Social business and privacy concerns

Elham Vahid

Master's Thesis
Master of Science in Information Security
30 ECTS
Department of Computer Science and Media Technology
Gjøvik University College, 2013

Avdeling for
informatikk og medieteknikk
Høgskolen i Gjøvik
Postboks 191
2802 Gjøvik

Department of Computer Science
and Media Technology
Gjøvik University College
Box 191
N-2802 Gjøvik
Norway

Social business and privacy concerns

Elham Vahid

2013/11/27

Abstract

Social media is the largest communication channel today, both inside and outside of the business world. The generation born in 1980s and 1990s which is known as generation Y, enjoys and benefits from sharing data on social media to communicate with each other and get feedback. Using collected data from social media assists business processes and development, since it provides new avenues for product distribution and customer analysis. Because collecting online customer's data and analyzing them is a large part of social business, privacy is of utmost concern in this new generation of business. Many privacy and even security issues have yet to be resolved; what level of power do customers hold against privacy invasion, for instance, and how much privacy invasion will customer tolerate. This thesis examines and investigates the potential impact of social media and big data analytic as it relates to new business practices. It analyses the privacy risk associated with using social media as a business tool to both communicate with customer and to monitor customer's online activities. It also highlights the role of privacy awareness, data protection policies, and how a good privacy practice can contribute to trust. Therefore faster business growth and better customer acceptance of social business and online applications would be provided.

Acknowledgments

First of all I would like to express my thanks to my supervisor, prof. Dr. Bernhard M. Hämmerli for all his support, advices and encouragement. Having him as supervisor was a best experience in whole my study life. In addition, I would like to thanks Ms. Catharine Ness from Norwegian data protection authority for her kind participation in my project. I'd also like to thanks my dearest Parinaz who read my paper and provided me with her feedback. Moreover, She was always beside me with her inspiring words. Finally I owe a great thanks to my lovely mom for all her support and her belief on my work. She was the one who gave me motivation all along this thesis study.

Contents

List of Figures

List of Tables

1 Introduction

1.1 Topic covered by project

Security and privacy play a significant role in this new generation of business. Threats like malware, brand hijacking and losing control of information are clearly considered as the known risks. However, a bigger problem, and one that is much less noticed, is privacy and data protection within the virtual world. Big data innovation, also known as the new and inevitable technology, has caused increased concern among consumers using the Internet. However, this technology is designed to improve business and consumer performance, users who choose not to get involved on account of fear of data and privacy insecurity thereby negatively affect business progression. Evaluating and resolving the issues of privacy and personal data protection in order to provide consumers with the desired privacy is necessary; risk assessments will afford productive solutions to the use of social media in this new generation of business processes.
This paper examines the impact of social media analytic, and how customer privacy can increase social business; first, social analytic and its aspects of privacy and second, improving user safety within the business platform.s This thesis puts forth that while the new generation of technology moves closes to a world of virtual business, issues of data privacy increase.
Lack of knowledge concerning security and privacy among users harms business growth. Many individuals avoid using technology altogether for fear of privacy invasion, including but not limited to social media and other online networking services. This thesis highlights the most prevalent challenges associated with using social media as a business tool; creating a safe online environment for users allows for a better business platform[16].

1.2 Keyword

Data Privacy, Data collection, Data mining, privacy concern, Cultural difference

1.3 Justification, Motivation and benefits

Social media is a tool being used in the business platform that conveys the term of social business. This term was first coined by Nobel Peace Prize winner Prof. Muhammad Yunus. The concept is that individuals and communities can interact, form relationships, make decisions, accomplish work and purchase goods. It is underlined by a spirit of collaboration and community, internally and externally[17]. Social media analytic is a type of big data analytic which being used in to aggregate the customer sentiments in this type of business.[18].
This analytic provides significant value of market services within the business world. While social media analytic highly benefits business decisions, it also presents substantial issues of privacy risks to both customers and businesses, both of which should be properly and thoroughly considered[18]
Privacy and data protection have been categorized as weighty current issues, as well as customer trust of online services. Many applications and websites have been created

in order to provide better services to customers, but this does little good if customers strongly doubt their privacy of such services. User knowledge plays a huge part in user activity, which in turn impacts business progression. This paper examines and estimates customer behavior concerning data protection and business progression.

1.4 Research question

In this section we provide some research questions that somewhat limit our area of study. The following questions helped us further define the limits of our research questions and achieve and concise thesis statement. Each question was considered in the study process, ensuring a comprehensive evaluation, answer, and summary.

1. What is the level of privacy risk within current social business?
2. What is the potential risk concerning the use of big data and social media analytic for business decisions?
3. How much privacy protection is required within social business to ensure customer confidence?
4. How can privacy assure users that social media is a safe and beneficial business tool?

1.5 Thesis purpose

The purpose of this study is to highlight data process and protection problems within social business; our research questions were developed in an effort to achieve this knowledge. Our hope is that this thesis will assist in the creation and implementation of an awareness plan that can minimize the potential risk of data mining and thereby increase user satisfaction. Technological advancements such as big data analytic and social media will grow and increase as time goes on; it is therefore an absolute imperative that we adjust our data protection policies and awareness plan concerning consumer concern .

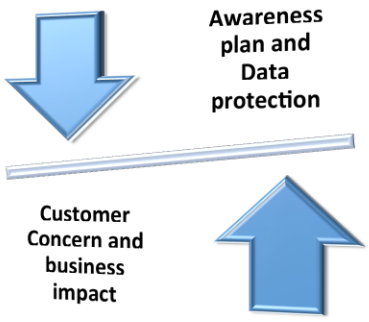

Figure 1: Thesis Purpose

2 Choice of Methods

This chapter describes the methods used to achieve our research purpose, and our step-by-step description of the chosen research method explains the reasons behind these choices. The research questions, is step one, since this is the basis for determining the best suitable research method.

Since the purpose of this thesis is the classify, summarize and grounded perspective on privacy risk within social media analytic and its impact on customers and business, the qualitative method of interviews and literature overview have best allowed us to reach this goal. Our interviews include organizational information, which provide coherent and current data on privacy concerns, including that of data protectors.

Markus Schewaninger[1] has described the reserach model in 3 different level as:[16]

- Explain and understand
- Design and discover
- Test and explore

According to the components of the Schewaninger research model, we focus on understanding, explaining and designing.

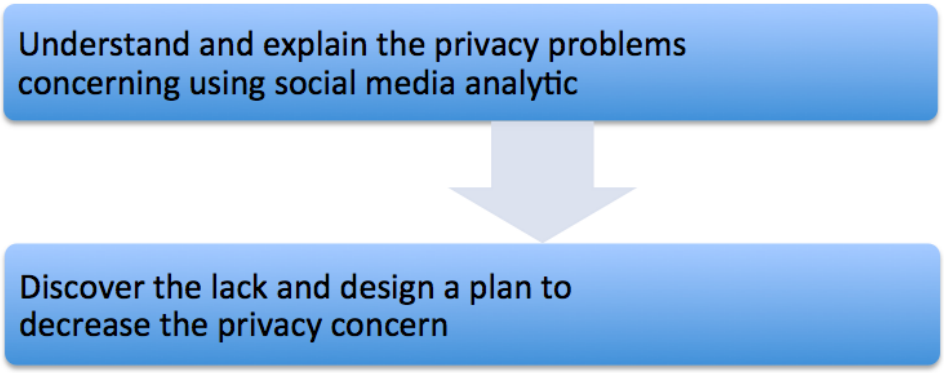

Figure 2: Research Process Level

Although social business and its privacy concerns is a fairly new domain of study, a lot of research has been done on related domains such as social security concern and privacy attacks on social media. Reviewing these case studies[19] allows us to elicit the necessary information and knowledge associated with this real world problem, and thereby assists

[1]Director of the International World Organization of Systems and Cybernetics, and the author of sytematic conceptfor the research process

us in crafting policy solutions and risk management. Questions and concerns raised in our research questions section provide a fairly thorough foundation on which to base our literature review.

We collect extensive data and information relating to the real world privacy problems of big data , etc., which provided a rounded identification and analysis of privacy concern issues within social businesses, and its impact on customer acceptance and usage. Social business is a very broad topic to study. Therefore, our narrow focus on consumer data privacy.

According to the research process described by Leedy we design our Research process as shown in the figure.

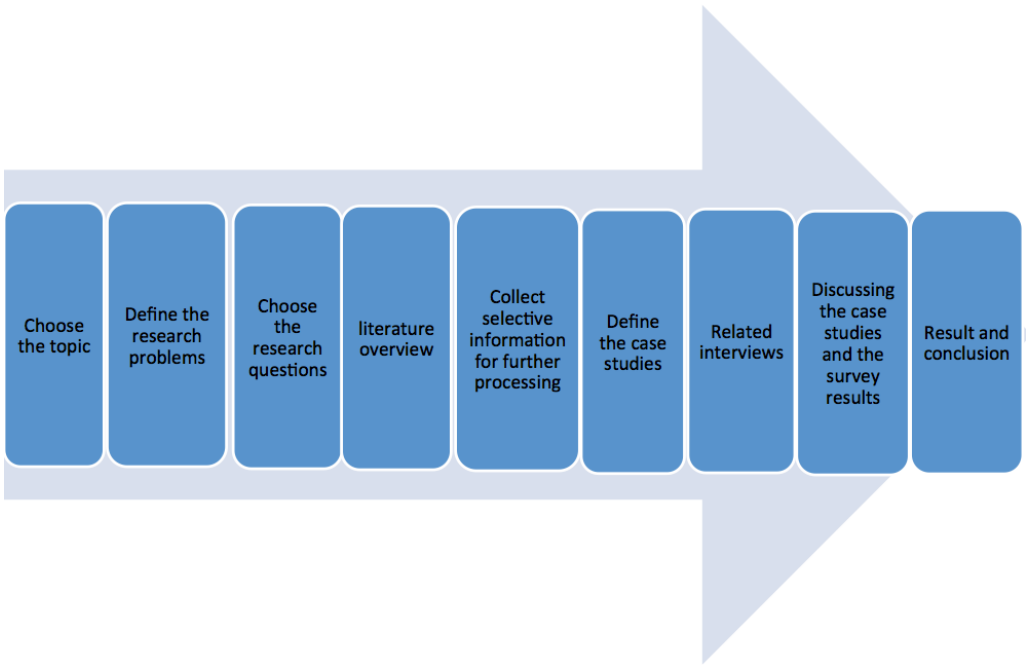

Figure 3: Research Process flow

2.1 Qualitative or Quantitative research methods

According to the research methodology defined by Leedy[20], quantitative research method uses accurate numerical data achieved by survey, statistics and experiments.

The data provided by these approaches need to be analyzed in order to sufficiently answer the research question While, a qualitative method usually uses information gathered through interviews, observations and literature or document about human behavior (social and cultural) and situations [20]. Because the purpose of our reserach is to describe the problem of business, big data and also how data mining impact on customer acceptance, It is necessary that we study business behavior and customer perception in the current business processes.

This qualitative method uses information about privacy concerns from existing documents and experiences. Then it analyzes them in order to obtain the necessary knowledge in order to predict the required policy for future of social business. Moreover, our literature review[19] elicits the required information and knowledge necessary to analyze data collection and privacy risk management.

2.2 Alternative research methods

This thesis is centered on the interplay of user privacy and social media and business. We use the previous research of others on social media to attain satisfying answers to our research questions. This is of course the possible suitable way, which provide us to achieve the thesis study purpose in the limit time. While, Social business, big data and user data privacy are current issues that can be considered and analyzed using inductive approaches[20][21].
Regardless of the limited time the method can vary. Our best approach was to consider a specific social media platform, such as Facebook, monitor user activities and concerns to evaluate consumer perception, and to then examine the impact of stakeholders and companies using the same platform.
A good design questioner and survey also could provide the best avenue for collecting holistic data from both spectrums. More time and researchers are needed to explore both factors with in their entirety and with greater detail.

2.2.1 Methodology Part 2

In mid-term assessment we realized that our understanding of the many interactive components within social business was too broad. We deemed the following components to be the most important, and focused on these:

- Social media or big data analytic
- Data aggregation
- Impact of big data analytic on business decision
- Impact of big data analytic on consumer consent
- Data privacy protection and policies
- Customer concern and awareness
- Customer satisfaction and confidence

By Looking at the research problem option to finalize the thesis purpose we came to the conclusion that the broad approach would not sufficiently cover details on all matters. Therefore, we subsequently narrowed our focus on the following items:

- Data privacy management
- Data privacy protection in Europe union
- Customer awareness in order to protect their privacy
- The Policy and awareness plan framework for customer acceptance and their satisfaction in order to be involved in data analytic.

With regards to our research questions, the second half of our thesis focuses mainly on research questions 1,3 and 4, namely customer privacy, data protection, and data

awareness policy. In the end we analyze the collected knowledge to reveal our protection framework and awareness plan. Because the research problem is still too broad, we divide this to smaller case studies and units of Europe Union and in particular, Norwegian data privacy authority. Using a qualitative method including case study and deep document review contribute us for preceding the research study.
As an alternative using a quantitative research through a comprehensive survey of European social media users to gather accurate values would provide us more accurate value, but it is not an appropriate method in order of time limitation for this study. Rather, we chose to use, in addition to document reviews, short interviews with those using social networks and online interactive websites with a focus on user awareness and confidence. The required information was further substantiated by an interview with the data protection authority in Norway. Our concluding discussion focuses on how policy, awareness, and data protection directives can be effective regarding user privacy protection. We divide the rest of the thesis into 3 case studies:

1. European data protection
2. Norwegian data protection authority
3. awareness

To examine each of these studies, we chose different approaches. For the case of European data protection we used literature overview and legal overview of the European Commission. For Norwegian data protection authority we interviewed a high-level member of big data in the Norwegian data protection authority. For the awareness study we have interviewed several students of the HiG information security program to evaluate the maximum awareness and consumer perception of big data collection and privacy.
To provide a more thorough examination, we collaborated with a student of information security to ensure the thoroughness and legitimacy of a holistic awareness plan.

2.3 Thesis outline

- Chapter 1: Introduction and description of the research problem; research questions
- Chapter 2: The methods used to achieve the research purpose
- Chapter 3: State of the art in Social networking; social business; big data and its known privacy issues
- Chapter 4: Examine the big data risk and its impact on both business and customer
- Chapter 5: Determine the privacy risk on Facebook and twitter and describing the customer perception on privacy
- Chapter 6: Investigation 3 case studies. Data protection assessment in European commission; Norwegian data protection authority and awareness assessment in academic group
- Chapter 7: Discussion and survey result
- Chapter 8: Conclusion and recommendation in order to enhance the business performance and customer consent
- Chapter 9: Future work and case studies for further research

3 State of the art

3.1 Social Media within business

According to the Wikipedia Social media[22] is an interaction media among people to share their ideas or information. Statistic reports claim that more than 500 million people joined social networks like twitter, and a billion joined Facebook, in the last 10 years. Significantly the way of living, gaming, learning and working is changing[23]. This also impacts the business processes.One of the first concerns of enterprises is how employees are using social media with respect to security within corporations, for instance, what they share with others and what information and documents they have access to.This concern is not just about data leakage by employees over the Internet, but about the fact that Social Media is a target for cyberattacks[24]. For example, advertisements on social networks are much more successful than pornography websites for the purpose of malware attacks. Global association for enterprise governance of information technology addresses 5 important potential risks[25]:

1. Viruses/malware
2. Brand hijacking
3. Lack of control over content
4. Unrealistic customer expectations of Internet-services
5. Non-compliance with record management regulations

Although the part of security risk is beyond our study in this thesis. In fact the security impact of social media on business can itself be a research study.

3.2 Social business

Social business is a new business model innovation that has the possibility to be located somewhere between a profit-maximizing and a non-profit organization, existing to fulfill social objectives.[26]. In fact a social business is a business that use social tools and techniqus to become 3 characteristics. These 3 characteristics are[1]:

1. Engaging
2. Being transparency
3. Nimble

Moreover, this new business platform is self-sustainable[26].

Sandy Carter[27]is IBM's worldwide Vice President of Social Business. She is one of the key on social business in IBM. During her conference in May 2013, she predicted that within 2 years, the usage of social media for social businesses will increase by 72%, and that within 3 years business applications will have social media embedded in it[1]. She defines the business worlds concluding 4 parameters:

- Social business
- Big Data
- Business process
- Data Analytic

Regarding risk management, Sandy Carter claims that along with using social business as a new business line, it is necessary to develop a reliable social disaster and recovery plan. Furthermore as we see in the figure, big Data and social media analytics[28]play a main role in social business decisions. While markets start using social media analytics to understand the customer attitudes, interests, and so on, they also convey security and privacy risks to business processes.
Since the social media's abilities will be the main business tool, that make us a motivation to determine and examine the potential of privacy risk which will be increased in next 3 years.

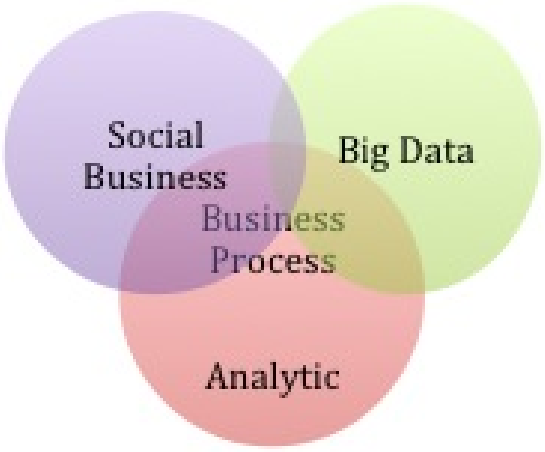

Figure 4: Parameters of business world[1]

Sandy Carter mentions 5 ways convergence matters to corporations[1]:

- The power of social sharing information: expertise and trust
- Value will be created not for market segment, but for individuals
- Innovation is becoming part of corporate
- Social networks are the new production line
- Result requires leadership

With regards to what she mentioned the individuals sentiment and consent are the goal in business, however at the same time the user need to trust the system. They should

accept the business service activities. In this case we see the risk perspective on privacy aspect and data management. Sandy Carter believes that sooner or later if companies want to be in the market competition, they should engage the social platforms in their business. If we assume her perspective view is real then the need of being prepare for threat and risk which can occur through Social business, specifically in big data should be located as a high priority for security and privacy experts.

3.3 Expected business potential of social media in the next 5 years

These days, mobile devices come preprogrammed with social networks like Twitter, Facebook, LinkedIn, and Google+. This is growing day by day. Social media is not just a communications network. It is being used more for business purposes and customer perception.The IBM 2012 CEO Survey revealed that 57% of CEOs identified social business as a top priority, and that more than 73% of CEOs are making significant investments to better pursue and utilize social media[1]. That means 73% of companies are about to deal with privacy concern carries by this innovation. At the same time according to the TRUSTe[1] survey most[11]of consumers are worry on online privacy.

3.4 Major policies that have been created for social media by big companies

A lot of work study regarding Social media hazard probabilities have been done so far, especially in security policy, social network and business asset security. Chris Boudr-eaux, creator of the blog Socialmediagovernance.com[29], creates a policy list over the usage of social Media. In this database, there are policies provided by many brands and agencies[29]. This document helps to clarify the varying points of view that large companies and businesses have regarding the usage of social networking; it also addresses the security concerns of different corporations.

3.5 State of the art in big data and social media analytic

Big data is in fact a terms to un-structured or semi-structured data which companies collect to discover the business patterns[30]. Mostly the data being collected from blogs and social media websites, analyzed, and the values provided by analyzed data being used to assist in business making decisions. This type of big data analytic call social media analytic. The target of using this data analytic is for the purpose of customer sentiment which helps the business process and customer satisfactions[31]. Data analytic can be provided on any type of big data no matter what format of data it has[13]. In fact business organizations utilize this analytic to enhance the performance of their services. In this paper anytime we talk about big data analytic or data analytic we are considering the social media analytic which is one of the data collecting applications. In the meantime, many companies and IT technology providers collect data in order to analyze the value of the data, and these companies sell their results to other companies. The target of this technology is mostly gathering the customer insights in the relation to their trade production line. Regarding to this type of trade, Federal trade commission of United state, FTC is considering and examining the big data impact on companies. It also provide some rules and legals that we will mention them in the next chapters[32].

[1]Global data privacy management company

According to the recent news published on theguardin.com, NSA tool is a good example of big data. This tool collects almost all of the user activities over the internet. NSA provides analysis to collect a huge amount of data for analytic purposes. In particular, it is even allowed to search the body of emails, chat conversations, browse history, etc., which has been claimed that such a tool is being used to protect the United States citizens[2].

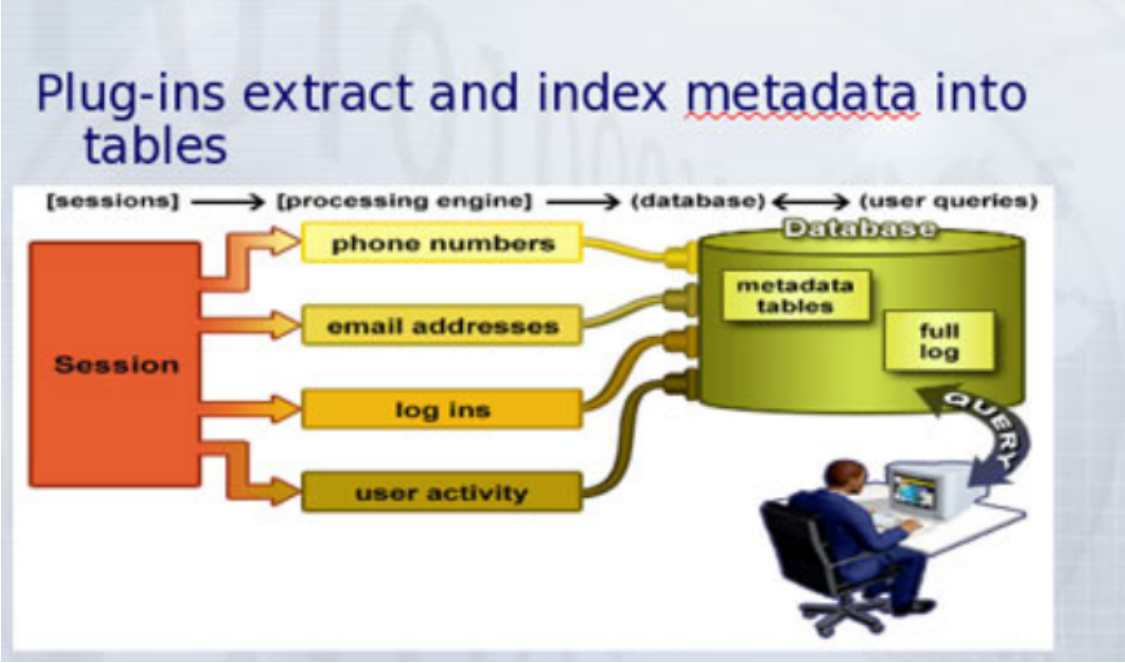

Figure 5: XKS and the online session[2]

The collected data from the session are being stored as metadata package. For example if data is a phone number, this phone number includes the call time duration and and the time call started, etc; for email it includes sender and receiver and location[2]. In the end different queries can be searched from the datasets.

Information Systems Audit and Control Association[33] defines big data as a new technology to help businesses make decisions. The big data approach and the size of its database varies by the targets of each business; for instance, some have bigger or smaller databases to store the data they collect[33]. These kinds of data being collected are used to better understand customer tendencies, thereby predicting more effective ways to improve business services.

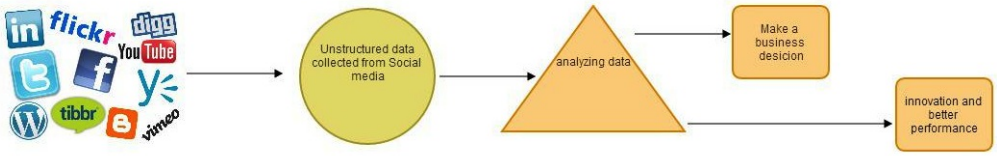

Figure 6: big data process

ISACA[2] also mentions that while many businesses and corporations take advantage of this new technology, big data carries significant security and privacy risks to the business world. For instance, two major risks that should be considered are protecting collected data and at the same time use the collected data in a lawful manner[33]. According to ISACA and COBIT 5[3] framework, 4 aspects of controlling big data should be considered:

- Approach and understanding
- Quality
- Confidentiality and privacy
- Availability

3.5.1 Big data application

Facebook and LinkedIn are two example of big data applications. Once a user registers on either of these websites, data is collected based on the habits and interests of the individual and stored anonymously. Regarding to nation secure law for analytic purpose data store anonymously. For job interests on LinkedIn, for example, the user must supply personal and job related information that will be used by recruiters to locate individuals whose work experience falls into their search terms. In fact this application producing data of how we live and how we do business, who we like to be our friend, what brand we like, etc. From a business standpoint, if we can manage to filter the published data that appears on social networking sites, we can control the security mining of the data[34]. Because companies become more engaged with this social media platform on a daily basis, it is inevitable that in the close future we will become more and more dependent on these sorts of big data applications.

[2]Information Systems Audit and Control Association:http://cart.sammydress.com
[3]A Business Framework for the Governance and Management of Enterprise IT

3.6 Privacy protection level for business and Data collector

According to the European Commission Justice, data collectors are not allowed to collect and store personal data of internet consumers. In fact they should follow the rules and laws. Once a user registers with a social media, they start sharing their personal data, such as identity, photos, geographic location, etc. Although information about individuals is available, that does not give permission to data controllers to ignore user privacy and to collect their personal data. Business holders are attracted to these data for their business purposes. In this case, protection directives should define the laws and rights associated with privacy policies and data protection[35].

Data collectors should clarify their purpose in such data managing processes. Here we mention some laws that have already been determined by the European Commission relating to privacy detection[35]:

- Collecting and managing data is allowed only if it is legally permitted
  In this case the purpose of collecting and managing the user data should be in the domain of determined legals.
- Respect to protection and reply to compliance
  User has the right to sue the company or big data provider; if it is justified as misuse, the data should be removed immediately and the collector reported to the national authorities.
- Cooperation with national data protection supervisory authorities
  Each region has its legals and laws. But if the result of data analytic value will transfer to the area out of European union, the collaboration of the national protection laws should be considered. In fact the protecting of data should be guaranteed.
- Respect specific obligation in specific cases regarding to data protection
  Reliable and effective data management in business processing is a point which should be consider in addition to the data privacy protection. Therefore the data management or data analytic should be processed with respect to legalities. Specifically, data should not identify the user about whom data has been collected.

3.7 Privacy setting on browsers

A possible solution to risk of breach of privacy is setting the browser safeguard. In fact, according to the Wikipedia, privacy enhancement-technology allows and encourages users to have more control of their essential personal data. A good available option is privacy that is secured by the browser. However there are many different browsers and different versions which provide varying degrees of privacy. For instance, Internet Explorer 10 has the following privacy features to enhance data protection such as[9]:

- **Search in private**
  Search in private This feature hides all information related to browser history, passwords, etc. each time the user closes out the browser
- **Do not track header** This options does not collect data about a user's visit while they are browsing. It also blocks third parties from collecting the user's data. This level of protection sometimes limits the user's browsing options.

Regarding browser-based privacy tools, there is also the privacy add-on. This tool is an application that helps personal the browser to ensure more privacy and security. Each browser provides specific add-ons that can be installed and utilized to extend browser capabilities[36]. For instance, the popular browser Firefox produced a specific application that contributes the following privacy protection features[37]:

- **Lightbeam for Firefox**: helps users control the viewer ability of third parties
- **anonymoX**: It makes anonymous browsing possible
- **Ghostery**: Allows users to dictate who track their browser activities
- **Donttrack me**: Allows users to block online tracking

There are significantly some add on applications for Google Chrome, Internet Explorer and other browsers. Some of the applications presented by different companies and websites as privacy add-ons can carry security risks. Therefore it is prudent for users to be aware of what add-ons and installations are downloaded as privacy enhancements.

3.8 User online behavior

The figure bellow is a survey on consumer behavior. This survey is done by some student from university of Salerno. They chose two groups of consumer ICT[4] and non-ICT group; The type of participants is addressed in the appendix. The result in the figure shows that mostly non-ICT or general user do not take action on their data protection. They rarely delete the cookies and almost 40% never read the terms and conditions. However ICT group are more aware but still 28% never read the polices online. In this survey, they stated that some consumer are neutral about their data protection and some feel comfortable to disclose their data. However, it is not discussed if they are aware of big data collecting or not. In this survey it is also mentioned that no-ICT consumers are more concern about their privacy than ICT consumers[3]

[4]Information and communication technology

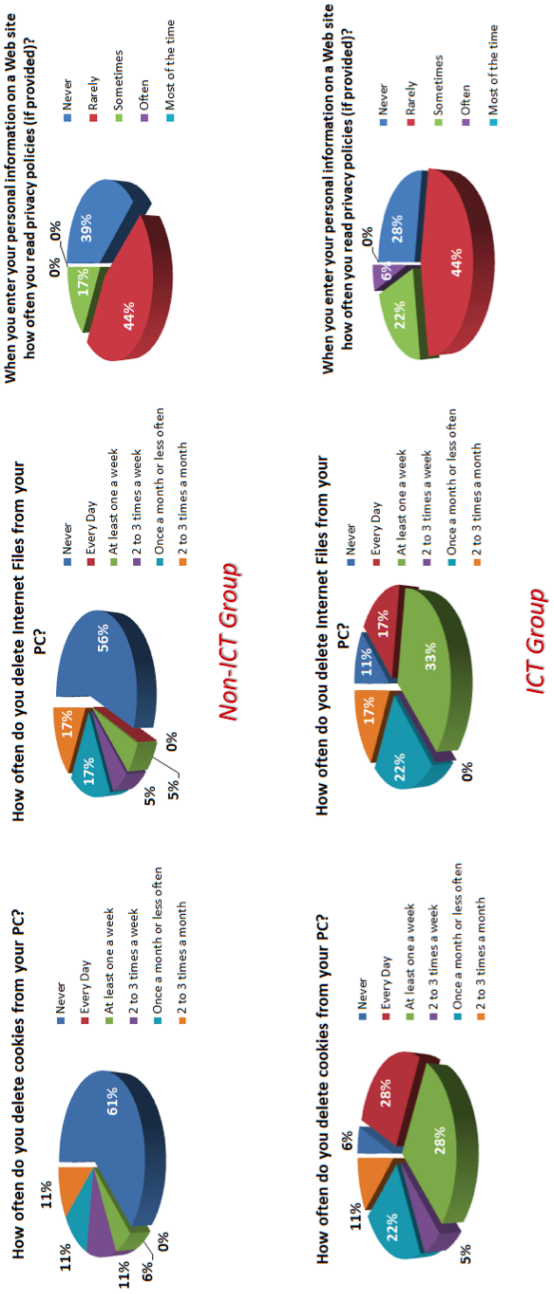

Figure 7: User online behaviord[3]

4 Big Data impact on business and consumer

As we mentioned already in the chapter of state of the art, big data plays an important role in the new generation of business. This technology helps businesses make crucial decisions to enhance their service performance. According to ISACA[1] [25], while big data greatly benefits businesses, it also presents security and privacy risks that need to be considered. Business decisions depend on the analysis of big data; wrong manipulation of this data can result in decisions that are detrimental to the business[33].
One of the major issues concerning big data security is the concern of reliability[13]. In other word how the value of collected data can harm the business process.

For instance, let's consider LinkedIn. Large amounts of personal information is published by the users in order to be used for job demand, yet how can this data be qualified by a prospective employer? Are the users of LinkedIn real? Is the presented data reliable?

Big data is a useful, but if privacy level is low priority in this phenomenon then it make a big issue. Data protection is necessary for big data services, since social media and Google, for instance, monitor and utilize personal data in order to make valuable assessments about customer sentiments. However, this collection and processing of personal data addresses five big concerns[33].The first four concerns impact the user and customer, while the last one impacts businesses and stakeholders.

1. Privacy: policies should adapt to the new technology in terms of privacy protection.
2. Global governance: international law is not adequate enough to sufficiently adjust to the regulatory frameworks of this new technology.
3. Personal data ownership: legal and security commissions should consider the users' rights in terms of controlling their data.
4. Transparency: too much transparency too soon presents as much of a risk to the stability of the personal data ecosystem as too little transparency.[33]
5. Value distribution: reliability and accuracy of businesses impact the value of the business.

4.1 Type of collected data by Companies

Based on a report done in December 2013 by the Federal Trade Commission (FTC), the following points highlight the data clasification that can be collected by trading companies[32]:

1. Product identification
2. Type of customer
3. Each users' percentage of product services
4. Total amount of each product

[1] Information Systems Audit and Control Association:http://cart.sammydress.com

5. User behavior on a company's website
6. User interests and behavior on social media
7. User activity on mobile devices both online and offline

The data generated by Internet communities, social media and Internet networking sites is usually unstructured and needs to be rearranged to fit the frame of the business[38]. Without rearranging, this unmanaged data is considered harmless in the event of an audit or lawsuit[39].

FTC's white paper claims that each company should provide a report describing their reasons for, and the types of, data they collect. For example, if a company collects data about teenagers, they should clarify why they store such information, and how long they store it for.

FTC also asks companies to provide their method of personal data collection, and how they share this data. It is required that companies define their privacy policies and security policies, that customers want to view it[32].

4.2 Big data risk management

Big data is a fairly new innovation to the way that data is stored and used within business process. This is totally different of what we used to as data warehousing. This type of data collection is becoming a main component within the business world. Therefore there are a lot of security and privacy concerns, which has not been solved yet, the resulting privacy concerns need to be solved, and privacy and security risk management should be of high priority in this new generation of the business world.
Big data privacy is now a hot topic, which makes for big discussions between CISO[2] [40]teams, social media providers such as Facebook and Twitter, big data analytic providers, and business corporations.
In the table of risk management we mention some major privacy risks and threats over the big data processing. We obviously can realize that the impact of big data as an interactive component in the social business is very broad. The risk factor falls on, and impacts, both the consumer and the business.
Dirty data and manipulating data are unreliable data, as we mentioned, and negatively impact business decisions. This should be pursued as an entirely separate topic of study and research, since it is too vast to examine in this paper. For the sake of this paper, however, these threats demonstrate the high-risk potential of the aspect of privacy. We will examine and study how the privacy aspect impacts consumers and, accordingly, business progress.

[2]Chief information security officer, https://www.eccouncil.org/ciso

Risk Statement	**Description**
Private and sensitive information leverage for both company and consumer	• Identify telephone number and geographic location for social network users • Assets and sensitive information for corporation
Manipulated data	• Wrong business decision based on manipulated data • Damaged reputation
Abuse of data collection	• Selling data to the intruder and enemies
Dirty data	• Unreal or unreliable information • Low Quality or accuracy This type of data generate false values, which can create disaster for both businesses and customers
Lack of knowledge of privacy agreement in social media	Such agreements on Facebook, Google, etc. often go unread, and are sometimes signed by users with insufficient knowledge or concern
use of datasets from untrusted parties	untrusted parties that can misuse data or manipulate data

Table 1: Risk statement of big data[13][14][15]

4.2.1 Data privacy management on customer side

The fast growth of technology and the role of the Internet in our life have cultivated concern about personal privacy. This concern is growing rapidly, given that life is becoming more and more dependent on the Internet and on electronic transactions. Credit cards, Smart Phones, online banking, email, instant messengers, and GPS satellite are a few examples. Marketers enthusiastically use these avenues to target new customers, thereby contributing to the big data and social media analytic[41].

The birth of big data analytic created privacy and data protection concerns, as more people began using social media and the Internet. The fact that companies collect and utilize users' personal information is understandably disconcerting. What's more worrisome is the fact that many users are unaware of the fact that there are laws about privacy and data protection. This huge issue of online privacy[42] and data collection needs to be thoroughly examined and investigated. The impacts of this concern on social business and business processes will be examined in the next chapter.

According to a recent research survey, Germany has the highest level of data and privacy protection in the world. The graph below "User confidence on their data privacy," compares the confidence level of individuals within various countries. This graph is valuated by the report presented by Warwick Ashford[42].
This graph shows that most users who feel they can trust the social media regarding the privacy of their personal data are from Germany. Most countries do not have a privacy policy for companies who collect user data. Consequently, this leaves users dissatisfied, and reduces the reputation of social businesses.

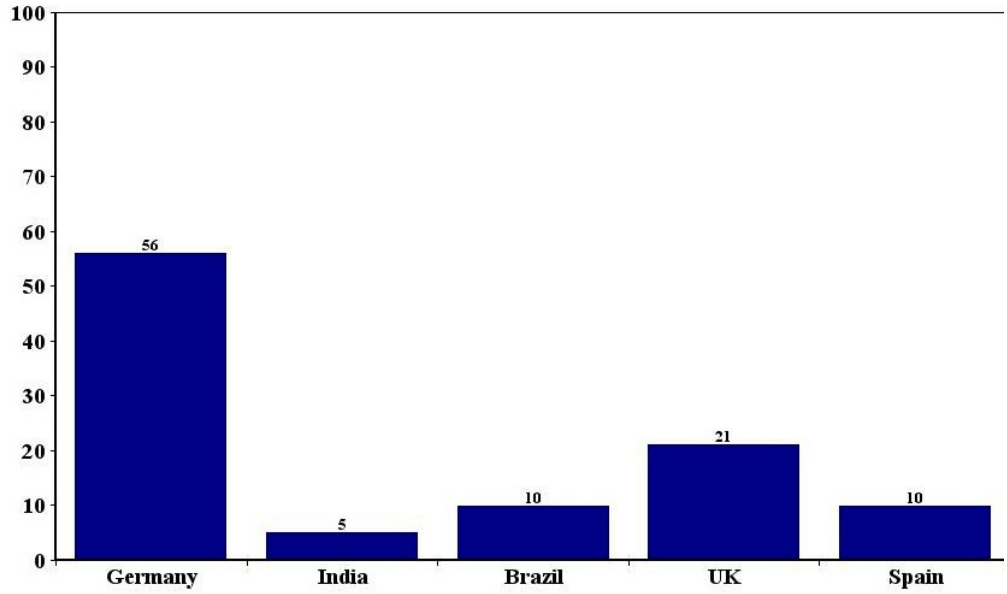

Figure 8: User confidence on their data privacy

A good example of the privacy risk to users is Google. This company anonymously collects user data, and according to recently published news, Google collects data and images sent over wi-fi networks using its street-view cars. This has instigated a new investigation on Google's activation by ICO[3] [43].

4.2.2 Big data risk management on business process

This paper does not evaluate how big data tools and companies such as Hadoop[4] [44]collect data; rather this paper is concerned with how such data storage impacts the safety, businesses performance, user trust and privacy expectations. Furthermore, we examine what might happen in the event that unreliable and unreal data is collected, since the collection of bad data leads to bad analytic, bad business decisions and ultimately business disaster.

Year by year businesses get more engaged with big data and social analytic. However, the question lies in how much they actually trust this technology, and how aware they are of security and privacy risk.
Data leakage and data protection has always been an issue for business corporations, but now big data and its features carries more specific concerns. As long as business corporations are aware of the risk posed by big data they can mitigate the rate of security threats, since customer data and all such sensitive data within the business platform are considered assets.

Here we mention some points that indicate weaknesses in business enterprises in hopes that data collection can become better managed:

- Lack of awareness on data processing within a company
- Lack of knowledge and awareness concerning data processing and the value of the data collected by big data providers.
  With respect to data quality, businesses aim to have a data management officer or a DMO in their organization who can deal with data quality, potential risk, data security, etc. Such specificity, however, is beyond the scope of this paper.

[3] Information Security Officer
[4] www.hadoop.org

4.3 Big data assessment

Concerning protection and privacy by big data collectors, the following concerns should be sufficiently answered by big data providers, and social media providers such as Facebook, LinkedIn, Google, etc[15]:

- When should the collected data be returned or destroyed?
- How will data privacy be controlled by social businesses?
- How much of a budget should businesses use towards data protection in big data technology?
- How much allowance should the government or big data collectors be given to monitor user activity?
- How much user activity can Facebook and other social media monitor?
- How much of a budget can or should be spent on big data privacy and data protection?

4.3.1 Risk mitigation points

- Use the private cloud[13]
- Converged storage[45][13]
- Review and correct all information gathered to ensure reliability[13]
- Ability of the publisher to remove data
- Customer awareness of privacy agreements online.

4.3.2 Big data analytic and privacy challenges

Below are listed four challenges regarding the threats from big data, as introduced by Meiko Jensen: [46].

- Interaction with individuals:
  One of the more significant ways to collected user data is through network traffic. While users may not be aware of this, network traffic provides a level of transparency into user data, through collected cookies, URLs, IP addresses that can track their activities. Arguably, this is a breach of privacy, and as a big data analytic target, it is a challenge if it discloses such individual user data. This has become one of the major issues of privacy compliance.
  According to the law of privacy compliance, users should be made aware of the fact that their personal data will get collected, and also of how the collection of their data will be used. If users decide they no longer trust the big data processes and thereby refrain from continuing to share personal information, the problem still remains that their previously collected data exists in the possession of the big data collectors. Here an issue pops up align to how reliable is that big data services in order to following the law respect to the customers expectation.
- Re-identification attacks:
  This threat is considering linking the databases which are included of personal data of

users, re-identifying the users is almost feasible by attacker. This issue is certainly not acceptable by user[46].It is possible for to re-identify a user who may have stopped sharing information on the internet and perhaps even deleted their social media accounts. In fact by collecting data from different datasets, it is still possible to identify the user. Deleting the name is not enough, because it is easy to put some other information such as geographical location, phone number or even user's interests which can build up the identity of a user again.

- Problems by False data:
  Another major concern is the validity of the data gathered. The big data analytic result is related to the query, which the dataset has been based on that. If the entire dataset has been manipulated or is false in part or in whole, the big data analytic result will be useless. Imagine that datasets are correlated. The type of linkage between datasets should be reliable. For an instance correlating the datasets on IP basis may lead the false result as it is possible to have the same IP address for two different users. The threat to privacy in this terms is from big data query result and make a wrong outcome value on individuals.
- Economic problem issues by big data:
  Big data is becoming such a significant aspect of business that some companies collect and sell both the collected dataset and its analytic result to customers. This significantly effects the economic aspect of businesses, since such confusion and distraction is a good way to destroy data efficiency.

4.4 Privacy impact on business

With regards to what we achieved and studied so far in this paper, we aim now to dig deeper in the scope that how privacy affect on business performance. For the purpose on how consumers can trust more on business and its services, explicitly it is needed to examine the concern point on consumer side. In fact it is highly needed that customer accept the website platforms, mobile applications and online commerce. Business needs to have a good relationship with its customer. Therefore privacy assessment in online activities is very critical to make a progress in business[11].

In order to analyze the current problem, privacy awareness and policies, we focus on data protection breaches, specifically in European states and in particular, in Norway. The next chapters we reveal the privacy assessment and the actions, which have been done so far by European data protection commissions and other data privacy officer. Then we come further to the perspective need of policy, regulation and awareness.

5 Privacy Management

5.1 Social network transaction and its privacy threat

Regarding data transactions over social media, it is essential that information security officers examine and investigate security and privacy threats. Below we briefly examine the current security study about privacy protection, published by ENISA[1] [47], and then analyze the security threats and their impacts.

5.1.1 Who is interested to user's data

Before determining the specific threats of social networks to users and consumers, we first need to outline the groups interested in the data which are published online[32]:

- big data collector
  According to the material covered in Chapter Two, big data analytic and social media analytic are interested in the users' activities. They also sell the value acheive by data analytic to other companies.
- Market and business, in particular Social business
  A goal of social business is being aware of customers' interests and conceptions. By monitoring customer activity, businesses collect data that assists in decision makings such as new production lines, etc.
- National law authorities
  Sometimes the authorities collect data specifically related to a person or group which has been under criminal investigation or a lawsuit.
- Hacker and intruder
  The typical reason hackers and intruders collect data is to abuse user information, which almost always results in disaster.
- company competitors
  This group is usually interested in user data that relates to employees, employers and customers of their competitors, which can sometimes be used to damage reputations.
- Government
  The government may be interested in user data to monitor potential threats to national security.
- Medical research centers
  These groups are interested in monitoring user activities so that they can calculate statistic reports.

[1] European Union Agency for Network and Information Security:http://www.enisa.europa.eu

5.1.2 Google Analytic and privacy concern

Today, Google analytic plays a significant role in business intelligence as a tools to improve business processes and decisions. Business stakeholders and enterprises are highly interested in the data collected by Google analytic. Around the world, the information privacy direction and commission are struggling against the threats that can and have resulted from the Google data monitoring. The biggest concern is centered on how Google uses their collected data, for what reason they collect this data, and how much private data is being collected by Google daily. While Google is free, it can easily get sued by companies and organizations. Below is a quick look at how Google analytic works, and how it impacts consumer privacy and confidence. If such a system is to be used, business intelligence should know and study customer insight, and strive for customer satisfaction.

Google analytic have control on the user activities and can elicit information such as IP address, the time of viewing websites, number of visitors of a website, location of visitors and etc. This possibility is just as easy as opening a Google analytic account and registering some information about the requester and also the information of the specific website that we want to analyze. This is exactly what enterprises use to analyze their business performance and customer attraction and the customer or user behavior on their specific website. The figure of Google analytic shows an example of it that has been presented by Google itself as a pattern.
Google has policies and principles which dictate their collection and utilization of customer data[48]. Following is some of the basic user data Google analytic gathers through their search services[4].

- Registered information or profile
  Information submitted by user. This is the data users enter into a Google application website, such as telephone number, name, picture, etc.
- Device information
  This information relates to such things as Smartphone or laptop model or phone number.
- Log information
  Log information is data such as search queries, telephony log information, time and date of calls, etc.
- System information
  This is data such as browser settings, browser language, and cookies, which can be linked to a users Google account.
- User location and geographical information
  The scope of some options allows Google to collect the information about surrounding areas that are listed as a Wi-Fi access point.
- Anonymous identification of users
  This is data and information grabbed by a user's browser such as cookies, IP address, pixel tag[49], etc.

Google claims that their reason for collections these types of data is to provide users with more services. [49]. However, too many other businesses and analyzers are taking advantage of these collections. The statistical value of the dataset that is being generated by Google analytic is free of charge to other collectors, and can be used for both business decisions and client satisfaction. Stakeholders' desires are noted, and customer activities are subsequently collected. These actions cause great concern to bother customers and information security agencies, and creates the challenge of security and privacy and how to protect personal data. Sandy Carter's speech touches on the fact that engaging in social business and business intelligence comes with high risk, but avoiding this system creates bigger problems. Therefore, more knowledge, and in particular, more policy, is necessary to ensure both satisfaction and safety[1]. Google analytic and enterprises considering data mining in order to client satisfaction by providing better services. However, from information security and policy compliance sight we emphasize on more privacy and security aspect.

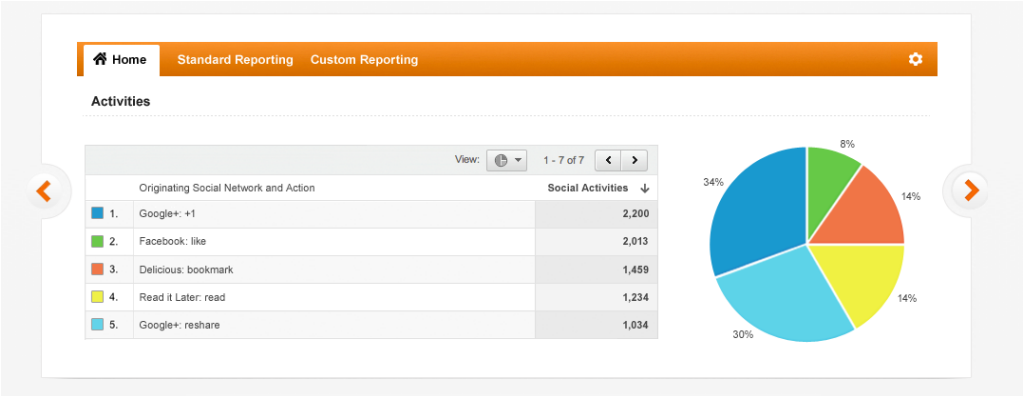

Figure 9: Example of Google analytic[4]

5.1.3 LinkedIn and privacy concern

LinkedIn is a great social networking website with a high amount of members. Member profiles are used as a marketing tool to specifically target recruiters. The site provides broad network connections between professionals within particular areas of expertise, and allows recruiters to search for possible candidates via social networking. While extensive research has not been conducted, security agencies and data protectors are researching the interplay of user profiles and privacy. The main concern is that while the LinkedIn platform can be a good place to locate possible business opportunities, user privacy is not easily enforced. The privacy policy published by LinkedIn states that the site automatically catalogs user location data and each location has the specific data controller. LinkedIn Ireland, for instance, has managed to generate this control throughout the entirety of Europe. This site collects the personal and profile information beside cookies and device information, etc.

LinkedIn further claims their willingness to disclose such user information to third parties as is permissible by the law[50].

LinkedIn publishes any user information that is posted as "public," and therefore feels allows to disclose such information to third parties. LinkedIn also makes user profile

information available on search engines. However, companies are very limited when it comes to monitoring what their employees share on their user profiles, which is a major risk against company identity, leakage of business structures, and company competition.

5.2 Data protection and prevention techniques

Today, more people are getting engaged on social media and online networking. Although most Internet users are unaware of how to properly protect their data and subsequently, how this lack of protection can be a very real danger to them. There are some techniques that can enhance the privacy level.
Techniques such as big data and social media analytic are some examples of how user data is being attacked. Users are ignorantly sharing personal information and identification on websites, and data collectors are collecting all of it, albeit "anonymously." The need to examine browser configuration and user data protection is great, since user aims to use applications and platforms such as Facebook, LinkedIn, Google+, etc.

According to what we noticed in the previous section, when a user visits a website, through some script user information such as cookies and histories can transferred to visited website. The code generated by JavaScript can grab some information of user's browsers. Third-parties can monitor the user online activities through cookies. Disabling the feature such as cookies and JavaScript is sometimes an option, but some websites will not allow users to browse the website. For an instance some popular website such as Expedia, gap.com, and Netflix cannot be visited if the cookies are. Most pages are not even visible if JavaScript is disable. In this cases, users receive an error message or a blank page for visiting a website. Sometime disabling these features just impact on third-parties accessibility and sometimes it limits the first-parties visibility[51].

Proxy and browser implementations are two techniques available to users to increase their privacy online. However, sometime these techniques can reduce the accessibility of the websites. Proxy-base techniques are not dependent on browsers and can limit both the user and the organization tracking. In fact, proxy is a better and easier way to protect the privacy for an entire organization[51]. For an instance a proxy can remove all cookies. It can also control the code which is being transfer by JavaScript[51]

User private data on browsers can be such things as IP, email, password, cookies, cache, visited pages, browser history, etc. Below are some techniques for users to minimize privacy concerns: [51]

- Disables cookies
  This is the most common way to protect data.
- Disable JavaScript and its contents
  As we mentioned already, JavaScript can take information from cookies and other user data in browsers and send it to the visited website. While disabling this feature is possible, some website require this option to be activated.
- AdBlock for Google Chrome, Opera, and Safari
  This filter is available on some browsers and allows users the option to surf the web without getting ads, banners or popups[52]. While this feature does not directly protect user data, it assists users in avoiding browsing unwanted websites that appear as

ads.

- Disable images
  It is possible to disable images displaying in some browsers, which can sometimes be used as a means for collectors to gather user data.
- Disabling third party servers Some websites use third party servers for parts of their transactions, which allows collectors at these servers to gather user data.
- Using BugMeNot technique Sometimes using such techniques as these allows users to bypass some website registrations processes.[53].

While every browser has specific functions, it is necessary that the issue of privacy be examined; which browsers are being used mostly by companies? which browsers are most popular? For customers, it is important that their data be protected while not limiting their use of website services.

From the websites and some social network application they still do not allow user disable JavaScript or cookies for having access to the website transactions.
Further research needs to be conducted on how users can protect personal data and still have full access to website functions. This includes the mobile applications of smartphones, which catalog location services and geographical location.

Regarding to what we examined as an example of known technological solution and configurations, user awareness is still crucial to data protection. Still some questions remain that how much user is aware of these protection techniques. In addition, how comfortable consumers feel in their online activities adds to the overall progression of social media and business. Moreover, it is also critical that what is the impacts on business if user have more awareness on these protection features and set them as high privacy level. For answering this questions, we will now focus our research on the examination of three case studies, each of which strongly contribute to the premise of our thesis.

5.3 Privacy and customer consent

From the business standpoint, customer consent and acceptance of services aids in economic growth and business progression. However, this target cannot be achieved unless customers are satisfied all along the business services. From the customer standpoint, the impacts of big data privacy is a big concern.

Customer consent plays a major role in privacy policies, and these two components should go hand in hand. Customers have the right to know what type of data is being collected through social business services and social media transactions. Additionally, they have the right to be made aware of how their data is being processed. Even information that is shared or posted as public should still require user consent so that big data collectors cannot take advantage of this information. The strategy for terms and conditions should be based on an agreement between both the user and the social business. Sometimes users are fully aware of data collection, while other times their information is subtly collected and passed on to third parties.
Data privacy protectors in the EU Commission strongly note that customer or user con-

sent should be required. They have increased the strictness of their rules and regulations in an effort to provide more user consent. One regulation relates specifically to the use of cookies to data collection, and indicates that cookies can only be used if user has provided such consent. The privacy protection efforts are not holistic enough to cover all issues, however; browsers, for instance, are automatically set to collect cookies and users who are not computer savvy may not know how to change this setting. A pro-privacy solution is for browser operators to reset cookie activity so that, by default, they are turned off. The limitation to this option, however, is that many websites require cookie function to operate[54]
Unfortunately, researchers seem to currently have user consent to data aggregation and big data in only their short-term sight. We can hope, however, that they soon perceive this issue to be a long-term one; big data collection will continue to assault customer privacy until the necessary changes to privacy policies are implemented[55].

5.4 Innovation in social media and user consent

While the content of terms and conditions sometimes varies, the concepts are always the same. In some cases, users sign an agreement, and at some point in the future the website makes revisions. In this case user consent is based on the old statement and the new policies or data processing might not be acceptable by customers or users. An example of this is Facebook; when it first began, user profiles were automatically set on public and users were required to manually change this setting. Now, Facebook has become a critical component in social business processes and business decisions. Users thought they had a control on their data by changing the privacy setting align to their consent. Facebook has changed its policies, and has collaborated with third parties such as game application providers, commercial companies and business enterprises. The privacy settings subsequently changed, but users who signed up for a profile under the initial terms and agreement are now faced with the fact that their data, according to the new terms and agreement, is being passed along to third parties. While, technically speaking, Facebook is following all the policy rules for user awareness by providing a terms and conditions agreement, they are not sufficiently focused on thoroughly informing users as various features are updated or changed. In fact this innovation is not fully adjust to consumer consent.

6 Case studies and interview result

6.1 Case study 1: Policy and data protection compliance in European union

According to the International Law and European Commission, laws strictly state that personal data shall be lawfully processed[35][56], particularly concerning the collection and storage of personal data. This Commission has been established in order to provide high standards of data protection for user information that's published over online networks.

Here we address some policy and privacy laws, which have been mentioned by the European data protection Commission. With respect to data collection, all data controllers such as medical examiners, or business enterprises and data analyzers, have to follow the laws. They should consider client or user privacy rights. Although these laws have been created for the European region, there are still huge differences in confidence rates throughout individual countries.

For the year 2002, all websites collecting user information were forced to notify the users of how they use the data stored in their websites. Adversely, users should have the freedom to disallow their information to be stored by website browsers. In the year 2009, the electronic privacy directive 2009/136/EC, replaced the opt-out rule with an opt-in consent rule 2009/136/EC[57][58].

Currently under investigation is the question of whether or not the recent browser setting is enough to keep user activity and user data securely protected. The latest proposal from the European Commission puts forth that this opt-out/opt-in rule should be clearly presented to users by each website. In early 2012, the European Commission started reforming the laws relating to data protection in hopes of increasing the strength of online privacy rules[59][57]. It is still unclear, however, how much security is required for users to feel satisfied in their social media and online transactions. Thorough investigation and clarification by security center officers about the big data analytic is a major concern for users and business clients.

6.1.1 Cookies and privacy issue

ENISA[1], the Information Security Commission in Europe, has conducted a brief study on cookies, their impact on privacy and crafted new policies regarding privacy. Here we explain how cookies impact both privacy and security. In fact there are two types of cookies:[5].

- Non-persistent or temporary cookies
- Persistent or permanent cookies

A web browser can use both types of cookies. Web servers can use both non-persistent and persistent cookies. Temporary cookies are used to store user status information as a

[1]European Union Agency for Network and Information Security:http://www.enisa.europa.eu

user moves between pages on a website. An example would be a user who is doing online shopping; language and country preferences would be stores via permanent cookies, while their list of transaction information would be stored using temporary cookies. The concern, therefore, lies in how reliable this storing process is at identifying individuals. Also, are there third parties, and who are the third parties, who have access to this data storage? ENISA claims that 80% of online providers use cookies to collect user's data; some use both types of cookies while some use only one type[5].

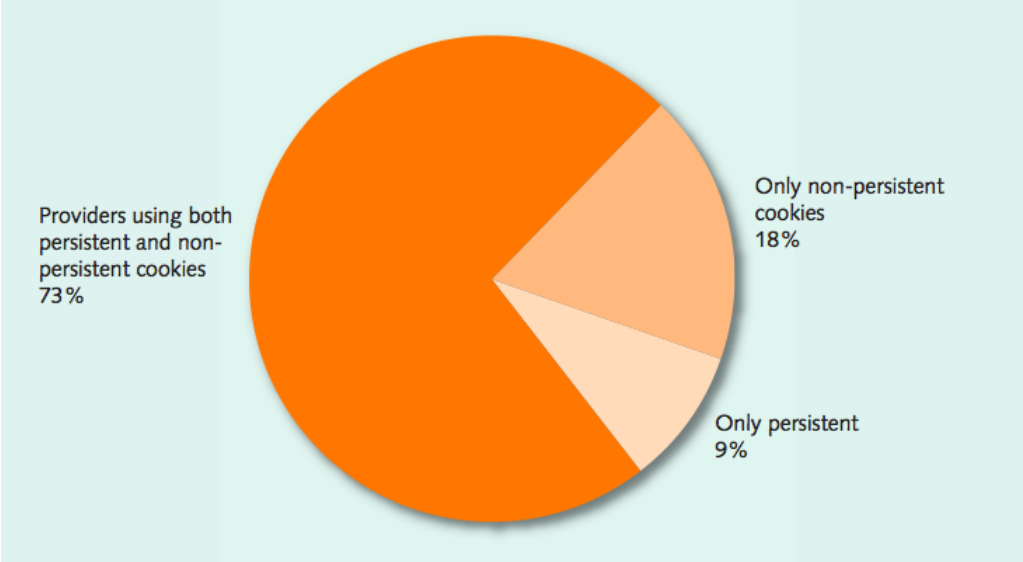

Figure 10: online providers use cookies to collect data[5]

With respect to privacy concerns, ENISA mentions that one of the major concerns is that cookies can sometimes be used for profiling, such as what pages users visit and the time spent on each site. Cookies can also save the authentication used to log in session. Cookies tracking user activities can also be transferred between the domain which sent them, and third parties such as advertising providers. ENISA mentions that this is obviously a serious threat to data privacy from third parties, since cookies stored can also be linked to social network user profiles[5].

Accordingly, within the EU policy framework, specific laws regarding cookies have been mentioned regarding personal data protection; it is crucial that users trust online services and social networking websites. New business transactions and social business transactions often take advantage of the data collected by cookies to develop data analysis. Enisa affirms that customers need to be fully informed about such realities, and know how their data is being used. Some of the data collected is transferred outside of the EU union, and in this case the laws and rules can vary. This transfer can create significant issues, since better policy requirements need to be considered for data not in EU territory[5].

6.1.2 Policy and legal act defined by EU security commission

According to the European Commission, there are two considerations that data controllers or persons processing user data should be aware of. First, they should notify the

data protection commissioner of the reasons or purposes for collecting data. Second, the processing of personal data should be done with respect to eight simple principles[12]. Follow are the principals cited by Data protection act 1998 in virtue of Council Directive 95/46EC. In addition these policies convey to all states in Europe[60][7]:

1. Data must be processed fairly and lawfully.
2. Personal data must be processes for reasonable purposes.
3. Personal data must be adequate, relevant and not excessive.
4. Personal data must be accurate and updated.
5. Not allowed to keep for longer that necessary.
6. Personal data must be processed in accordance with the rights of the data subject.
7. need to keep data secure.
8. personal data must only be transferred to countries with adequate security.

Obtaining user consent on online registration pages to ensure that users are educated is highly needed; such consent can be obtained by an opt-out or opt-in clause. The opt-in clause is the best method to obtain consent.With respect to consent, it is obliged that customer need to be aware of all business purpose and have the feasibility to stop such an aggregation. This controlling by user is being called opting-out option[61]. An example for an opt-out method is a company sending users an email without taking advantage of the information that has been registered by the use on the website. In this case user can use the opt-out to get rid of it. An example of the opt-in method, however, would be a company sharing its dataset or collected data with third parties. In this case the user did not have the option to give consent of data transfer[60].
The EU Commission has planned to reform these laws regarding data protection. This change is necessary because the Commission needs to adopt new standards and adjust its laws and rules to correspond with the new technology. In fact, data collection, data analysis, selling data to markets or even transferring data across countries is a new challenge for data protection authorities and commissions. Users disclose their private information in huge amounts, but would like to be given the option of consent about how their data is being collected and used by websites, third parties, and companies[6].

6.1.3 Public data

Open source data is data that has public availability, and that is accessible to all users on the internet. However, with regards to the EU Commission framework, these types of data still need to be protected by data privacy directives. The EU directive notes that any data that might lead to the identity of an individual, or poses a danger to individual privacy, should be considered sensitive data and thus be protected. The public access data is not confidential data, but should still be protected under EU regulations and laws[62].

6.1.4 Eu reform latest framework and data privacy protection

All states within the EU should follow the EU laws, and adapt their actions with the definitions of the European directives. With regards to the culture and human factors, business situations of some countries have different statement. Therefor in the specific situation the EU laws can varies to be stronger than other European states[7].
The new framework of EU commission is challenging with both protect online user data

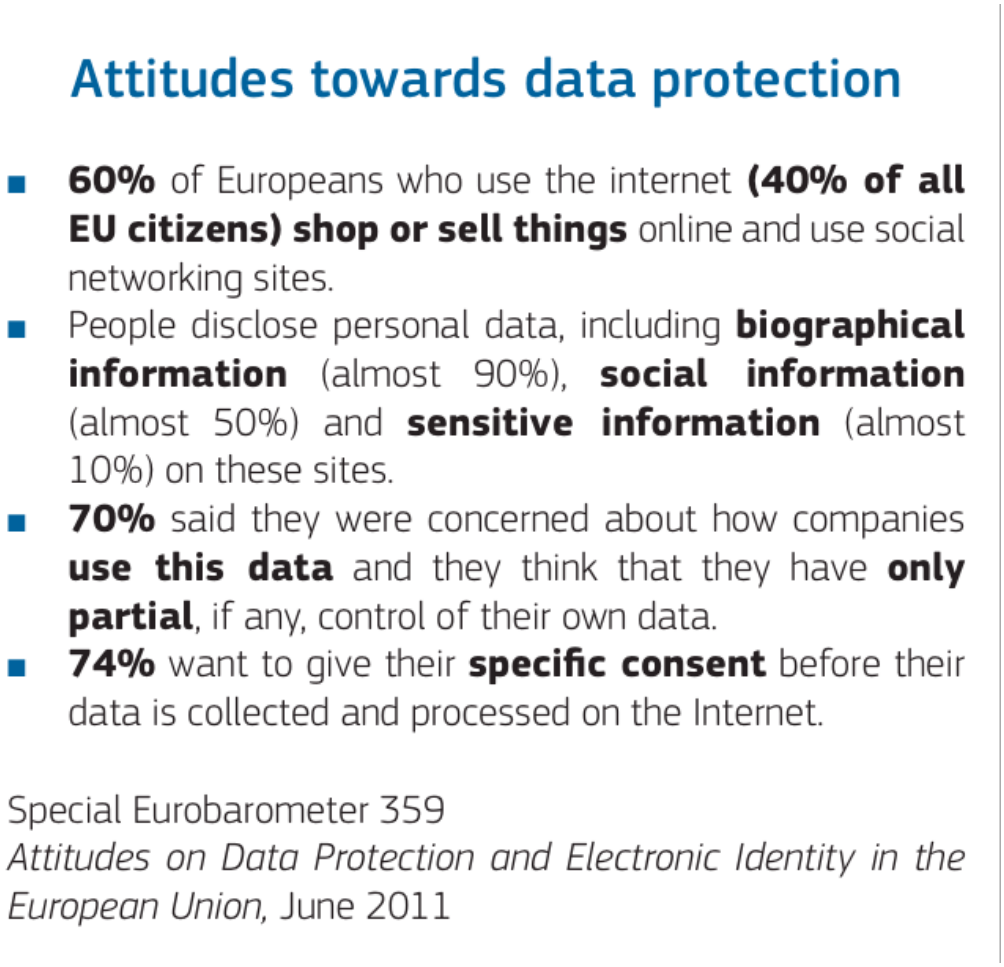

Figure 11: Attitude toward data protection[6]

and also at the same time lets market keep developing in technology and their business processes. According to the survey done by European commission in 2011 70% of European citizens are concern about how companies process their data and 74% want to have control on data and give the consent before their data be processed. Therefore European commission start reforming and renew the policies in order to obtain consumer's consent. The new framework of the EU Commission is challenging, since it must strike a balance between online user data protection and the technological advancement of business processes. In this section, we address portions of privacy regulations that were released in April 2013 by the EU data protection. Regarding cultural aspects, however, the construction of privacy rights can vary across the countries and regions.

Users need to have the right to control whether or not their data is being tracked by browsers. It is also critical that users need to be made aware of the fact that their personal data is being tracked, and given the option for browsers to either DNT or DO Not Track data. Follow sections we briefly listed the points have been cited by new EU commission.

Advertisement and user tracking

while online advertising is one of the attractive component of social business. It also carries privacy concern for users. Many users complain they do not feel comfortable that their data being recorded in order to being used for advertising purposes. According to the latest survey 40% of European are unconfined regarding this data collecting or profiling. EU directive Act.5(C) in 2010[7],] EU has mentioned that this user tracking should be under the e-Privacy Directive. In fact the tracking individuals has been known as a big challenging issue on privacy.

What is considered personal data or sensitive data

Personal data protection is a critical issue, whether or not users understand this. Therefor, it is important for the EU directive to clarify for users what is considered personal data. According to the European Commission, personal data includes all data that can identify a person. Sometimes data is collected anonymously, but still it is possible to re-identify a user indirectly. Additionally, many European internet users consider their financial data to be sensitive data. However, it does not technically fall into the category of personal data or data projection regulation. In addition, data location and biometric data are under specific directive protection category, but it still needs to be protected even if is it not defined as personal data[7].

Digital identity

According to the European Commission, digital identity is a collection of all available online data. This type of data can identify a users birthday, gender, nationality, address, medical records, purchase history, and interests. Additionally, IP addresses, cookies, location and browser fingerprints need to be under the data protection regulation.
Now by the new reform of EU directive all online and digital information and data are being amended into the category of data protection regulation.[7].

Anonymous data

Anonymous data is not considered as sensitive, since this type of data cannot be used to identify individuals. However, anonymity is being used as a method of securing user data and protecting privacy.

Data protection cost and benefit

The European Union Commission mentions that data protection regulations might be beneficial to the costs of business clients, business stakeholders and data collectors. It is still difficult to determine, however, the costs for all aspects. What is clear is that privacy levels based on consent can enhance user satisfaction, and cause acceptance of business progression. According to the EU data protective, making all data public and available means ending user convenience and consent. The purpose is to maintain a high level of data protection and thereby lower privacy risk.
Economically, there is a desirable level of protection policy that is nearly unfeasible if protection regulation levels are low. The EU protective claims that when social benefits of privacy protection outweigh the cost of privacy protection, the generic benefits of privacy protection are at their maximum level. If the required privacy protection level is lower than what is desired, the business benefit is in minimum level. In fact, the difference of cost and benefit makes it challenging to reach the desired level of privacy protection regulation.[7].

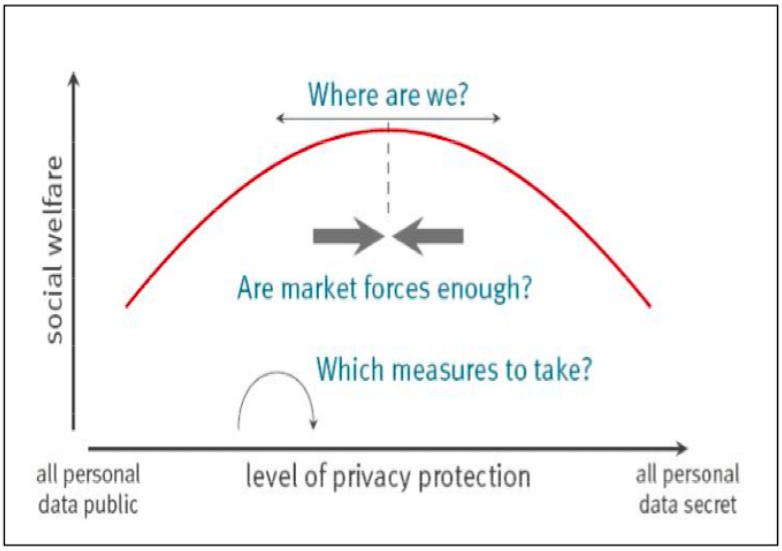

Figure 12: Desire levele of privacy protection[7]

Modernization of Data protection regulation

With the birth of big data and data analytic, the new technology relating to data processing requires increased respect and modernized reform to the various components of protection. First it is needed to enhance the user rights on data protection. Secondly, updating the tools being used in the terms of data aggregation. Furthermore, updating our understanding of and reactions to data aggregation is both important and necessary. Protection techniques should focus on identification privacy; particularly, constant development and improvement of these techniques is needed as data protection regulations adjust. In this term, EU commission claim that new strong compliance is needed. Both markets and the EU Directive Commission should focus on the satisfaction and confidence of users by creating rules that are accurately followed by data controllers[7].

6.1.5 EU commission and policy perspective

The data regulation, as implemented by the EU Commission, in applicable on various levels and in various directions[7]. Below is a brief review of the 2013 EU reform policies[7]determined by the new EU data protection regulation framework:

- Each state of the EU has different cultures, therefore these differences should be considered within the protection regulation framework
- Data protection regulation should also has positive economic effects[7]
- Regulation applies to all social websites and online services
- Policies should be well defined, using simply language
- Users should have control of their data, and be able to dictate what is transferred to third parties, used by businesses, or deleted
- Date regulations must consider the best way to handle user identification to ensure

that the highest level of data protection

- The need for a system of compliance by IT organizations is significant, and should be directed at data collectors, business organizations, and social websites to ensure that only proper and reasonable data collection permission is given out
- Each state of the EU should introduce and reinforce which laws should be used and followed by data controllers

6.1.6 EU data protection and customer acceptance of business

The greater extent to which businesses can provide privacy protection, the higher the rate of acceptance will be among users. Trust is the key component in business progress, and business focus should be on lowering risks of privacy against user data. Businesses that have a privacy protection officer have a higher chance of offering more privacy protection to clients, which subsequently increases client trust. While, at the same time some consumer are not sure if companies or data collector does not abuse of the user's collected information.This does not eliminate, of course, the reality that some officers within particular businesses abuse their exposure to user data, and thereby further damage user distrust. The EU Commission tries to make the privacy protection regulation modernized to ensure a system that is simple yet strong, and businesses benefit themselves by complying with the local authorities. Businesses that are proactive with these initiatives and comply with the standards of data protection by following the regulations help maintain a healthy business economy[63]. Without significant clear policies for both businesses and collectors, business satisfaction is much less likely to be achieved. It is therefore necessary to implement effective data protectives for both customer and business, which is what we will discuss further in Chapter 7.

6.2 Case study 2: Norwegian data protection authority and privacy

In this portion as we already mentioned in the methodology section, we describe the interview result we had with Chatarine Nes, the responsible of big data in data protection authority in Norway. Here we examine and reveal the concern and the privacy protection activities which has been considered so far by Norwegian authority.

6.2.1 Interview discussion with Norwegian data protection authority

1. **The collaboration of EU commission directive and data protection authority laws**
   The European data directive regulation and policy is applicable to all states in Europe, and the Norwegian data protection authority follows these regulations and directives. This means that laws and directives defined by the EU Commission have little to no flexibility. It is still possible, however, to attain stricter or more lenient adaptations. Catharine Nes mentions that "all European states will in the very near future follow regulations determined by the European commission and we cannot have any specific amendments on these regulations."

2. **How Norwegian data protection deals with privacy issues**
   The laws require that data protection authorities control all enterprises. When authorities receive a report about a new application or data aggregate, they control the application to ensure all components follow the EU laws and directives. According to the European privacy law, any company with specific applications that collects data is obligated to inform the data subjects; the person from whom the data is collected, regarding what data is collected, why data is collected, how the data is to be processed, and to whom the data will be sold. Additionally, if a company start collecting data, it should always considers the legal basis, which is usually consumer consent.

3. **Terms and conditions provided by data collectors**
   According to the EU Commission rule, all companies dealing with data and aggregate customer data should provide a terms and conditions. By this agreement consumers can be aware of how their data will be process. In this case the terms and condition should be understandable and not too long.
   These terms and conditions are sometimes time consuming, confusing and thus unattractive to new users; the terms and conditions provided by companies like Apple and Google is almost 10 to 50 pages long. However, while some users are too impatient to take the time to read and understand them, this is a safe way for companies to inform users of how personal data will be processed. Subsequently, companies should strive for terms and conditions that are succinct yet thorough since clarification of the terms and conditions educates users about data usage. According to data protection authority studies, very few app owners and developers provide users with an acceptable terms and conditions of user data processing. After controls executed by the Authority, app-providers have amended their privacy polices so they now comply with the laws.
   An example of an app, which initially did not comply with the laws of terms and conditions is Traffikanten, developed by Ruter Company. This app is used by Norwegian commuters on their Smartphones to rout their transport. In the beginning, they did not inform users of their agenda to collect data. After the privacy policy amendment,

however, Ruter Company now provides a terms and conditions to users. Even with user confirmation, companies like Ruter Company should use consider using collected data as anonymous values when engaging in data analysis and selling the data to other companies. It should be also mentioned that those who were started using this app very early before Ruter provided the terms, have never noticed any of this changes

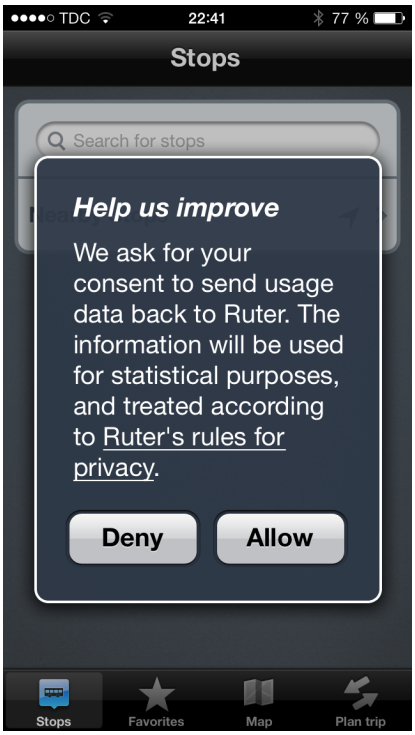

Figure 13: Traffic router application terms

4. **Norwegian Data protection Authority and educating the public**
   Part of the responsibility assigned to data protection authority tasks is to inform users of their rights on data protection. For the last couple decades, Norwegian data protection authorities have collaborated with education authorities. This campaign has been made for 9 to 17 years old students to provide them awareness of processing data over online application and websites. In addition there are some seminars to provide consumers and companies with the knowledge and training necessary to understand and follow all laws and policies.

Figure 14: Privacy awarness campaign by Datatilsynet[8]

5. **What is the big concern for privacy protection with respect to the big data technology?**

   Even though big data analytic providers analyze data anonymously, it is still crucial for data protection commissions to keep users safe of the risk of re-identification. There are still many challenges relating to big data, whether or not collected data is really anonymous, and how easy it is to re-identify individuals. It may be necessary to redesign big data strategy into an algorithm that allows for higher levels of privacy.

6. **Data privacy consent survey**
   Regarding consumer expectation and acceptance, Norwegian data protection authorities are in the process of conducting research to determine how safe users feel, and how comfortable they are with disclosing personal data. The result of this survey will be publish in early 2014.

7. **Norwegian Companies and big data**
   There are not many companies using big data in Norway, since this is a fairly new concept to Norwegian companies. It is, however, very attractive, and will most likely become more popular within the next five years.
   A food court chain that calls Coop, for example, has begun collecting customer data to analyze shopper behavior. They use a company called Dunnhumby bases in UK to analyze their data. In addition, some companies such as Finn.no[2] which is an online shopping classification website and newspapers such as VG[3] have started using big data processes. Most big newspaper companies are already started to invest on user behavior; in this case they start using data analytic tools.

[2] www.finn.no
[3] Norwegian newspaper

6.3 Case study 3: Privacy awareness

With regards to the role of social media, big data, website and online application in new business life, here we examine the consent and privacy knowledge of some consumers. Although business processes use data collection technologies, this aggregation may not be the most desirable or convenient for users. Privacy protection commissions have initiated some strict regulations about protection to control business, controllers and big data analytic services. There is still doubt, however that users are fully aware of their privacy rights or of the risk associated with their distribution of personal data on the Internet.

According to a report conducted by ENISA, users should know how their data is collected, and how it is being transferred to third parties[57]. They also need to be aware of how to protect their data. Many online networking users create profiles on websites and register with their personal identification data without any concern to privacy. They disclose phone numbers, job status, name and location. This behavior indicates that there are two types of people, those who trust the system and those who are ignorant to privacy risk. There are some people, additionally, who are neither trustworthy of the system and who refuse to share any personal data online. Age difference is another component to user behavior, as can be widely seen on websites such as Facebook, Twitter and other social networking websites.

6.3.1 Terms and condition on online websites

All website weather as social networking or any other type of websites that being used as a tool to collect individual's personal data have to determine their terms and conditions status. Consumers are much more likely to read and agree to a terms and conditions if a social networking or other social website provides it. If users are not satisfied with and subsequently do not agree to the terms and conditions, they should not be allowed to join a website. Most users are not accustomed to being required to read and agree to a terms and conditions when they wish to join a social website. Without the willingness to become sufficiently informed about a terms and conditions, however, users waive their right to data privacy. With this in mind, and in regard to international e-policy laws, all websites should establish and provide a terms and conditions template that aligns with legal international frameworks.

6.3.2 Terms and conditions on Facebook

As mentioned earlier, Facebook has a 14,000 word terms and conditions and user data policy; this policy falls under the international safe harbor framework[64].
When a new user signs this term and conditions, a agreement is being made between the user and Facebook. Facebook explains in this terms and conditions how the sharing of user data works, how this data is used, and how the coookie technology works. It further claims that they use data information collected by cookies to share with third parties such as advertisement, games, or any other services provided to consumers. Facebook further mentions that they use data only when the user gives them permission, and that user data is disclosed anonymously. If a user deletes their Facebook account, their data remains on a backout system for 90 days. Facebook uses cookies to monitor user activity for advertisement purposes and to monitor the use of Facebook services. Facebook's terms and conditions also mentions that users can control their browsers and cookies on their devices citeFacebookpolicy.

Most users are unaware of their rights to privacy when they join Facebook, and many do not know what they signed. While many users are concerned with the safety of their personal data, they believe that reading the terms and conditions is a waste of time and is not necessary. There is a possibility to use Facebook policies setting to limit access; this setting cannot protect all data; although these settings can help the user feel safer about disclosing personal data. Facebook always monitors at least a small number of user activities regardless of user consent, such as data collected and transferred to third parties relating to advertising partners, games, etc.
Many websites are connected to Facebook and its analytic reasoning, such as Google, which collects data for analytic processes concerning businesses. Some argue that if users choose not to take the time to read a terms and conditions, how would they know for what is reason of data collection and data analysis, how much of their user data is linked to their identity, and how much of their activity data is disclosed to data analytic providers.

6.3.3 Privacy on Social media and user awareness

While using social networks and their services is both attractive and beneficial to users, users should pay attention to the risks and threats associated with such participation. Enisa; the European information security aganicies states that the most significant attackers against data privacy are third parties, data collectors, data collector providers, and even other users or members of social network websites[47].

The issue of data privacy exclude mobile applications. Individuals using social network websites from their mobile devices run the same risk of data abuse by third parties as those using these websites from a computer. Many mobile application users do not pay accurate attention to their publicity or privacy settings. Third parties can and often do take advantage of this behavior. Initially, regardless of the device being used, all privacy settings on applications are set as public, including Facebook, LinkedIn and Google. If a user is not aware of this, or does not pay close attention, their data can be shared with and disclosed to third parties, as well as other attackers, hereby allowing data analytic providers to collect data.

Figure 15 is an example of the Viber app[4], which allows users to make free calls and share personal data with others, such a photos. This app provides access to a user's contact list, and pictures in their photo album. Google states in its policy for this app that their data collection is used only for the purpose of analyzing service performance, but Google analytic, by default, has been set to ON, which means it records and collects all data sent and received through this app.
Viber specifies the terms and conditions of the privacy policy, but it is important that users read it so that the privacy settings can be changed and thereby limit the access third parties have to user data. According to an online survey on community websites, users spend very little time reading the terms and conditions provided by mobile apps, and subsequently use social networking websites with ignorance.
For an instance because of some privacy issues which occurred in Italy. Data protective authorities in Italy recently established an awareness plan to assist and inform users who joined social networking sites[47].

[4]Free call, text and photo sharing mobile app

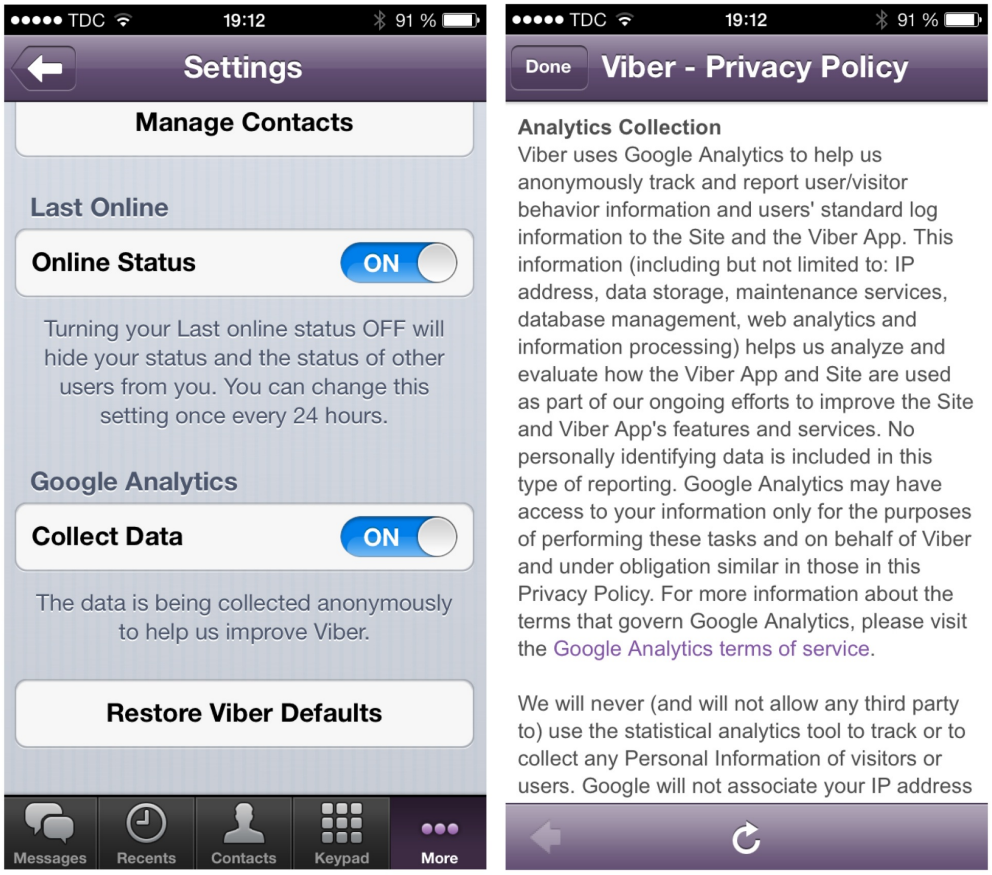

Figure 15: Google analytic on viber

6.3.4 Interview result on user awareness

As already mentioned in this paper, interviews are a beneficial tool in our effort to explore user awareness. This cluster of interview questions focus specifically on customer behavior and knowledge on social media regarding privacy concerns. It is generally perceived that customers do not have sufficient knowledge about privacy risk, and have also not been sufficiently trained to prevent the assaults on personal data. We interviewed five different master security students; the reason we chose this group of students is that because this is their area of study, they have more knowledge about privacy concerns, and a better understanding of this concept. Our interview conclusion provides a holistic overview of user awareness at a maximum level. Although the amount of interviewees is fairly limited, we still believe that the information they provide allows for a thorough summary of this topic. For the sake of personal privacy, we discuss the interview results with a level of anonymity.

Discussion of interveiw result

1. **Activity in social media**
   All five students participating in this interview have accounts on social networks, specifically Facebook and LinkedIn. Some of them does not spend high amounts of time on any of the sites, but they keep their account activate. Some other spend a plenty amount of time networking. Facebook is the most popular site among them all.

2. **User activity and data required for registration**
   The students interviewed stated that if they are asked to register with basic information such as email address and first and last name, they generally do. One student mentioned that they try to avoid sharing this information, but if these fields are required, they concede. Another student put forth that it is allowable to insert fake information, or at least an alias, to ensure privacy against attackers.

3. **Knowledge on privacy aspect**
   These interviews revealed that users generally think they maintain a sufficient amount of knowledge about privacy protection. That means if they share any data they know what they do and have control on that. They all are in believed that they have high-level knowledge on what they give away to the sites. However, after being asked the following questions, their beliefs were disqualified.

4. **Awareness of what websites and social media identified as terms and conditions and user privacy policies**
   Sadly, all five students admitted to never having read the terms and conditions or any privacy policy published by social websites or mobile applications. One student stated that they might consider reading these if data privacy becomes a serious issue. Another student asserts that "I assume I don't have any right based on those terms and policies." As previously proposed, it is inconvenient for users to read the terms and conditions because it is believed that there is nothing to gain from taking the time to read them.

5. **Control on browser settings such as cookies and JavaScript**
   Obviously, most of information security student are aware of the risk or threat of cookies and JavaScript. Some students state that they delete their history and block cookies and JavaScript options only after registering their personal information on a new website or shopping online. They believe, however, that this is not necessarily a secure way to keep their data protected. As well, all five students doubt that merely JavaScript management and cookie and history deletion is sufficient to protect against data collection.

6. **Public access**
   Because the students we interviewed represented a number of different cultures, our results varied based on social framework and background. We were able to come to the general conclusion, however, that some people feel secure in sharing their public information like a photo, job or education status; others block any publicity. Those registered on LinkedIn generally have their profile set to public in an effort to expand their efforts to be recruited by companies. All were entirely unaware of LinkedIn's policies and of its analytic partners.

7. **User awareness on data analytic provider and user tracking**
   One student states that as long as data collection falls under the international data protection laws, they consents to sharing personal information. They counter claim, however, that sensitive data such as that from medical documents should never be collected. He mentioned that he is not fully aware of data protection directive laws in order of his rights. The other students believe that they are not confident in any way in data collectors such as Google analytic and strictly try to block these collectors from their Facebook or other applications and websites they are registered with.
8. **The need of awareness and more policies**
   Some of the students interviewed for this paper still do not feel comfortable with the level of privacy on the internet. Their thought is that there are some organizations that misuse their data. Regarding cultural differences, the consensus is that data protection authorities and e-governance directives should organize awareness plans to manage privacy risk and its consequences. They also mentioned that there is a high demand for sufficient education and guidance on how to protect personal and sensitive data. One student believes that while policies have already been established, adjustments need to be made so that protection plans progress along with technological advances.

6.3.5 Interview questions on privacy awareness of students

1. How much you are involved in social media networks such as LinkedIn, twitter, Facebook, Google+, ,etc?

2. How often you register your personal info such as address, mobile real name, when you are being asked for it in any online transaction such as online shopping, etc.

3. How much you have knowledge on your privacy aspect on social media and online website?

4. Have you ever read the conditions and policies provide by websites in particular social website, before you become member in these websites?
5. Do you have any control on the cookies and JavaScript or any other browser setting in order to enhance privacy protection?

6. Does Your personal data has public access on websites?

7. How much you are aware of the data collecting by some companies and analytic provider to analyze your data how is the sense of that, do you feel comfortable?

8. Do you think it is needed more policy or awareness plan for privacy protection?

7 Discussion base on case studies

7.1 Policies and directives on data protection

The case study referenced in Chapter 6 examined the EU data directive and its insight on privacy levels. We previously mentioned that the EU data protection directive 95/46/EC is about to reform and determine stricter regulations concerning user consent and higher privacy levels. The EU directive on data protection gives us a thorough overview of what has been defined and specified by them regarding privacy levels. More businesses than ever are using the internet to increase their progression. From the business standpoint, technology is become much more convenient and customer oriented. However, from the customer standpoint, it is still very unclear what is the best way to minimize privacy risk and the impact it has on personal data. The European data protection commission strictly demands that companies, data collector providers, and application providers disclose their need for and process. EU strongly emphasize that personal data should be collected anonymously. Collaborating different dataset can lead to re-identification. The way of how to re-identify individuals is beyond the scope of this paper but it is important for us that the privacy risk is still remain there.

There is no easy way to discuss and remedy search for the best data protection regulation, although a few basic principles can serve as a guide in designing policies and principles.
Regulations need to be comprehensive enough to cover all potential privacy risks, yet not suffocating to the point of limiting any social media activity; they should be solid enough to withstand the tempests of constant use, but pliable enough to be reformed if necessary[6].With regards to the consent before designing data directive framework, it is necessary to examine what privacy level most satisfies social media users. It is expected, of course, that the perfect privacy level would provide the perfect level of confidence and safety. According to the reformed plan of the EU commission, they are in the process of better aligning their policies with the risks of privacy. Firstly, their new policies should be more holistic in their approach and thereby cover all states. Secondly, the big data analytic innovation is being pursued by more businesses every day and new policies should be strong and comprehensive enough to manage such influx.

7.2 Privacy knowledge and social business acceptance

In Chapter 6, the interview we conducted with students in the field of information security was conducted with the express purpose of finding out how they estimate privacy levels when they engage in online activities. All students we had interview with are member at least in one of the social media such as Facebook, Google or LinkedIn, etc. Most of the students believed that they have sufficient control over what data they share where, and how to limit collector access by changing browser settings. Further, we realized that they did not have very much knowledge about big data technology, and subsequently lacked the necessary knowledge to limit or dictate what data is being collected, and how

these collectors are processing their data. All of the students stated that they think more knowledge, for them and for the general public, is needed concerning big data analytic and data processes.
We also realized that almost none of them read the terms and conditions or the policies determined by applications provider and social media platforms. This behavior made a challenge for information security officer such as ENISA. They need to know:

- Does user know there is any risk?
- Does user care about the risk?
- Which aspect of privacy does user care more about?

After addressing these questions, data protection officers can determine how to adjust privacy policies with user consent. Even if users have insufficient knowledge and ignorantly provide their consent, this does not give the collector the right to aggregate personal data. Users who lack a thorough knowledge typically behave in one of two ways: they completely avoid being involved in online transactions, or they blindly engage in social media networking.

User awareness cultivates user consent, which in turn cultivates social business and trust social medias. If users understand how to protect their personal data and how to prevent the risk, they are more likely to engage in social media and other websites to disclose their information.

As our interviews with the students showed, we are still quite far from where we want to be concerning privacy levels. Users very rarely read policies or terms and conditions, and rarer still are they even curious to know that the data they share online is being disclosed to third parties. In Addition browser setting are all by default configure to collect. Cookies, JavaScript, browser history and the option of transferring data to the third parties like advertisement are all activated by default. As well, users are often unaware of the default settings on their browsers and apps and subsequently present themselves as easy targets for data collectors.

The figure below shows an example of a Safari browser . It shows 902 websites store cookies and other data on this browser. Websites are also allowed to track the user. This behavior is allowed by default. According to the overview we had on some web browsers setting we can admit that Most users are not aware, and have no intention of educating themselves, to the privacy level their device is set at, yet often complain when their data is collected without their consent.
Privacy risk potential is no all about what their share. It is also considering data collected through browsers and website visiting session or even the user IP which can lead to identify an individual. Although, at the same time if the security of the browsers is high some websites services are not reachable. For an instance, most of the net bank transaction is not possible without running java.
While this study cannot cover all aspects of preventing privacy risks by browser settings, our aim is to reveal that user knowledge and awareness is not and has not received the

same level of attention and focus as its counterpart of business innovation in light of big data, analytic, etc.

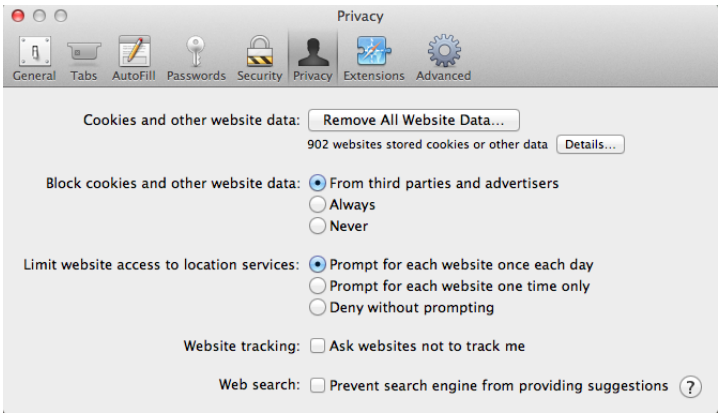

Figure 16: Privacy setting in Safari browser

The results of our interview with students show that the level of knowledge when it comes to privacy is very low, in particular, in Norway. Means if they have more knowledge they will act differently. Social business is based on collecting and using data, which happens over the Internet.
While the browser setting can decrease both security and privacy risk, but consumer rarely have control over it. In addition the awareness program is very necessary, yet it is not clear how it should be planed to use the browsers protection add-in applications and as well as settings. It is assumed that awareness plan can be designed by privacy commission or data protection authority to educate users.

7.2.1 Privacy and awareness training

Lack of knowledge about big data in business processes in Europe is a major issue. Although, in Norway, there are only four or five large companies that deal with big data collection, such as Finn.no, Futer.no and Coop, in the very near future, however, big data collection will become a large part of business processes. Data protection authorities, big companies and software developers such as Microsoft should thus consider a user awareness plan align to this tool. Microsoft has established a basic training plan that includes awareness tips for both adults and children in an effort to increase data security and privacy. Microsoft has also made an effort to inform users on how to protect their privacy on the Internet toward against identity theft and unwanted data disclosing. Users can learn about regulating who views and collects their data and how much of their data can be collected, who can monitor their activities and how to block their tracker[9]. These efforts are good, but yet we believe that more extensive plans should be made. It has for example mentioned that the new system operator have security essential embedded.

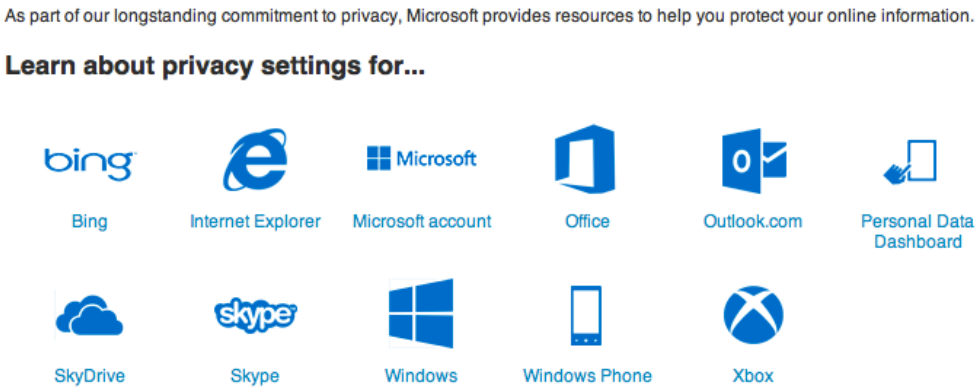

Figure 17: Learn about privacy setting protection[9]

7.2.2 Cultural efficiency in confidence

Culture and ethnicity are two of the main measure relating to data privacy and security, since the method on business communication, service and processes has been changed, and then social frameworks show different levels of efficiency in different cultures. Even within a country, however, this poses a challenge; in Europe, for example, the efficiency of data protection directives vary from state to state.
TRUSTe is a global data privacy management company that helps businesses safely collect data aligns to privacy compliance[65]. According to a survey recently in 2013 conducted on US consumers, 89% of users are concerned about their online data privacy, and this percentage is significantly increasing[11]. More details regarding this survey is in the appendix chapter of this paper. TRUSTe report cited that obviously, user insecurity impacts business performance; this issue has become a major concern for information security officers and privacy protectors. This concern has been started to rise along to business innovation. Many American companies are taking advantage of big data; this pattern is still fairly new to European states and many Europeans have yet to discover the full risks associated with big data and data aggregation. In addition, it is unclear for consumers how is the future of their privacy.
The survey by TRUSTe puts forth that many US consumers avoid using all aspects of their phone apps or websites, since they are not completely confident in the terms and conditions of the user agreement, and they do not believe there is an adequate preventative against risk. With regards to this survey, further research is necessary to examine European user behavior, consent and confidence as well.

Most consumers in Europe are in believed that companies or data collector is responsible to protect their data. However, the users self are responsible on what they share and how to control their privacy[11]. Therefore they need knowledge and need to be trained how they can have a control on data processing through companies or any social media providers. Although most data collector provider addresses how they process consumer's data but it is still needed to be trained in a comprehensive manner .

7.3 Privacy in Norway

As we already mentioned in the previous section, big data analytic and social business services is a new topic in Norway. According to an interview we conducted with Norwegian data protection authorities, Norwegian citizens need more extensive training on data protection since increased Internet activity is a fairly new phenomenon in Norway. People are not sufficiently aware of how to deal with big data. All sates in Norway are in the same line and all comply the same directive.

Norwegian authorities believe that it is still to early to judge about the confidence and user consent on business services. They are conducting research on user confidence online which will hopefully be completed in January 2014. This will hopefully provide new insights on privacy concerns in Norway. As more people increase their use of social media, concerns about big data processes and social media analytic will increase dramatically. Laws and policies must consider consumer privacy rights, and business benefits at the same time. For an instance, the data analysis by Ruter.no[1] provide better transport services for users. Ruter.no addressed that they use cookies in the purpose of statistical context, favorite functionality and the data that help ruter.no to remember user log in authentication. In addition it mention that that when it be used on phone any data that can link and identify the individuals not be collected.

7.3.1 Facebook and data processing

Since Facebook is a commonly used social media website in Norway, data protection authorities conducted a case study on how Facebook processes personal data. There are many concerns surrounding this topic, one of the main points being data collection of non-members. Collecting the IP addresses is not pleasant for users. In this report has been examined once the user consciously accept the conditions and privacy policy, any data processing by Facebook is on user's responsibility.The following points are some of the generalized doubts that this case study revealed:[10]

- Are users thoroughly aware of data protection policies, and are these policies easily understood?
- What is the best solution for users who are reluctant to read the terms and conditions?

. The figure bellow shows the type of data that being process by Facebook. This data's being used by advertisement, applications, social plug-in and partner sites.

The biggest question concerning all these aspects is who is most responsible for data leakage: ignorant users, or data collectors who take advantage of user data? The Norwegian authorities do not yet have an answer to this question, but should seek to make policy changes to match technological changes. With regards to privacy quality management, the Norwegian data protection authority is collaborating with the Norwegian broad of technology and the center of ICT[2] in education to establish training for the new generation of internet users[3].

[1] Transport moblile app, https://ruter.no/en/about-ruter/privacy-practice/
[2] Information and communication technology
[3] www.dubestemmer.no

Category	Definition	Type of data
Mandatory profile data	Personal data one has to provide in order to be a member	Name, gender, e-mail and date of birth
Extended profile data	Personal data one may provide	Network, profile photo, mobile phone number, hometown, sexual preferences, name of school/university, religious/political views, favourite music/film/author, name of family members, e-mail contacts, etc.
Personal network data	Data showing your interaction with other people and objects on Facebook	Friends list, family, relationships, pages/groups/people you like, etc.
Self published data at home	Data one publishes or uploads on one's own profile	News feeds, notes, photos, videos, links, etc.
Self published data away	Data one publishes on someone others profile	Comments, wall messages, etc.
Other users' data	Data about you published by other users	Photo, video, tags, etc.
Behavioural data	Data Facebook collects about your habits	Pages you visit, topics you write about, games you play, etc.
Connection data	Data from your connection to Facebook	Type of connection unit (mobile or PC), browser, location of connection unit and IP address.
Metadata	Data about data	Type of camera used to take an uploaded photo, etc.
Derived data	Data about you derived from all other data	If 90 percent of your friends from your University network are fan of a special rock band, you are probably a fan too.

Figure 18: Data categories of data processes through Facebook[10]

7.4 User acceptance of social business

As Research suggests that US citizens are more conscious of data privacy concerns than are European citizens, since they have been engaged with social business and social media for longer. The survey by TRUSTe shows that many consumers worry about big data, though we cannot see this worry as prominently in Europe and specifically in Norway. European users have not been educated about how much personal information is good or bad to share online, or what rights they are signing away by agreeing to a terms and conditions. This unconscious make them feel secure sometimes. The survey by TRUSTe[11] suggests that because American users have low confidence in customer privacy policies, many avoid using Smartphone apps or online businesses who are known to collect user data. In many sate in Europe people are not much involved in such a business where collecting data. All this being said, it is not easy to determine the needs of a privacy management program, yet it is crucial that within the next three years a plan be implemented and the need of this program will be sensible.

Privacy concerns are rising, and this does not settle well with business providers and stakeholders[11]. Businesses aim to absorb more customers, and their satisfaction is ne-

cessary for productive business interactions. Therefore from the first day a comprehensive policy framework is needed. The European Commission has attempted to provide accurate rules and laws which should be followed by companies in all their business steps. Customer awareness in the core of all these proceedings, and this is accomplished by businesses and companies providing terms and conditions to convince the consumer. Below are components of a good policy plan:

- Train users on what their rights are, and what potential privacy risks exist
- Assist users in changing their behavior; encourage them to read and sign all terms and conditions
- Provide safeguard methods for users to enhance their knowledge of privacy data

Companies obliged to inform user why and for what reason they are collecting data. In fact, companies who inform their users of what and why data is collected have a better chance at gaining trusting customers. This awareness can lead to an unexpected negative outcome. That means at the same time rising the user awareness can increase the level of privacy concern. This hypothesis needs to be studied through a survey; how people act after and before awareness plan.
In the next section we examine how user attitudes often change after data protection training. Privacy management should be embedded in business services; an example of such privacy management is provided by TRUSTe[11].
There are 3 steps that a company should consider in this privacy management:

1. Certify
2. Monitor
3. Control In the first steps they need to clarify and assess the current privacy level such as why and what and how long the collect data, etc.
   the second steps is to monitor the privacy program in order to check if it follows the regulations.
   the third step is to manage cunsumer activities to control the opt-out,cookies, etc. This program also covers all type of online platforms, such as mobile application, cloud, Advertising and web.

The aim is to have the same level of privacy for each type of consumer. Regardless of gender, age, and education, privacy levels should match the business. Obviously, a group of higher educated adults are more conscious of their rights and the risks associated with data sharing than are a group of young children. Therefor it is highly needed to plan a train and privacy policies, which cover any type of consumers. Reasonably, having a secure and wise online society is a big target that cannot be achieved easily. Therefore the cultural difference and background knowledge in the policies and awareness plan should be considered.

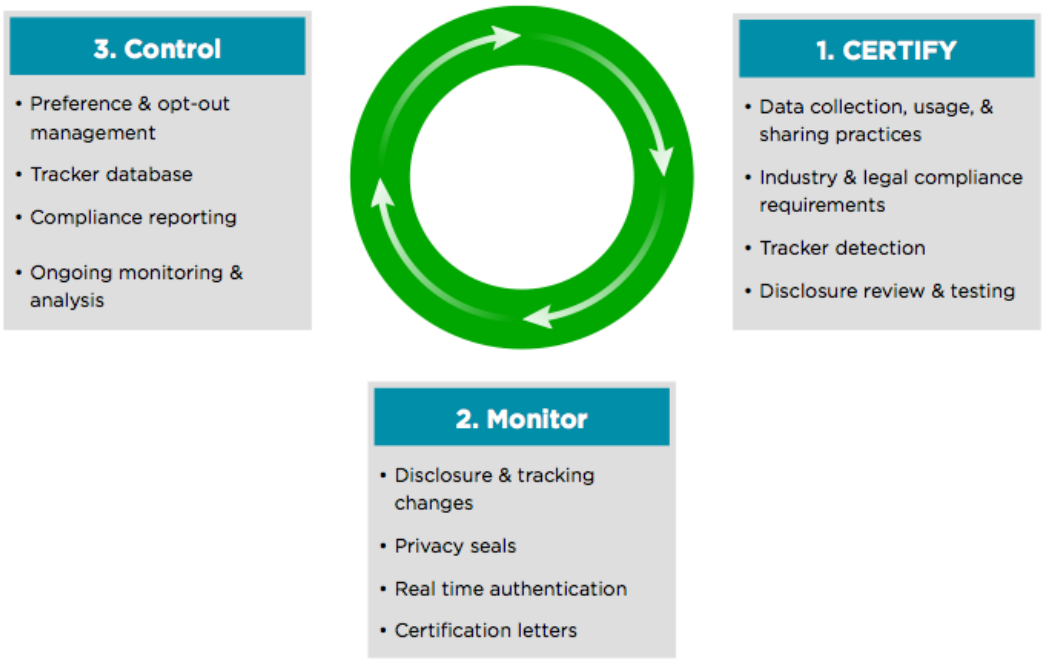

Figure 19: Learn about privacy setting protection[11]

7.5 Being trained and evaluate the user behavior changes

In this section of the paper we test the impact of awareness training on users and their attitudes. We collaborated with Runar Moen, who is writing a thesis on creating secure software. One of his goals was to train software providers to acquire more knowledge on potential security and online privacy risks. He created a blog on which he planned to educate people and train them about data privacy and security. At the same time, he managed a training session in person and explained more about privacy risks . His research participants were all academics and software developers; individuals in both groups were asked to read information about security and privacy awareness, and to take the training session. After the class, all participants were asked to answer some questions about their consent and their attitude on privacy and security compared to their consent and attitude prior to taking the class.

After receiving the survey answers and the values we analyzed the result in the purpose to provide our thesis target. The result is demonstrated in the figures bellow.

1. First we are analyzing How many respondents were concerned about privacy risk before reading the training blog or attending the training session?
   The pie chart shows that 85 percent of participants were concerned sometimes about their privacy on online application and web services before being trained. It also dedicate that 15 percent were always worry on privacy online. Considering the result reported in TRUSTe survey, there is still better consent in our selected group than what we see in the US, although there are countless factors such as more trust or less awareness that create this difference.

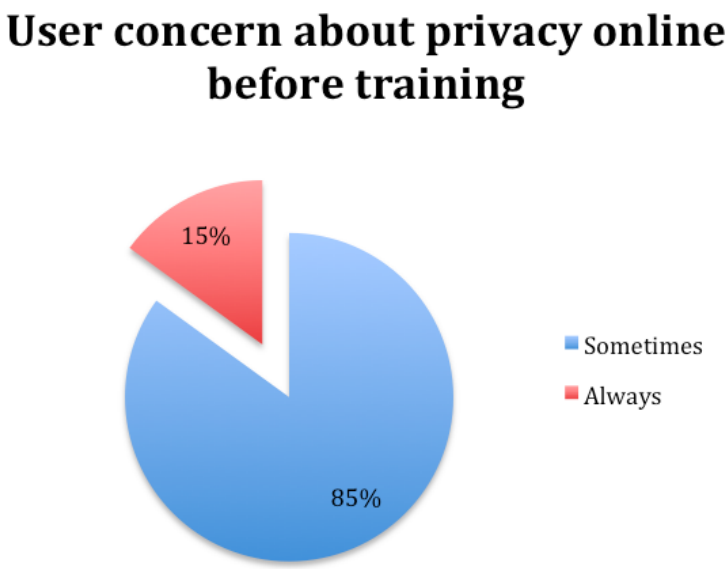

Figure 20: User concern on online privacy before training

To prove our belief that each state has different insights on privacy risk and data collection or analytic, we might need to conduct a very holistic survey in each European state.

2. How much knowledge did participants have about online privacy risk potential prior to training?

Survey shows that 57 percent of participants had high amount of knowledge about

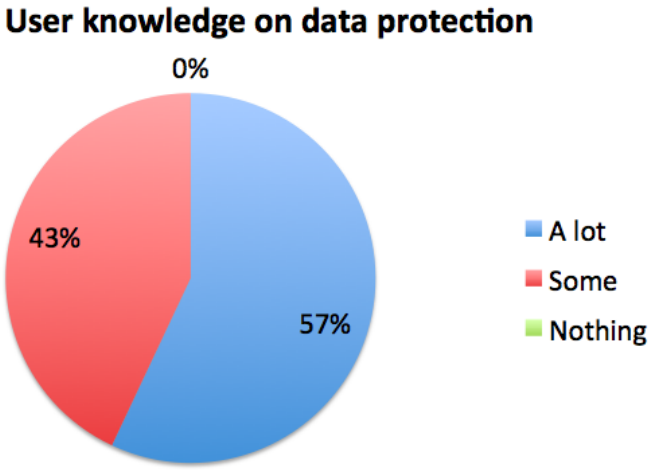

Figure 21: User knowledge about online data protection before training

online privacy risk and data protection before training, while 43% had some awareness. We should note that this amount of awareness for an academic group of people

who are software developer, is still very low. This amount can significantly decrease in the group of general or uneducated users.

3. After training, do participants feel more safe and confident, or less safe?
   A very unexpected result in the figure shows that 71% of those trained felt just a little changes on their concern and their trust on the web apps and data privacy. 29% of participants claimed that there is no changes in their consent or trust level after training. This group believes that it is still not clear what exactly happen to their data; how much security and privacy risk can occur by using the online applications. This group worries about their password, bank transaction, and identify.

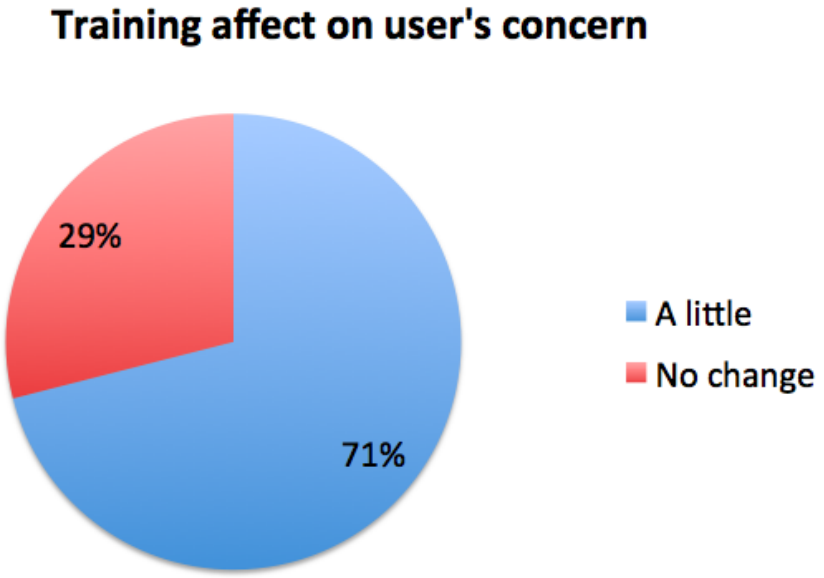

Figure 22: Training affect on user concern

4. In which ways do participants feel more comfortable, and from what did they learn most: reading the blog or attending the in-person training session?

   Participants were most comfortable with the in-person training session. Some of them did not even read the blog correctly. the result of survey indicates that 72% of participant learned more from in person training. It seems an online page with security and privacy, or policy information is not attractive enough for users. Based on this information, we have concluded that this might be a reason why users generally do not read the terms and conditions. As previously mentioned, a major concern with data protection is the fact that users do not read and sign the terms of agreement. We can get a result that it might be the reason why the amount of confidence and trust is higher than US. It might be reasonable that in American culture the lawsuit system force people to be more conscious on what they sign in matter of consent.

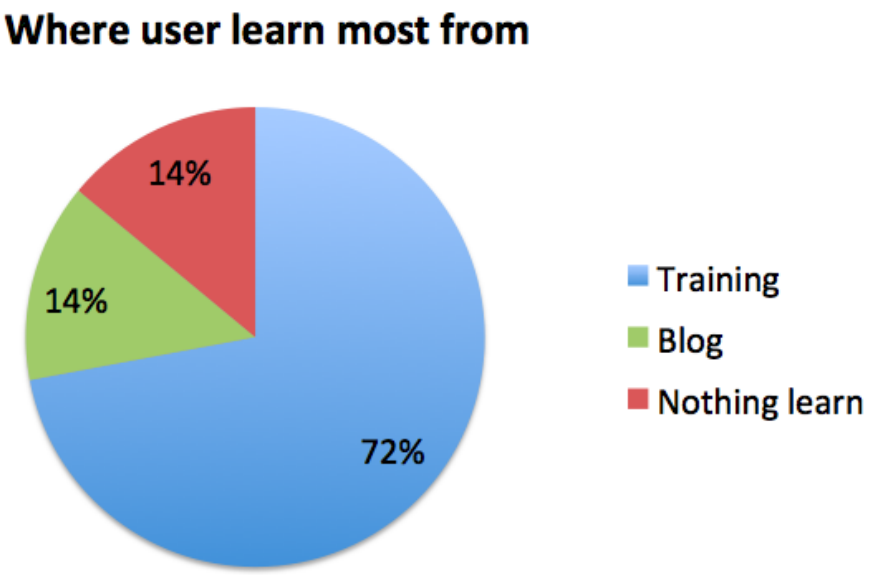

Figure 23: Where user learn most from

5. What did participants consider to be sensitive data? Participants defined sensitive data as pictures, health documents, job statements, and passwords. Any information other than what is personally posted as public considered sensitive data, including IP addresses, cookies, browser history, etc. Furthermore, any data that allows data collectors or attackers to identify users is also sensitive data.

7.6 Survey Questioner

1. Were you concerned about your privacy on Internet before the training and before you did read the blog?
   - A lot
   - a little
   - Not at all
2. Have the blog and training affected your view on privacy?
   - A lot
   - a little
   - Not at all
3. How often do you worry about online privacy?
   - Never
   - Sometimes
   - Always

4. Do you think normal web-users should know more about security and privacy online?
    - A lot
    - a little
    - Not at all
5. Did the training teach you more about how to defend against attackers?
    - A lot
    - a little
    - Not at all
6. Have the blog teached you more about how to defend from attackers?
    - A lot
    - a little
    - Not at all
7. Have you ever tried to prevent data leakage?
    - A lot
    - a little
    - Not at all
8. Do you in general feel safe when using web-applications?
    - A lot
    - a little
    - Not at all
9. Have the training and other information changed how safe you feel online?
    - A lot
    - a little
    - Not at all
10. What did you learn most from?
    - Blog
    - Training session
    - Didn't learn anything
11. What do you consider as sensitive data?
12. If yes to the questions about interest for learning more, what do you want to know more about first?

8 Conclusion and recommendation

Big data and social media are two significant tools for modern businesses, yet two major concerns exist as a result: privacy concern and user consent. The latter presents significant risk to both data protection authorities and businesses, since there is a lack of thorough research on users' view of data privacy and user online activity. All business holders, data collectors and big data providers should consider the importance of consumer consent and confidence.

Consumer consent is a matter of business survival; data collection conducted without user knowledge often results in lack of user participation, and lack of user participation hinders business growth. Businesses should ensure that users are conscious of the legal rights and aspects concerning privacy protection rights. Compared to the growth of social media and social business, privacy awareness plans and policies are lagging far behind. Social media usage is much higher than security or privacy defense and risk mitigation knowledge; such imbalance is detrimental on many levels.
Currently, there seems to be a definite divide between technology and privacy and data protection; these two components should make more of an effort to work together to create consumer satisfaction and trust. Many current browsers have the capabilities to provide increased security and privacy compared to previous generations of browsers, yet the default settings on almost all browsers are set on minimized users' privacy and security settings. This proves that it is not technology that is at fault, but awareness and policies that are lacking in aggregation and disclosing data.
Many users do not understand the importance of reading the terms and conditions that are provided by some social media websites, and what will happen to their data once it is published and disclosed over the Internet. Many are still unaware of the ways in which companies collect their personal data, or that companies sell their data to third parties. Users need to be properly informed of the risks related to data leakage, and to reality of data attackers.

Privacy policy and data protection play an important role in current technology innovation. Before social business grows any bigger, it is crucial that time and budgets are spent building a productive and mutually beneficial foundation on which future social business can develop and consumers can remain satisfied. Consumer behavior needs to change so that users can productively utilize the new technology with trust. This will never be achieved without a strong privacy awareness plan. The role of data protection authorities in each state, as well as European data protection directives, are very important. Institutions such as ISACA[1] [25] and other privacy and security training centers have collaborated with companies to ensure better data protection directives. Social media and online application technology is rapidly changing; we need to have a more sufficient response to the potential risks. We had neither the time nor the resources to pursue

[1] Information Systems Audit and Control Association:http://cart.sammydress.com

quantitative research for each European state, but the research within the scope of our thesis provides a better understanding of user perception and user consent. It will also help us realize what type of awareness program will be the most effective as social business progresses. We realize that European countries, Norway in particular, have different insights on big data privacy than the United States; this difference contributes to the cultural differences that impact social business process and service. For instance, consumers in Europe generally have more trust in online business transactions than Americans, although a more comprehensive survey is needed to confirm this assumption with accurate values.

8.1 Awareness recommendation

According to the interviews we conducted, our conclusion is that the need for user awareness is very high. ENISA[2] mentioned that the first step to defense against privacy and security is increasing awareness.
More extensive study needs to be conducted on what time of awareness would be most effective and holistic. It may be easiest to have a campaign in schools, or even in individual communities, to educate the masses; it may be more feasible for governments to delegate a budget for a nationwide awareness plan. Because cultural aspects create varying factors within each country, as well as gender, age, and educational differences, it may be necessary for various awareness plans to be implemented. As social business grows, our approach to privacy protection needs to become more proactive. Below are some awareness points to consider concerning the progression of social business and the absorption of more trusting and confident customers.

8.1.1 Main factors in an awareness program

- What is the browser default setting configuration?
- What types of data can users share that is publically accessible?
- What kind of data collector, company, application or web services can users trust?
- What is big data, and how does it impact consumers?

8.1.2 Awareness alternatives

- Awareness programs in school and educational institutions: privacy and data collection should be taught as ardently as language and mathematics
  In the school the privacy and data collecting should be taught as serious as language or mathematics course.
- Data protection authorities should collaborate with governments to ensure the creation and implementation of effective and comprehensive programs that cover all students in varying levels of education.

8.1.3 Effective awareness

Europe should design an effective awareness plan for each state. Some suggestions for such a plan as put forth by David Lacy[66] are listed below:

[2]European Union Agency for Network and Information Security:http://www.enisa.europa.eu

- Playing a game: This is a good method for children and young users
- Using a Memorable message. Using a memorable message (a song or catchy rhyme perhaps) is always helpful
- Using images
- Hitting the spot
  People like to compare things. Using popular companies to show users the realities of data collection; real story examples of privacy invasion; real world scenarios for handling privacy risk. It helps consumer to know how to handle the risk if they face to such a privacy issue or any related concern.
- Awareness Scenario

8.1.4 Assess the local habit

Each gender and age group within each state needs specific training, as it pertains to them and as they can best understand it.

8.2 Policy recommendation

One of our research questions considers how privacy can help convince users to get more involved with social businesses and to trust data collectors. More specific and thorough study is requires to build the concept of this theory, but even on the surface this thought is easily understood. The less data collected without consumer consent, the less likely consumers are to trust social media and data collectors. The opt-out and do-not-track-me options are examples of user options that can act as safeguard alternatives to informed users. Additionally, we make the following recommendations:

1. In order to policies, better collaborations and dialog between data protection authorities and companies are needed [67].
2. As a plan to be proactive, it is needed to design the system from the scratch end embed privacy aspect.
3. Need of a great data process management team in each company
4. Policies created by companies and web providers should be aligned with international laws and, as well, need to convey all type of consumer consent.

5. Terms and conditions on websites and online applications should be short, easily understood, and aligned with data directives.
   further survey and human factor assessment is necessary to determine what kind of structure is most effective regarding consumer perception and expectation

9 Future work

This study emphasized the impact of big data on consumers. The following concerns could not be evaluated in this paper, but need to be pursued through further research and analysis:

1. The impact of unreliable and fake data, collected from social media on business
   If the collected data over social media is the base for business decision, then a dirty data can impact the business services. It also can damage the business reputation.
2. Comprehensive survey on consumer habits and perceptions of privacy regarding cultural differences within social business;effectiveness of terms and conditions.
   The result of such a survey helps business to examine how to design their policies and conditions in order to absorb more consent. In our study we mentioned that user not interested and patient to read the conditions and policies provided by applications and online websites. in this case a quantitative study on user perception can contribute us to estimate an effective policies, terms and conditions design to have it more understandable and more acceptable by consumers.

3. The feasible potential changes on browser settings to ensure greater privacy protection

Bibliography

[1] Carter, S. 2013. Catching the wave:trend and strategies for social and mobil. IBM Slides. http://www.youtube.com/watch?v=gYMtHAz-SbA.

[2] Greenwald, G. July 2013. Nsa tool collects nearly everything a user does on the internet. theguardian. http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data.

[3] Malandrino, D., Scarano, V., & Spinelli, R. 2012. Impact of privacy awareness on attitudes and behaviors o. University di Salerno.

[4] Google. Google analytic website. google.

[5] Enisa. Feb 2011. Bittersweet cookies. some security and privacy considerations. http://www.enisa.europa.eu/activities/identity-and-trust/library/pp/cookies/.

[6] commision, E. October 2011. Commission proposes a comprehensive reform of the data protection rules. http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm.

[7] Malandrino, K. I. & Luchetta, G. April 2013. Online personal data processing and eu data protection reform. IEEE.

[8] Du bestemmer. http://www.dubestemmer.no/en/913_years_old/Privacy/#content.

[9] Learn about privacy setting. Microsoft. http://www.microsoft.com/security/online-privacy/overview.aspx.

[10] Arnes, A., Skorstad, J., & Michelsen, L. P. 2011. Social network services and privacy. http://datatilsynet.no/English/Publications/Hva-skjer-med-personopplysninger-i-Facebook-/.

[11] Solove, D. J. 2013. U.s. consumer confidence privacy report. Truste.com. http://www.truste.com/us-consumer-confidence-index-2013/.

[12] Winton, A. & Cohen, N. January 2011. European data protection and privacy everything you wanted to know – and more. white§Case.

[13] Goodendorf, L. february. Managing big data privacy concerns: Tactics for proactive enterprises. *Tectarget*. http://searchsecurity.techtarget.com/feature/Managing-big-data-privacy-concerns-Tactics-for-proactive-enterprises.

[14] Laskowski, N. June 2013. turning dirty data into business insights of your customers.

[15] Eric B. Parizo, S. S. E. Jan 2013. Lacking privacy laws aid growing ciso role in data privacy management. *search security, Techtarget*.

[16] Schwaninger, M. 2007. A systematic concept for research process. markus.schwaninger@unisg.ch.

[17] Wikimedia big data. http://en.wikipedia.org/wiki/Big_data. last modified on 16 september 2013.

[18] Kuketz, D. 2012. Big data insight for maximum business impact.

[19] Patricia Cronin, frances Ryan, M. C. 2008. Undertaking a literature review a step by step approach.

[20] Leedy, P. D. & Ormrod, J. E. 2012. *Practical Reserach planing and design*. Amazon.

[21] et al, S. 2003. Pierce.

[22] Wikimedia social media. http://en.wikipedia.org/wiki/Social_media. last modified on 16 september 2013.

[23] Bateman, K. 2013. Generation y a hazard to european security. computerweekly.

[24] Wikimedia cyber attack. http://en.wikipedia.org/wiki/Cyber-Attacks. last modified on 6 september 2013.

[25] Meadows, R. 2010. Top five social media risks for business.

[26] Yunus, M., Moingeon, B., & Lehmann-Ortega, L. 2010. Building social business models. Elseveir. http://www.elsevier.com/locate/lrp/.

[27] Wikimedia sandy carter. http://en.wikipedia.org/wiki/Sandy_Carter. last modified on 25 april 2013.

[28] Wikimedia, social media analytic. last modified on 24 july 2013.

[29] Boudreaux, C. 2013. Social media governance. http://socialmediagovernance.com/policies.php.

[30] Rouse, M. March 2011. Big data data. *SearchbusinessAnalytics*. http://searchcloudcomputing.techtarget.com/definition/big-data-Big-Data.

[31] Rouse, M. 2012. Social media analytic. http://searchbusinessanalytics.techtarget.com/definition/social-media-analytics.

[32] Leibowitz, J., J, C., Rosch, T., Ramirez, E., Brill, J., & Ohlhausen, M. K. February 2013. Order to file special raport.

[33] 2013. Big data impact and benefits. http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Big-Data-Impacts-and-Benefits.aspx.

[34] Nielsen, J. K. april 2012. Social business and big data: the business intelligence goldmine. http://www.socialmarketingforum.net/2013/01/social-business-and-big-data-the-business-intelligence-goldmine/.

[35] commision, E. july 2013. collaborate with national data protection supervisory authorities. http://ec.europa.eu/justice/data-protection/data-collection/index_en.htm.

[36] What are browser extensions or add-ons and how to install them. Guiding Tech. http://www.guidingtech.com/8005/beginners-guide-to-browser-extensions-add-ons/.

[37] FireFox. Fire fox privacy add-ons. https://addons.mozilla.org/en-US/firefox/collections/mozilla/privacy/.

[38] Stackpole, B. october 2011. Big data prep: 5 things it should do now. *computerworld*. http://www.infoworld.com/d/business-intelligence/big-data-prep-5-things-it-should-do-now-177090.

[39] Rouse, M. april 2010. unstructured data. *SearchbusinessAnalytics*.

[40] Wikipedia. may 2013. Chief information security officer. http://en.wikipedia.org/wiki/Chief_information_security_officer/.

[41] Embo & Macmillan. September 2012. The changing privacy landscape in the era of big data. *Molecular Systems Biology 8:612*. Article number 612.

[42] Ashford, W. Jun 2013. Consumers demand action to protect their privacy online. *computerweekly*. http://www.computerweekly.com/news/2240186687/Consumers-demand-action-to-protect-their-privacy-online.

[43] Ashford, W. may 2012. Ico reviews google wifi snooping investigation following us report. *computerweekly*. http://www.computerweekly.com/news/2240150886/UK-reviews-US-report-on-Google-WiFi-snooping.

[44] Wikipedia. 2013. Apache hadoop.

[45] HP Info world, H. Nov 2012. A next generation strategy for big data. *Converged Storage, IDG Dossier*.

[46] Meiko Jensen; Independent Centre for Privacy Protection Schleswig-Holstein (ULD) Kiel, G. 2013. Challenges of privacy protection in big data analytics. Molecular Systems Biology 8:612.

[47] information security agancy, E. February 2010. As soon as it happen. http://www.enisa.europa.eu/publications/archive/onlineasithappens.

[48] Google. Google policy privacy. http://www.google.com/intl/en/policies/privacy/. Last modified on June 24, 2013.

[49] Google. Anonymous identifier. http://www.google.com/intl/en/policies/privacy/key-terms/#toc-terms-identifier. Last modified onJune 24, 2013.

[50] LinkedIn. Your privacy matters. http://www.linkedin.com/legal/privacy-policy. Last modified on September 12, 2013.

[51] Wills, B. K. M. E. 2007. Measuring privacy loss and the impact of privacy protection in web browsing. IEEE.

[52] Addblock. Wikipedia. last modified on May.2013.

[53] Bugmenot. Wikipedia. last modified on October.2013.

[54] Room, S. 2010. The new eu cookie rule – so, we need to get consent then? Computerweekly. http://www.computerweekly.com/opinion/The-new-EU-cookie-rule-so-we-need-to-get-consent-then.

[55] Solove, D. J. November 2012. Privacy self-management and the consent dilemma. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2171018. Social science Research Network.

[56] Lee, A. B. *Data protetin law*, chapter 3, 58. 10. 2002.

[57] Castelluccia, C. & Narayanan, A. October 2012. Privacy considerations of online behavioural tracking. IEEE.

[58] Enisa. june 2010. Article 29 data protection working party. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf.

[59] commision, E. january 2012. Commission proposes a comprehensive reform of the data protection rules. http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm.

[60] Singleton, S. & Ustaran, E. *Data protection act*, chapter 1, 9 and 29. 2. 2007.

[61] What is consent. Office of the privacy comissioner in Canada. http://www.priv.gc.ca/resource/tool-outil/english/toolbox_primer-on-consent.asp.

[62] FUSTER, G. G., HERT, P. D., & GUTWIRTH, S. 2011. Privacy and data protection in the eu security continum. www.ceps.eu. Index policy brief No. 12/June 2011.

[63] commision, E. June 2011. How will the eu's data protection reform benefit european businesses? http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/7_en.pdf.

[64] Facebook. Data use policy. https://www.facebook.com/about/privacy. Last updated on December 11, 2012.

[65] Powering truste in the data economy. TRUSTe. http://www.truste.com.

[66] Lacy, D. 2009. *Managing the human factor in information security*. Wiley.

[67] November 2010. Summary of replies to the public consultation about the future legal framework for protecting personal data. European comission direcorate-general justice.

Appendices

A Interview questions with Norwegian data protection authority

1. Except for what has been defined in EU commission as data protection regulation what specific the Norwegian authority consider in order to protect personal data.
2. Have Norwegian data protection authority ever done a survey to examine how many people are confident and consent regarding Big data analytic processes? If yes describe a little bit?
3. What is the potential of privacy risk with regard to using dataset collected by aggregator? Is there any particular policy or regulation Norwegian authority would define?
4. How they control website and business companies if they are collecting data legally?
5. In the website it has been mentioned that Norwegian data protection Authority has asked some question of Facebook with regard to privacy concern? Does the answers make new policy requirement to protect user's information?
6. How much cost spend on privacy protection level
7. With regarding to the privacy awareness plan or campaign what This Authority organization does in business side and User or customer side?
8. With respect to that user are doing online shopping, and sharing their personal info over the net, etc.? How many Norwegian you estimate that is engaged in social business and social media activities?
9. Is there any training and awareness plan in the TV or schools?
10. How you get aware if big data analytic provider cross the legal and board?
11. There is an optimal privacy protection level, how you estimate in the specific case of Norwegian user.
12. How you see the future of collecting data involving in business , customer acceptance ? Do you think for having the privacy protection is enough to have policy regulation?

B Changes key on data protection principles

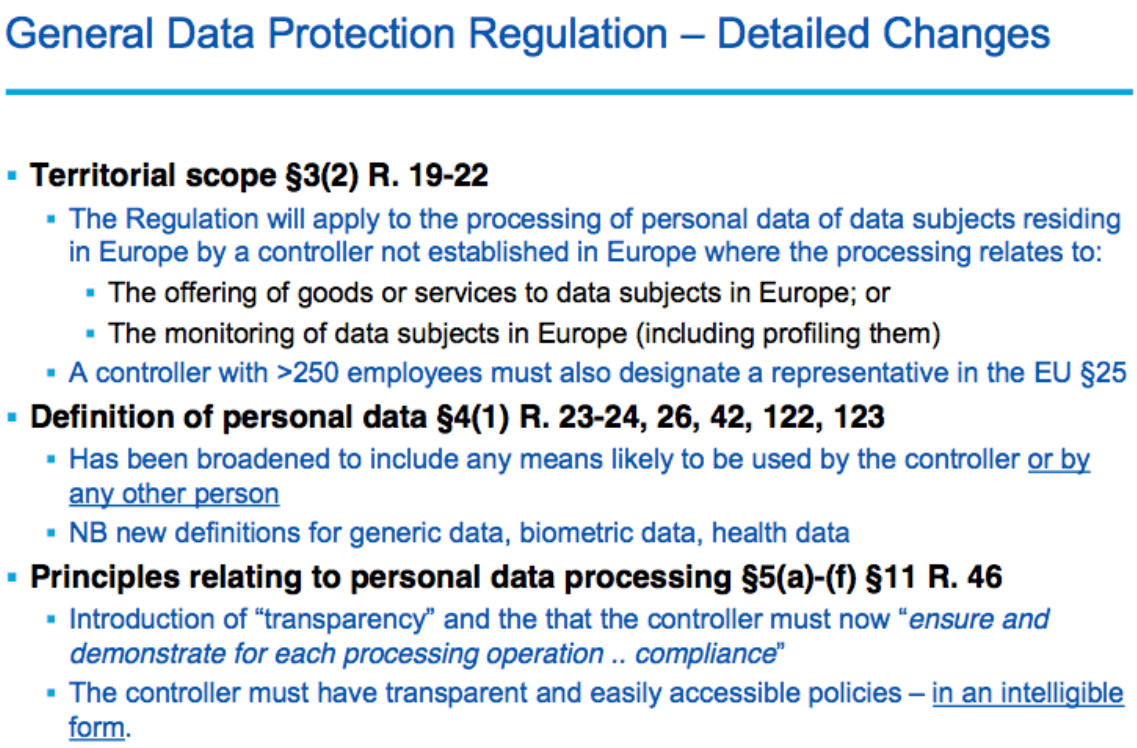

Figure 24: Detail changes on data protection regulations[12]

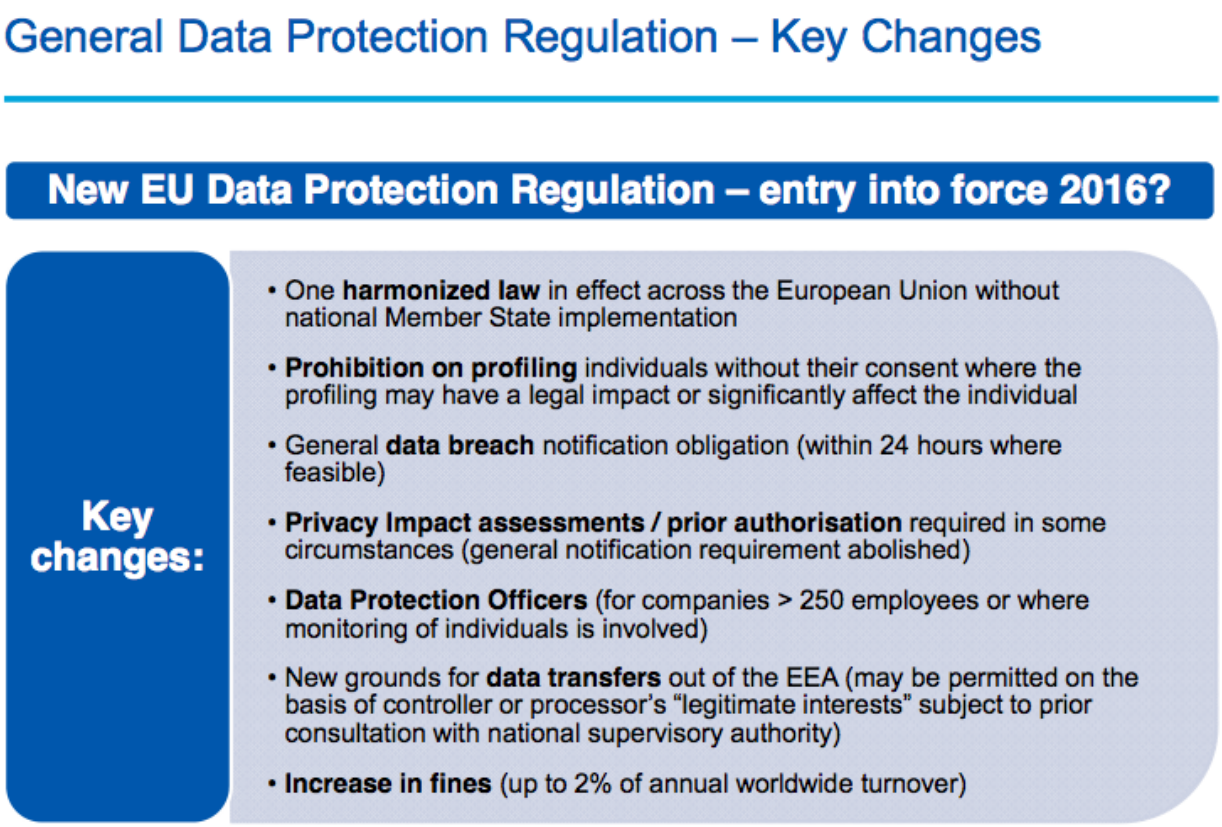

Figure 25: Key changes perspective[12]

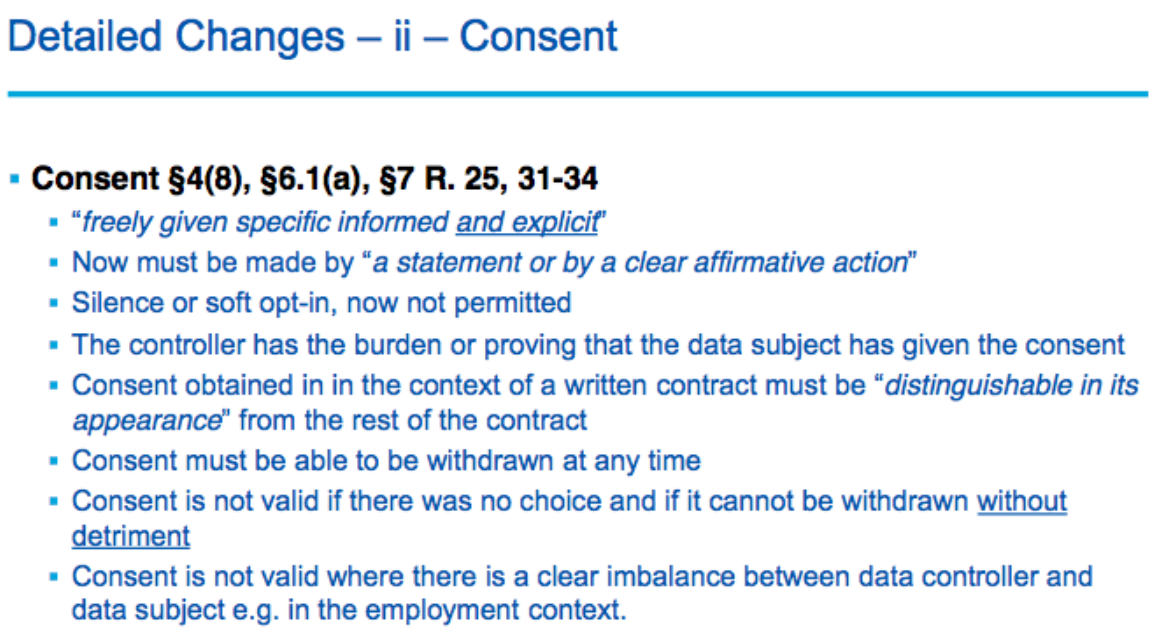

Figure 26: Consent perspective[12]

C American user behavior on privacy online conducted by TRUSTe

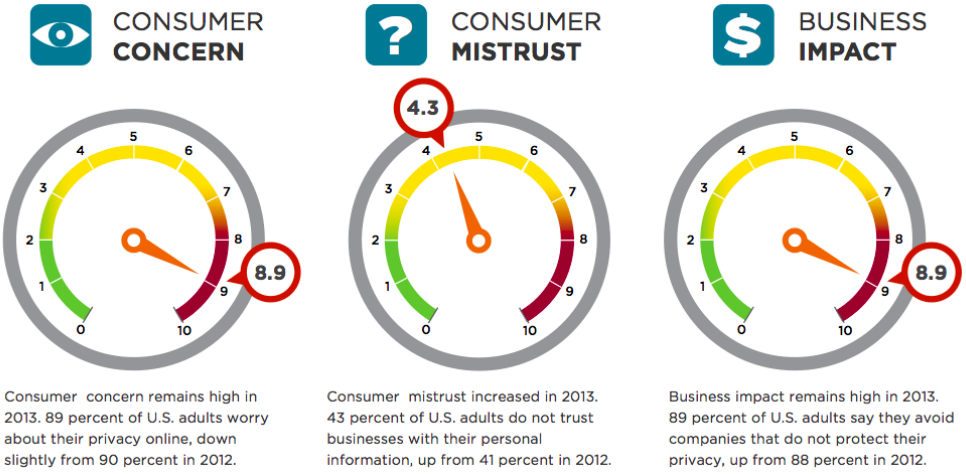

Figure 27: User behavior on privacy online[11]

C.1 American consumer concern

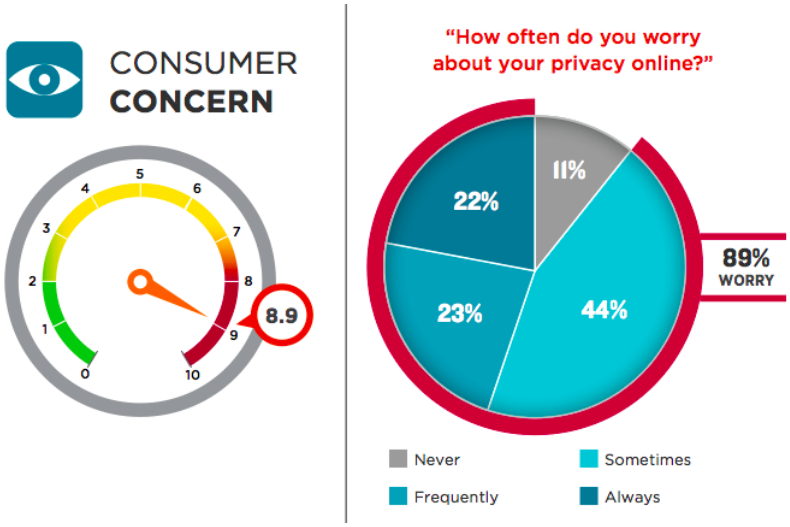

Figure 28: User behavior on privacy online[11]

C.2 Amercian Consumer trust on companies

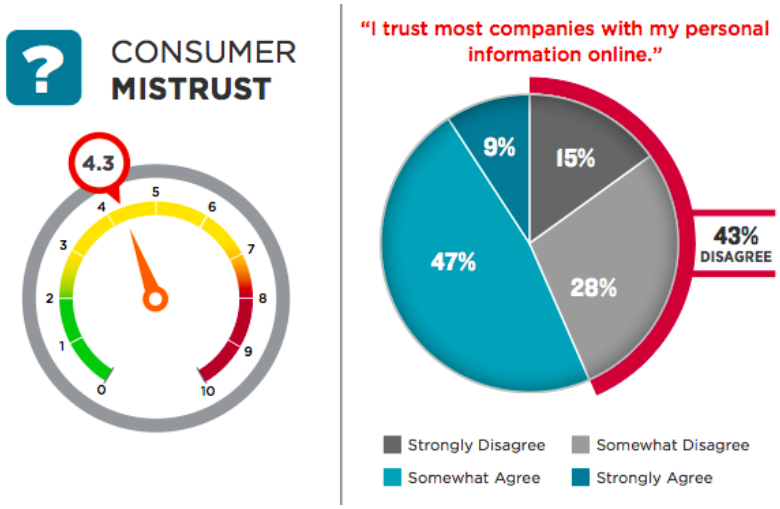

Figure 29: User behavior on privacy online[11]

D Demographic of Participants in the survey done by students from university of Salerno

demographic.jpg

Variables		*non-ICT* Group	*ICT* Group	*Chi-Square* Sig. Level
Gender	Male	28%	67%	0.0194
	Female	72%	33%	
Age	20-23 years	33%	44%	N.S.
	24-26 years	61%	50%	
	27-32 years	6%	6%	
Education	Bachelors	50%	11%	0.0113
	Masters	50%	89%	
Time spent online per day	0-2 hours	17%	0%	0.0351
	2-6 hours	72%	50%	
	6+	11%	50%	
Internet Expertise	Inexpert	83%	28%	0.0065
	Competent	17%	33%	
	Expert	0%	39%	

Figure 30: Participant demographic[3]