number-active-users-facebook-over-230449748.html) [08-05/15]

Twitter (2015), [https://twitter.com/privacy](https://twitter.com/privacy) [05-05/15]


University of Borås is a modern university in the city center. We give courses in business administration and informatics, library and information science, fashion and textiles, behavioral sciences and teacher education, engineering and health sciences.

In the School of Business and IT (HIT), we have focused on the students’ future needs. Therefore we have created programs in which employability is a key word. Subject integration and contextualization are other important concepts. The department has a closeness, both between students and teachers as well as between industry and education.

Our courses in business administration give students the opportunity to learn more about different businesses and governments and how governance and organization of these activities take place. They may also learn about society development and organizations’ adaptation to the outside world. They have the opportunity to improve their ability to analyze, develop and control activities, whether they want to engage in auditing, management or marketing.

Among our IT courses, there’s always something for those who want to design the future of IT-based communications, analyze the needs and demands on organizations' information to design their content structures, integrating IT and business development, developing their ability to analyze and design business processes or focus on programming and development of good use of IT in enterprises and organizations.

The research in the school is well recognized and oriented towards professionalism as well as design and development. The overall research profile is Business-IT-Services which combine knowledge and skills in informatics as well as in business administration. The research is profession-oriented, which is reflected in the research, in many cases conducted on action research-based grounds, with businesses and government organizations at local, national and international arenas. The research design and professional orientation is manifested also in Innovation Lab, which is the department’s and university's unit for research-supporting system development.