Information privacy and applications
A case study of user behaviours and attitudes in Norway

Hanna Kaupang

Master Thesis in Media Studies

Institute of Media and Communications

Faculty of Humanities

University of Oslo

December 2014

Year: 2014

Title: Information privacy and applications. A case study of user behaviours and attitudes in Norway

Author: Hanna Kaupang

http://www.duo.uio.no

Print: Reprosentralen, University of Oslo

Abstract

A recent study conducted in Norway shows that there has been a rise in concern about information privacy in the general population. However, as the study, presented by Datatilsynet and Teknologirådet (NDPA and NBT) (2014) shows; most respondents are not willing to sacrifice the convenience of applications to protect their information privacy. This lack in correlation between concern and action is what has been termed "the privacy paradox". In a study cited by Norberg, Horne & Horne they found "that higher levels of trust were related to increased willingness to provide personal information" (2007, p. 107). The argument was that the privacy paradox might be connected to trust.

In this master thesis I have made an attempt to uncover if the privacy paradox might be a reality in Norway. By asking two different groups of respondents about what they consider private information, and how they in turn protect that information, I have made an attempt to uncover whether the respondents act upon their concern for privacy in their everyday use of applications. In an attempt at understanding why there is a lack in correlation between concern and behaviour, I applied a variable of trust. Considering the general assumption that Norwegians have a high level of general trust towards others, I also interviewed a group of German students to see if their concerns and actions would vary from the Norwegians and if that could be explained by general trust. To stimulate the groups to think about how they would protect their personal information, I demonstrated a recent application, named "ValYou".

First of all, I found that the German group of respondents demonstrated a more sceptical view on how their information was stored and used online, than the Norwegian group did. The former group was also more informed about threats to the privacy of their information, but did not seem to act upon that concern. They admitted to trade off their privacy concerns for the convenience of an application. The Norwegian group admitted to not take many precautions in their everyday use of application, which could be explained by the groups' high level of general trust (GT). The latter argument would consider the privacy paradox to be more of a reality in the German group, considering their apparent trade off. The attitudes and behaviours amongst the two groups could be argued to be connected to trust, on two different levels.

Preface

Before I started working on this project I did not anticipate the emotional roller coaster I was about to enter. A master project is a lot of work! With that said, it has also been a great experience with many wins. I have many people to thank for their help, practically, emotionally and financially.

First and foremost, I want to thank my project supervisor, Charles Ess, for the all the help with the project, his suggestions and willingness to give of his time to a project that was pressed for time. Your encouraging, generous and kind advice has been of immense value to a stressed out student.

I also want to thank Telenor, for providing financial aid in form of a grant, which made the whole difference in making time to write the report, and for their willingness to discuss and "brainstorm" in the early stages of the project. I also want to thank their representative Wenche Nag, who believed in the project from the beginning. That helped a lot!

Finally, I want to thank my family and friends for supporting and encouraging me, emotionally, practically and financially. You know who you are!

Hanna Kaupang
December 2014

Table of Contents

1 Introduction

Some would say that we have come a long way from the "Gold Rush"-resembling early days of the Internet and new technology, where trust levels were high and the Internet was like the Land of Opportunities. Some twenty years later, the Internet may still be the Land of Oportunites, maybe even more so. However, "[t]here is a fear that the sociality enabled by the Internet is like a Wild West, with good and bad people being mixed up in indiscernible ways." (Harper, 2014, p. 1). It could seem as though Harper is pointing to how new technology have enabled almost anybody to enter and make use of the internet to his or her delight, this meaning both the honest and dishonest. Nissenbaum claims that "[new technology] enables pervasive surveillance, massive databases and lightning-speed distribution of information across the globe." (2010, p. 1). Even though many might have negative associations to the word "surveillance", and maybe rightfully so, Nissenbaum's aspects can be argued to be positive to the world society at one point. The fundamental idea of surveillance can be argued to be for the protection of the people and thus benefit for the society. However, it cannot be overlooked that both "surveillance, massive databases and lightning-speed distribution of information" (Nissenbaum, 2010, p. 1) provides means and opportunity for harm on the society too.

Following the thoughts of Harper (2014), in this thesis I discuss this balance between opportunities and threats between new technology and information privacy, possibly with more weight on the threats. In the following section I describe the background the for research project starting with the opportunities of new technology.

1.1 Background

"Surveillance, massive databases and lightning-speed distribution of information" have provided the world society with extensive opportunities (Nissenbaum, 2010, p. 1). In general, new communications technology provides opportunities such as increased possibilities of communications across the globe. Such as the ability to communicate with the other side of the world in a matter of second, and reach the same place in within 24 hours (Nayab and Edwards, 2014). This has had a massive effect on the world society, e.g. decreasing several distances, actual, cultural, mental etc. between people across the world. One example of a benefit of this is how it is has become possible for a person that e.g. needs an urgent heart

transplant to have a new heart brought from the other side of the world in a short amount of time, or even travel to another country to receive an operation (Fenwick, 2014). In the health sector alone new technology are saving lives on many levels; from complex surgical instruments, to applications that locate people with CPR training in near proximity when someone has a heart attack (Baase, 2013, p. 357). The website "Google Flu Trends" is said to be able to detect influenza spread before others. This is made possible through monitoring certain search terms and the frequency of them (Landau, 2008). To put it into Nissenbaum's terms: Google use their massive databases of information and conduct surveillance their users to detect flu outbreaks. Furthermore, new technology has during the last century been a part of increasing global life expectancy from by 34 years from the 1900 and to year 2006 (from 30 years to 64 years). Where diseases would take many lives in earlier years, new technology has been a part of reducing the threat of these (Baase, 2013, p. 360).

It is not only in the health sector new technology has been a part of a shift in life quality. According to Baase, new technology helps developing countries increase economic growth (2013, p. 360). The Norwegian telecom company Telenor is providing countries such as Pakistan with mobile financial services. So-called "branchless banking" is expected to provide several benefits for the Pakistani people (Easypaisa, n.d.). The telecom company states that it is possible to reduce the amount of people without access to financial services by 20 per cent and creating 20 million new jobs by the year 2020. This in turn might increase the national BPN by 3 per cent (Telenor Pakistan, n.d.). These examples are merely a few of many of the positive consequences of new technology during the last years.

As noted in the first section of this chapter, Harper argues that the internet provides a mix of people with positive and negative intentions. Even though new technology brings benefits that are in some aspects quite literally keeping people alive, it seems as though that with every new technological advance, a new societal problem arise. "With PCs and floppy disks came computer viruses and the beginnings of huge challenge to the concept of copyright. With email came spam. With increased storage and speed came databases with details about our personal and financial lives" (Baase, 2013, p. 23).

Media are increasingly reporting of breaches in information privacy; about the information privacy invasion of ordinary people. Identity theft, stolen passwords and surveillance seems to be just a few of the crimes committed today. In the early days of August 2014, 25 000

peopled sued Facebook Ireland for breach of information privacy and illegal sharing of personal information about the European users, to the American mother company. The information privacy regulations in Europe was said to be more rigid than the American regulations. However, Facebook was accused of taking advantage of so-called loop holes (Njie, 2014). The previous day, the Norwegian newspaper, *Aftenposten*, reported that Facebook was implementing a new privacy policy allowing them to see what you and I are doing when we are not logged on to the social networking site (SNS) (Lund, 2014). Facebook and Google have that in common that they gather and store a massive amount of information about their users, and analyse the information to sell to advertisers. These advertisers again use the information to target information directly at a smaller and smaller segment of the population, due to the fact that new technology is making it possible to target the consumers personally (Nisssenbaum, 2010; Baase, 2013). The users are enjoying the benefits of this when they search for something on Google, and the engine suggest something based on the information it already has. Information on Facebook is also filtered by algorithms made on the basis of userin formation. This could be argued to be a positive thing, because the fact is that new communications technology is providing endless amounts of information, too much information for any human being to process (Hildebrandt, 2013, p. 1). However, the most recent example of how it might be misused was shown when Edward Snowden leaked NASA documents showing that the US had conducted surveillance on ordinary people in and outside of the US, partially through the information found in Google and Facebook databases, amongst others. In this thesis I am not debating the Snowden-leaks. However, the case is used as an example to show that the information gathered in databases might also be used by someone meaning to cause harm.

The aim of this section have been to illustrate how new technology, which most people in the world are to some extent become reliant on, seem to provide negative and positive effects. In the following section I will narrow the scope onto the problem that motivated this thesis.

1.2 The problem

According to the survey conducted by the Norwegian Board of Technology (NBT) and the Norwegian Data Protection Authority (NDPA), the majority of Norwegians are more concerned about what their information is used for in the online sphere, than they were few years ago. This is likely due to the increased media attention and scandals such as the

Snowden-leaks. None the less, the report states that the respondents does not seem to take any particular precautions to protect their information (Datatilsynet and Teknologirådet, 2014, p. 29). When the respondents in the survey were asked if they would be willing to pay a monthly fee of NOK100 to use the same online services, without giving up their information, the majority answered "no". As the authors pointed out; one should be careful to conclude on anything based on this finding, seeing that it might just be that the amount was too high. However, it seems to exemplify a notion: even though people are concerned or even very concerned about the protection of their information privacy, they still give their information to those who might violate it.

A popular term for this problem is "the privacy paradox" (Norberg, Horne, & Horne, 2007) and has puzzled several researchers (see e.g. Nissenbaum, 2010; Norberg, Horne & Horne, 2007; Baek, 2014). Computer scientist Calvin Gottlieb stated that he did not think people really cared about information privacy, even though they would say they did when asked, because what they really wanted is the benefits provided when they give up their information in exchange for a good (as cited in Nissenbaum, 2010, p. 105). Smith, Dinev and Heng further noted on the paradox: "despite reported high privacy concerns, consumers still readily submit their personal information in a number of circumstances." (2011, p. 993). In a study cited by Norberg, Horne & Horne, findings attested to "that higher levels of trust were related to increased willingness to provide personal information" (2007, p. 107).

It would seem as though trust is a key concept to in the question as to why there is such a problem as the privacy paradox. In NBT and NDPAs report of their study on Norwegian's perceptions of information privacy, one of their remarks is that Norwegians are in general more trusting towards the government and therefore less prone to be concerned about information privacy than other countries (Datatilsynet and Teknologirådet, 2014, p. 29). This statement about trust may be strengthened by the 2011 report from OECD on trust as a social indicator, where Norway is the runner up of the countries with the highest levels of trust, next after Denmark. 89 per cent of the respondents expressed high levels of trust (p. 91). According to Jensen and Svendsen, high general social trust (GT) is often seen in welfare societies. In the same report from OECD, Germany, scores lower in GT. Ranking in the 15 place in GT, the European country seems to have a significant lower level of GT.

As previously described, new technology brings both opportunities and threats for its users, and one of those is what is often referred to as globalisation. The world community is becoming increasingly smaller and more integrated. E.g. Norway is more and more influenced by the US, Facebook and Google. According to Emarketer (2014) 75 per cent of internet users in Norway are also Facebook members, placing Norway in the top of the countries in the world with the highest amount of Facebook users. Which means that Facebook has a vast amount of information about Norwegian users. NBT and NDPA points out that even though Norwegians are protected by Norwegian laws within Norway, it does not apply in e.g. the US. This became visible when the NSA had conducted surveillance on Norwegian users on Facebook and Google amongst others (Datatilsynet and Teknologirådet, 2014, p. 23). The point of this argument is that even though there is a high GT in Norway, when information about Norwegian users are increasingly found in foreign databases, run by people that does not live in the welfare society of Norway, a problem might arise when the providers of the data bases cannot be trusted. I will discuss the welfare society, GT and trust in relationship with information privacy in the literature chapter of this thesis.

In this section I have described the problem of the privacy paradox, and the how it seems as though the Norwegians view information privacy. Even though I attach the privacy paradox to the current situation in Norway in this section, it is merely to introduce the paradox. In this thesis one of the aims is to uncover if the privacy paradox is a reality in Norway and thus a possible part of the explanation of why the Norwegian population are not acting upon their concern for information privacy. In the next section I describe the research questions of this thesis.

1.3 Research Questions

It could be argued that the focus in the NBT and NDPA survey is to some extent on the Snowden-leaks and the Norwegian population's concern for information privacy (Datatilsynet and Teknologirådet, 2014). When the report attempts to explain why the majority of the respondents state that they are concerned, but does not take any measures to protect their information privacy, the NBT and NDPA comments that the respondents does not understand the issue (Datatilsynet and Teknologirådet, 2014, p. 32). It seems understandable that it is difficult to relate to the ramifications of governmental surveillance when the respondents live in the protected country of Norway. Therefore, in this thesis, I

have asked questions focusing on the respondent's everyday lives. I operationalize the meaning of "everyday lives" for this thesis in the operationalization chapter.

By using the qualitative method of group interviews, where I asked groups with different nationalities about information privacy, the aim was both general and specific: in general I wanted to explore the respondent's attitudes towards new technology and information privacy in their everyday lives. In the specifics I wished to explore the possibility of the privacy paradox being a reality in Norway. Hence, I asked the following research questions;

RQ1

Does protection of information privacy affect people in their everyday use of new technology? E.g. will the uncertainty of what an application will do with personal information about an individual, hinder that individual in making use of it?

RQ2

Is there any reason to believe that the privacy paradox is a reality in Norway and can it be traced back to the high levels of trust amongst the population?

In the chapter on operationalization I explain what I mean by "affect", "everyday lives", "applications" and "trust". I write about the privacy paradox at length in the literature chapter.

For many people, especially the younger generations, the use of new technology have become a natural part of life. On average people look at their mobile phones 150 times during a day (Datatilsynet and Teknologirådet, 2014, p. 37). When something is a part of our everyday lives, it is sometimes difficult to view it from an outside point of view; we might be wearing blinders for a number of issues. To assist the respondents in their reflection on new technology and information privacy I made use of a so-called stimulus material in the group interviews.

1.4 Stimulus Materials

Stimulus materials are basically materials in many shapes and forms brought into an interview with the sole purpose of focusing the respondents on a topic (Barbour, 2014, p.

141). In a study about communicating health risks due to medical treatment, lifestyle, and more to patients, researchers found that people found it easier to understand and remember information about risk when it was presented through a visual aid (Garcia-Retamero & Cokely, 2013).

Most people would answer "yes" if they were asked about whether they were concerned about information privacy, if they were asked with regard to surveillance, Snowden-leaks and Facebook. However, the same people might download an app without thinking that it might have implications for their information privacy as well. In order for the respondents to grasp the concept of information privacy I have made use of a visual stimulus in the group interview to help the respondents visualise a problem.

The application that was used as stimuli is not a revolutionary application, nor does it present any higher levels of risk than other applications. However, the intention behind making use of this application was to present a new product that the respondents had not encountered before, and therefore start a thought process that might help the respondents think about their daily encounters with information privacy. The stimulus I made use of was the application ValYou, which is a newly developed payment application, created to simplify card payments. It is new to the users, because it enables a smartphone with the right technology to function as a credit card, and it simplifies the transaction process (ValYou, n.d.). The reason why it might make the respondents reflect on their information privacy is because it creates another function for the smartphone, and another threat for information privacy invasion.

In the previous sections I have discussed the problem with information privacy, the questions I asked to explore the problem and a part of the methodologies applied to answer the questions. In the following section I reflect on the expected findings in this thesis.

1.5 What did I plan to find?

The "consumer-protection view" of information privacy tries to explain the privacy paradox by noting that consumers in general are not aware of the risks they put themselves in when they venture into the online sphere and that they need to be protected. The supporters of this view argue that the solution is regulating the businesses, and leaving less of the responsibility with the consumers (Baase, 2013, p. 127). The discussion of whose responsibility it is to

protect the consumers' information privacy is one that I will not venture into in this thesis. However, there seems to be some reason in the view that people in general are more or less ignorant of many aspects of the use of their information (Baase, 2013, p. 128). That might be why the NBT and NDPA find that the Norwegian people seem to not be able to relate to the issues of privacy (Datatilsynet & Teknologirådet, 2014, p. 32). In his discussion on trust in the online sphere, Harper claims that most people operate on a sort of unsteady ground whilst being online, where they most of the time sacrifice the security of trusting the other end of the online transaction, for e.g. convenience (2014, p. 18).

Based on previous studies on information privacy in general, the findings in the NBT and NDPA survey, and personal conversations with Norwegians I expected to find that the privacy paradox is a reality in Norway. Even though the general population say that they are concerned for their information privacy (Datatilsynet & Teknologirådet, 2014) I expected to find that few let the protection of their privacy affect their everyday use of new technology. When interviewing a group of young Norwegians parallel with a group of young German students, I expected to find that the Norwegian students act less on their concern for information privacy due to the fact that the Norwegian population are said to have a high level of GT (OECD, 2011). By interviewing a group that came from a country with significantly lower levels GT (OECD, 2011), I expected to find both more scepticism and that more of the respondents let information privacy affect their everyday use of new technology in the German group, than in the Norwegian group.

I have now briefly described what I expected to find when I started the work on this research project. I will now continue to discuss why it is of importance to study the topic of information privacy.

1.6 Why study this topic?

Most of the researchers that have set out to research and define privacy and information privacy seem to have arrived at the same conclusion; it is too complex of a concept to define in one sentence (see e.g. Nissenbaum, 2010; Solove, 2008; Baase, 2013). Even though the opinions are many, this notion seems to be unanimous. General privacy is a topic within law, philosophy and psychology, amongst other areas (Baek, 2014), and have been researched for more than a century (Warren and Brandeis, 1890). An essential question to ask when

planning a research project is if it will add anything to the existing research (Everett & Furuseth, 2012), and by reviewing the existing privacy literature at a glance, it is easy conclude that the topic of information privacy is covered. However, as Hildebrandt (2013) argues technology has been changing the society for the last decade, and by the looks of it, it still is. As described earlier on in this introduction, new technology is causing major shifts in society that in turn presents people with new challenges to their information privacy. In the following section I point to a few facts that describe the situation within new technology and how it seems to push the limits of people's private lives. I will mention a few definitions and concepts of privacy and information privacy that will be discussed more at length in the literature chapter. In the literature chapter I also discuss the difference between privacy and information privacy.

1.6.1 Technology and innovation

Studies conducted in 2011 discovered that of the 340 most popular free applications at that time, only 19 per cent of them had a privacy policy at all. Furthermore, in 2012, a study conducted on the 101 most popular applications, above half of them transmitted information about their users to third parties (2013). Today, at the end of the year 2014, this information will be out-dated, and many of the application providers in question will have redeemed themselves. However, the rapid development in new technology continues to produce new technology and make it easier for anybody to become an application developer, which means that more and more providers without the necessary background in business and ethics will enter the market, which again indicate that the issue of personal information leaking out of applications might be a continuous problem. Furthermore, when talking about personal information, it is easy to assume that it is limited to the data people voluntarily plot in to create user accounts and so on. However, as location based applications are becoming increasingly popular, and the possibility of accessing free Wi-Fi in many public areas, the amount of online information about us is much more than just our name and address. So-called "wearable technology" is a category of new technology that is opening up a wider scope of available information about the users.

The industry expect the amount of wearable technology products on the market to be eight times as high by 2017 (Tekonologirådet & Datatilsynet, 2014, p. 36). One of the latest editions is the Apple Watch, which was released earlier this autumn and stirred questions

regarding information privacy even before its release. Sharing the same features as other wearable technology, the Apple Watch is designed to be a part of the consumer, not only an accessory. It is designed to follow the natural body movements of its owner. E.g. the watch's display turns on when it senses that the user lift his arm to look at it (Apple, n.d.). Wearable technology is created to observe and analyse the consumers' habits to help him in his everyday life without having to activate it (Datatilsynet and Teknologirådet, 2014, p. 36). One of the major controversies about this watch has been how it is created to track health information, such as heartbeats. The watch doubles as a fitness device, and the Attorney General in Connecticut is only one of the many that have expressed concern about how this information is stored and protected (Ribeiro, 2014)

Wearable technology is created to aid its owner, and be of benefit. However, increased usability comes at a cost. The fact that more information about you and your surroundings are recorded is only one of the potential issues. If the applications continue to have poor or none privacy policies, or freely sell their consumers information to third parties, the consequences will be many more breaches in information privacy. With the ever-developing industry of new technology, and innovative products that come closer and closer to our person, it is sound to say that the topic of information privacy is not yet exhausted. If Lekanger (2013) is right when saying that Norway is in the global top of countries with the highest penetration of new technology it seems legitimate to investigate why Norwegians seems to be taking few precautions in their use of new technology. In the previous paragraphs I have described new technologies possible threats to information privacy and why it is of value to continue to study the topic, especially in the context of Norway. In the following paragraphs I will discuss two more arguments to why it is of value to continue to research the topic of information privacy and new technology, starting with how drastic changes might affect the booming business applications.

1.6.2 The Golden Age of Applications

In the previous section I have described how new technology seems to demand more research on information privacy, due to the fact that it could be argued to continuously create new challenges (Baase, 2013). As mentioned earlier on in the introduction, no researcher has been able to define privacy in a short sentence. The fact that it is a debated topic, were some argues that information privacy is dead and that the efforts to protect it ruins the free internet

(Nissenbaum, 2010) and others, such as the ones advocating the consumer protection view, argue that it is the lawmakers responsibility to make sure people's information privacy is protected (Baase, 2013), creates challenges for the lawmakers.

At the first glance, it would seem as though the industry of application development is seeing exponential growth because people seem to act little upon their concerns for information privacy, and the lawmakers are not agreeing on how to protect them. Newcomers in the digital markets thrive on the consumers' enthusiasm and eagerness to try out the latest application, where they gladly sign up and tick the box that says "I agree to the terms" without reading the terms. The application ValYou is one of the newcomers that are relying on a widespread enthusiasm for the product to be successful. However, if the development is heading where some say that it is; that along with the rapid growth in new technology, the challenges will be greater and people will grow more sceptical, many of the businesses of today will face serious issues (Nissenbaum, 2010). It would seem like a reasonable argument to say that to continue the research on information privacy in the context of new technology, to ensure that the growth continues. In the following is section of this chapter is a third and final argument as to why it is of value to continue to research the topic of information privacy. Previously I have described the situation from an individual point of view, then a business point of view, and in the next section I describe the value of information privacy from a societal point of view.

1.6.3 Privacy and democracy

Philosophers in the privacy debate claim that the loss of privacy and information privacy may equal loss of autonomy. It is a core idea that a well-functioning individual in a democratic society is an autonomous one. Researchers say that the ultimate consequence of the loss of autonomy is the loss of democracy as we know it, seeing that one of the fundamental ideas of privacy is that it is needed for autonomy and the development of the autonomous self that make sound well-thought through decisions (Van der Hilst, 2013). Furthermore, privacy in general is said to enable peoples' ability to develop their identity and their psychological well-being. Rachels explains this by the notion that it is natural to "put on" a different nature whilst out in public, and then to proceed to relax and "be yourself" in the comfort of your own home and so on (1975). By being able to retreat into a private sphere, Rachels argues is positive for the maintenance of a healthy psyche, which is arguably a value for the

democracy. As I discuss in the literature chapter, Nissenbaum connects the effects of loss of general privacy to the loss of information privacy.

In these sections I have described two of many rationales as to why it is of value to continue to study the topic of privacy and new technology. I have described it from an individual, business and societal point of view. These three are merely examples of many rationales that could be presented to argue for the value of this research project. In the following chapter I briefly describe the structure of this thesis, before I go on to review the relevant literature.

1.7 Structure

To summarize and re-cap on the introduction: in a combination of reviewing the excising literature on privacy, previous similar research, combined with empirical research interviews I wish to answer two main research questions:

RQ1

Does protection of information privacy affect users in their everyday use of new technology? E.g. does the lack of a privacy policy in an application affect their decision to download it?

RQ2

Is there any reason to believe that the privacy paradox is a reality in Norway and can it be traced back to the high levels of trust amongst the population?

In the following chapter will review what I regard as relevant literature on privacy, information privacy and new technology. I will then go on to provide an overview of the method be provided, including operationalization of terms in use. In the fifth chapter I give an account for the limitation of this master project. Furthermore, I will report and analyse the findings in the research interviews. In the seventh chapter I will discuss of the findings in the light of the previously stated literature. I end this report by summarizing and suggesting further research.

2 Literature

In the introductory chapter I have referred to various definitions and notions about privacy. In this chapter I will discuss privacy, previous research and other relevant literature that form the basis for this research project. I start by accounting for a few of the basic notions of privacy in general.

2.1 What is privacy?

One of the very basic notions of privacy was explained by Rachels in 1975; privacy is the need or want to be "free from certain kind of intrusions" (p. 1). The Oxford English Dictionary defines privacy similar words: "the state or condition of being withdrawn from the society of others or from public attention; freedom from disturbance or intrusion." (n.d.) Reiman's explanaition of privacy is that it is "the condition under which other people are deprived of access to either some information about you or some experience of you" (van der Hilst, 2013, p. 53). These definitions stem from different schools of privacy thought, which will be discussed further in a later section. Nevertheless, they seem to have common denominator, which is captured in what Warren and Brandeis, who are said to have sparked the public debate on privacy, stated about privacy: "the right to be let alone" (Nissenbaum, 2010, p. 19)

So why do we need privacy? Why do we need to be withdrawn from others? Law professor Julie Cohen argues that privacy constitutes a "breathing room to engage in the process of boundary management that enable and constitute self-development" (2013, p. 1906). The idea of privacy seems to include that all individuals have a need to retreat from the public sphere to develop and flourish in our own selves. Solove distinguish between the two spheres, which he regards as equally important for a human life, in these words:

> [The public sphere is] the realm of life experienced in the open, in the community, and in the world of politics. [The private sphere] is the realm where one retreats to isolation or to one's family. [It is] the realm where the individual "is not bound by the rules that govern public life" […] The private life is a secluded life, a life separated from the compelling burdens of public authority. (2011, p. 41)

According to Solove, Rachels and other researchers, it seems as though that to be able to flourish in both spheres, the balance between the two is of essence. An individual needs to withdraw from the eyes of the world to develop the individual autonomous self, and additionally to step back into the public sphere to test and develop that self in cooperation and negotiation with other people (2011; 1975) It seems fairly simple to apply these notions to the daily life. As a master student of media studies it is easy to enter into a certain mode whilst being with peers, and being fully that person. However, to be able to form independent opinions, accumulate knowledge to fuel discussions and aid other students in their processes, it is vital to have the ability to withdraw to the privacy of one's own home, to think, read and discuss with close relationships.

Reiman compare the loss of privacy as living in a fishbowl, knowingly being observed at all times (2010, p. 75). Nissenbaum draws a parallel with the fishbowl into topic of information privacy. She argues that some organisations have the potential to look into "our fishbowl" (2010, p. 75). In Reiman's discussion of privacy, he accounts for four types of risk, two of them being extrinsic and intrinsic loss of freedom (Nissenbaum, 2010, p. 75). Nissenbaum's explanation of these two types of freedom might be exemplified with Rachel's portrayal of a wife spying on her husband when he thinks he is home alone. The wife is of the opinion that her husband would never do anything strange whilst alone, because "real people aren't any different when they're alone. No masks. What you see of them is authentic." (Rachels, 1975, p. 1). However, when looking through their living room window, she finds to her shock that her husband is parading around the living room pretending he is a military sergeant commanding his troops (Rachels, 1975, p. 1). If the husband would have been aware of that he had onlookers, and seeing that his wife had never seen this side of him, it would be reasonable to assume that he would feel that he lost his freedom.

> This occurs as those being watched begin to view themselves and their actions from the perspective of those watching. They are thus deprived of spontaneity and full agency as they self-consciously formulate plans and actions from this third party perspective. Privacy […] functions as "as a means of protecting freedom, moral personality, and a rich and critical inner life (Nissenbaum, 2010, p. 75).

A society is comprised of its individuals. It is reasonable to assume that if privacy is beneficial for the individual, it is also beneficial for the society. This notion may be explained in what Nissenbaum discuss as the collective value of society (2010). It is of value for the

entire society when individual privacy is granted, due to the fact that the need to be free from certain kind of intrusions is an essential part of a human beings ability to be an autonomous well-functioning part of society (as cited in Nissenbaum, 2010, p. 76). Furthermore, it is also argued that the core of a well-functioning democracy includes autonomous individuals, with the ability to decide for their own (Van der Hilst, 2013)

Some of the contradictory arguments on these notions of privacy are stating that privacy is just for the people with something to hide, and that privacy gives cover to criminal activity. Another argument is that instead of aiding those who are timid and do not want to express their opinions unless under an alias with privacy, the timid ones should grow strong enough to stand up for their opinions (Nissenbaum, 2010, p. 76). However, Nissenbaum argues that these notions, especially the latter, are idealistic notions of how a society should be, but that that is not the situation, and a society should strive to make their inhabitants thrive. She further notes that in "liberal, non-totalitarian societies significant areas of life are protected from public regulation" (Nissenbaum, 2010, p. 76). It seems essential for an individual to be assured privacy, both for the reason of individual development and psychological well-being as well as for the well-being of their relationships, according to Rachels (1975, p. 1). It also extends to an importance for the society, as an autonomous individual will add to a vibrant and well-functioning democracy.

These basic arguments of what privacy is for an individual and thus for the society, form the rationale of the importance for privacy in the society as briefly, discussed in the chapter where I argued why this research project is of value. In the following section I will continue to review research that argue for the value of privacy for the individual and society, when I give an account of two different schools of thought within privacy, "value-based definitions" and "cognate-based definitions".

2.2 Different schools of thought

In the search for a definition of privacy, two sets of "schools" have emerged: the "value-based definitions" and the "cognate-based definitions" (Smith et.al., 2011, p. 993). The first definitions that surfaced was value-based and one of them was fathered by Warren and Brandeis; "the right to be let alone". Warren, Brandeis and others in the same "school" believed privacy to be a right or a basic human value. In the EU, privacy is included in the

European Convention on Human Rights (ECHR) (Article 8) and links privacy and thus a right to respect for one's "private and family life, his home and his correspondence" (2010, p. 10) to "Human Rights and Fundamental Freedoms" (2010, p. 5). Hence, the EU view on privacy could be viewed in within the value-based definitions of privacy.

The paradox, however, to this school of thought within privacy, is that it would seem as though people in general are willing to trade off this alleged basic human value, as a commodity (Smith et.al., 2011). This notion seems to be what makes the so-called dot.com-economy thrive. People are enclosing information about themselves to providers of Internet applications, smart phones and smartphone applications, amongst others. This is what has been termed "self-surveillance" and resembles the characteristics of the privacy paradox (Smith et.al., 2011, p. 994). As a result of this issue "[p]sychologists and cognitive scientists then became interested in producing a cognate-based conceptualization general privacy - related to the individual's mind, perceptions and cognition rather than to an absolute moral value or norm." (Smith et.al., 2011, p. 993-994)

In the school of privacy as being a state or something to "obtain", the definitions describing privacy as a form of control of own private life and information, such as the one to be found in the Oxford English Dictionary as mentioned in the previous section: privacy is "the state or condition of being withdrawn from the society of others or from public attention; freedom from disturbance or intrusion." (Stevenson, n.d.). Reiman's definition, as previously mentioned, can also be argued to belong to this school of thought: "the condition under which other people are deprived of access to either some information about you or some experience of you" (as cited in Nissenbaum, 2010, p. 70).

The followers of the cognate-based school's criticism of the value-based school seems reasonable in 2014 where many are willing to give up their privacy for the use of e.g. applications. It is easy to question how deep the value of privacy is when it is seemingly easy to trade it off. However, as I discuss in the analysis and discussion chapters, it would also seem as though people's view on privacy is not based on rational decision at all times, that some of them are connected to e.g. cultural view (Ess, 2013, p. 6). One example of this is how two of the respondents in the interview with the Norwegian group of respondents expressing a want to be out of the prying eye of the internet with everyday aspects of their lives, not because they wanted to hide something, but it was of value to them to have a space

where no one could see them (Appendix 3, Interview 2, Norwegian group, p.1). I will discuss this in more detail in the discussion chapter. However, the point in this discussion is that it would seem that the concepts of both the value-based and the cognate-based conceptions of privacy each on their own cannot explain or provide a full understanding of privacy. It seems like sort of a mission impossible to create a conception that covers all aspects of privacy. Nonetheless, a professor at the Department of Media, Culture and Communication, at the New York University, Helen Nissenbaum, have been praised by other scholars for creating a conception that seems to fit the dynamics of the new technology society of today. In the next chapter I discuss her concept called "Contextual Integrity".

2.3 Contextual Integrity

When respondents in a survey claim that they are concerned about the privacy of their information online, whilst simultaneously providing applications with a large amount of information about themselves, it is reasonable to become somewhat puzzled. As previously discussed, attempts have been made to explain the reasoning for this puzzle, in order to regulate privacy in the most beneficial manner. If the lawmakers are uncertain as to what is considered private information amongst the population, it is close to impossible to know what information to protect. Furthermore, the challenged new technology bring seems to call for more than one solution. In 1890, when Warren and Brandeis sparked the debate about privacy as the right to be let alone, the issue regarded how people should have a right to be let alone by the press (1890) This right to be let alone could be argued to be an easier right to enforce in a society without digital intrusions. Hence, the call for a more versatile concept may not be as critical.

Nissenbaum argues that the conceptions of privacy to some extent have failed to take context into account. "Observing how privacy norms vary across and within social groups, some critics have concluded that privacy is at best culturally relative predilection rather than a universal human value" (Nissenbaum, 2010, p. 129). In one sense, this conclusion would prove useful on several levels. E.g. the culture shock for a Norwegian travelling to India could prove to be less violent if the Norwegian does not believe that his point of view on privacy is a universal human value. For instance, the Norwegians sense of private space could quickly be invaded in a country where people sit on top of each other in public transport. Nissenbaum's concept also starts at this point, saying that privacy is relative to the

context of relationships. However, the conception extends further than just the social norms of different cultures. Nissenbaum is of the opinion that there is greater complexity in the variations and that it is connected to the context or the "back ground social situation" (Nissenbaum, 2010, p. 128). "The central thesis […] is that right to privacy is neither a right to secrecy nor a right to control but a right to appropriate flow of personal information" (Nissenbaum, 2010, p. 127). According to the Oxford Advanced Learners Dictionary, "context" means "circumstances in which [something] happens or in which [something] is to be considered" (Hornby and Cowie, 1990, p. 254).

Nissenbaum's definition of context is that they are social settings, such as activities, roles, norms and internal values (2010, p. 132). When privacy is considered within different contexts, it could be argued that it no longer seems unreasonable for people to convey more information about themselves in some settings than others. Contextual integrity argues that it is not necessarily an inconsistency to care about privacy and still share generously within certain contexts (Nissenbaum, 2010, p. 127). The concept thus argues for the necessity to keep the integrity of the context with an appropriate flow of information.

In the previous two chapters I have accounted for different definitions and schools of thought in privacy, ending with Nissenbaum's concept of contextual integrity, calling for a more dynamic and versatile conception of privacy (2010, p. 132). In the next section I continue the discussion in privacy by describing different types.

2.4 Types of privacy

Even though I have moved from the discussion of more basic definitions on privacy and onto the more dynamic concept of contextual integrity, I will now take a step back and look at different types of privacy, before I move on to discuss privacy and new technology.

2.4.1 Three types

In the story from Rachel's about the wife spying on her husband, privacy is physical. The husband was dependent on a room where there was no one watching him, to continue to act like he did (1975, p. 2). For most people it could be argued that their bathroom or bedroom would be considered their most intimate and private space, where other people usually have limited access (Rachels, 1975, p. 1). In this type of spatial privacy it seems easy to determine

the contextual norms. In most Western instances, it would be inappropriate for almost anyone to be present in someone's bedroom when they were sleeping (Ess, 2013). This spatial notion of privacy is often referred to as "accessibility privacy" and is one of three types of privacy summarized Tavani. Warren and Brandeis' "right to be let alone" is a part of this type of privacy (1890) The second type of privacy is decisional privacy, which describes the right to make individual decisions without the interference from others. In the US this type have been essential in the discussions on e.g. abortion (Ess, 2013, p. 17). The third and final type of privacy according to Tavani is called "informational privacy" and describes an ability to control our personal information (Ess, 2013, p. 17).

In general, the discussion about privacy in the research interviews conducted in this project focused on information privacy, and what the respondents regarded as personal information. The privacy debate is filled with overlapping theories, making it impossible to isolate information privacy completely from other types. However, to be able to produce a productive study, it is vital to narrow the scope. Thus, the following section will focus on what informational privacy may be understood as.

2.4.2 Information privacy

The late professor of Public Law and Government Emeritus, Alan Westin, defined privacy as "[t]he claim for individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." (As cited in Solove, 2008, p. 24). In the European Union, privacy of information (or data) is included in the "European Convention of Human Rights" and is intended to regulate the processing of personal data. By personal data, the EU means

> [P]ersonal data shall mean any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. (European Comission Directory C, 2007, p. 4)

§1 in the Norwegian law protecting privacy of information (in Norwegian: "Personopplysningsloven") states that

The law intends to protect the individual against violation of privacy through treatment of personal information. The law intends to contribute to that private information are treated in correlation to foundational privacy laws, including the need for personal integrity, "privatlivets fred" and adequate quality in personal information (Justis- og beredskapsdepartementet, 2013).

As discussed in the first section on privacy, Nissenbaum describes the informational fishbowl, where organisations in theory are able to know enough about people for their lives to become transparent like a fishbowl. Furthermore, a person in an illustrative fishbowl will most likely alter his actions based on the knowledge that someone is "watching them" (2010, p. 75). The ability for organisations to know about people's lives partially stems from their ability to store massive amounts of data, analyse it and identify people down to small details of their lives. Additionally, high speed internet has made it possible to transfer information across the world in a very amount of short time. For instance, many Norwegian users of several different services storing data in the "Cloud", are storing their information in servers outside of Norway. These servers are in turn not required to follow Norwegian laws on privacy (Datatilsynet and Teknologirådet, 2014, p. 23). This means that even though the Norwegians' information privacy might be safe in the protective laws of their own country, it does not necessarily mean that it is safe in the same way under the laws of other countries. Ess argues for instance that the EU laws on information privacy are stricter than the US laws (2013). It could be argued that the Norwegian populations' information privacy could be at risk if the population continues to disclose personal information to servers and providers, that are not as concerned about protecting the Norwegian people according to their laws as the Norwegian Government would be. Therefore this project's main focus is on how the respondents relate to the privacy of their information, versus privacy in general.

I have in this section discussed types of privacy and more specifically informational privacy. In the following sector I describe information privacy in the area of new technology.

2.5 Information privacy and new technology

Based on the previous accounts of privacy it may be assumed that human beings in general need and want it at some level. It may also be assumed that the level and degree of privacy varies based on context. New technology is one of the aspects creating various new contexts to how privacy is conceptualized. In the following section I describe some of the information

privacy challenges brought along with new technology. When discussing privacy along with new technologies I talk about information privacy.

Earlier this fall, Apple released its newest member of the "i-family", the "iPhone 6" and whilst the critics was unimpressed with the newcomer, the iPhone had some features that caused both excitement and concern. The phone was equipped with a program providing the possibility to monitor your own health conditions (in the same way as the Apple Watch, discussed earlier in this report). Whilst it could be a revolutionary program for many people, some have have also uttered the words "selection society". The author of a recent news article in the Norwegian newspaper *Aftenposten*, painted this picture:

> Your daily runs are not so much daily anymore, and your diet as derailed after the holidays. Your general physician sends you a text; he is worried. The next week, your insurance company calls to tell you that if you do not make some changes to your lifestyle right a way, you have to prepare for a rise in your insurance premium. (Amundsen, 2014, translated from Norwegian).

When we talk about the concerns of invasion of information privacy, it is easy to think big, to think surveillance, and in that sense it is easy to be in opposition to the government conducting surveillance on the people of a society, it is easy to protest against the surveillance of our government. However, with the amount of information we voluntary give out, every day, we seem to be inadvertently saying yes to surveillance after all (also called self-surveillance as discussed in the introduction). In 2013, five billion people had their own mobile phone. In 2014, Facebook had 1.35 billion users (Statista, 2014). According to Baase, everything we do online, everything we download on our smartphones links the computer or the phone to a database storing information about the device (2013). With smart phones containing more and more personal information about us as individuals, the databases also know much more. In a study done by researchers and journalists, it was discovered that many applications downloaded on a phone stored a copy of the phones contact list in a database, and some applications stored and even distributed a phone's images, when the application had been given access (Baase, 2013). When more and more details about us are stored and then put together for analysis, a more and more detailed picture of us as human beings are available online. However, who thinks about these facts when a very convenient application just arrived?

The new phones in 2014 have the ability to store health data, and function as a wallet. Technology is becoming increasingly personalized, and applications are in many ways making people's lives easier. There is a constant market for more, and the developers deliver. Furthermore, it seems as though some is of the opinion that information privacy is the hair in the soup called "convenience". Based on previous experience, it could be argued that information privacy and convenience cannot entirely co-exist. "Increasing privacy and security often means reducing convenience. Protecting privacy makes law enforcement more difficult. Unpleasant, offensive or inaccurate information accompanies our access to the Web's vast amounts of useful information" (Baase, 2013, p. 42).

In this section I have described a small portion of the challenges of information privacy and new technology. In the introduction I mentioned that it would seem as though the privacy paradox, is linked to trust. In the following section I discuss trust in the context on new technology.

2.6 Trust

Online interactions are transactions conducted between people. According to Clark, technology is merely the medium that makes the interaction possible. In the conversation on trust and computing, issues such as trust in security systems and so forth are often the topic at hand. However, Clark argues that the more essential point of trust lies in the people behind the technology (2014, p. 18). Furthermore, when interacting with an unknown person on the other side of a transaction people trust others online every time there is a transaction of any sort. In the example of applications, it would seem as though people have to trust the providers. Trust them to deliver the expected product, trust them to not overstep boundaries.

> Trust […] is a relationship between trustor and trustee in which the trustor is willing to assume that the trustee will act in the best interest of the trustor. This does not mean that the trustor can predict exactly what the behaviour of the trustee will be, but that the trustee will use judgement and intelligence to restrict the range of actions undertaken. (Clark, 2014, p. 17)

It could be argued that trust in general is "a leap of faith", due to the fact that one participant cannot know for certain that the other participant is trustworthy. However, as it is easy to

relate to in everyday life, the trustworthy participants often possess some merits that the others do not (i.e. good reputation) (Clark, 2014, p. 18).

Clark argues that there are three levels of trust in between the participants of an online transaction (2014, p. 18). The first two are the levels of either trusting completely the other participants or not trusting them at all. The people or organisations are trusted completely often possess a number of merits making them trustworthy, based on the other participants opinion. The people or organisations that are not trusted at all seem to also possess merits that tell the other participants not to trust them (Clark, 2014, p. 18). The third level, which Clark argues that most of online transactions operate on, is were the participants of the transaction does not trust the other entirely. Due to several reasons, it is impossible for one or both of the participants to know if the other party is trustworthy.

In the previous discussion on the privacy paradox, it would seem as though trust is interconnected with information privacy today, where people in general trust new technology and the Internet with their personal information multiple times a day. It could be argued that trust is seen in "Cloud-computing" were people the recent years have stared storing more of their data in the so-called "Cloud". "The Cloud" is an external server owned and run by an organisation (such as Apple), which stores data, and make it possible to access data from any device with a connection to the Cloud (Karigiannis, 2014, p. 39).

Other than cloud computing, search engines seem to be another area in which the online participants seem to trust, especially the search engine Google. "Just Google it" has been a popular phrase suggesting that Google has the answer to all questions (van Dijck, 2013, p. 7). Even though Google may have many answers, it cannot be said to provide unbiased answers. Based on a set of information and algorithms, the search engine decides the result of a search. What I see when I search the word "trust" might be entirely different than what my neighbour might see. According to Harper, "search engines take you to what companies want to sell, not to what you want to know" (2014, p. 4). Nonetheless, with Google's popularity, being the largest search engine in the world it could seem as though many people trust the search results to provide an array of quality answers regardless of its faults (van Djick, 2013). Google, Cloud-services and other new technologies are widely trusted to store vast amounts of people's information.

In this section I have discussed how online transactions seem to be conducted between people online, with new technology as their medium, and that trust is a foundational part of the transactions. In the next section I briefly account for some reasons that might lead to trust in an online transaction.

2.6.1 Why do we trust applications?

As the celebrities who got their private pictures spread online experienced, even though Apple could be trusted with their private information, there were other people, such as hackers, that could not (Remling, 2014). This example is merely one of many that could witness to the distrustfulness of providers and other online participants. Therefore it seems legitimate to ask why? Why do people trust providers of applications or cloud services with their information? Trust on its own is a complex concept that is large enough to write countless books on its own. However, it is of value to this thesis to review some of the reasons why some find providers or other participants online trustworthy. Clark asks the same question, and accounts for some reasons as to why a participant in an online transaction might be regarded as trustworthy. The first is that the other participant in the transaction might know the provider. They might have had other transactions with that same provider and have experienced that they are trustworthy. The latter reason is often referred to a "positive feedback mechanism". This mechanism explains how when one participant makes a transaction with another and receives the expected outcome, it is likely that his trust in the other participant grows. The likeliness of he occurrence of a repeated transaction will increase, which in turn would cause a positive feedback mechanism, or a loop (Wikipedia, 2014). I will discuss this in the context of trust in the welfare society in a later chapter. Another reason for a participant to trust another in an online transaction is that they suspect that the provider would fear loss of reputation if they were to violate that trust or laws and regulations may restrict the provider (e.g. the reasoning why many chose a known provider at a higher cost, than a less known for less money) (Clark, 2014, p. 18).

In this section I have briefly described two reasons as to why a participant in an online transaction might trust another. In the following section I discuss the possible need for distrust in online transactions.

2.6.2 Positive aspects of distrust?

Trust could be argued to be a word with positive connotations. As Clark would put it, a society run on trust is a society of freedom. When people can be trusted it is argued that the need for strict rules, regulations and enforcements decrease (2014, p. 18). To most people in the world, this type of society would sound like a utopia. Most people in the world would probably not say that people in general could be trusted. A person that is unconditionally trusting towards people could be argued to put himself in harms way, in accordance with Baier's definition of trust:

> When I trust another, I depend on her good will toward me […] Where one depends on another's good will, one is necessarily vulnerable to the limits of that good will. One leaves others an opportunity to harm one when one trusts, and also shows one's confidence that they will not take it. Reasonable trust will require good grounds for such confidence in another's good will, or at least absence of good grounds for expecting their ill will or indifference. Trust, on this first approximation, is accepted vulnerability to another's possible or expected ill will (or lack of good will) toward one (as cited in Lagerspetz, 2014, p. 123).

The overarching argument in the general debate on information privacy seems to be that people cannot be trusted, and that the flow and spread of information online has to be regulated, to keep people safe from harm. Central definitions in the information privacy discourse relate to "control" and "limiting access to private information" which could be argued to suggest that unlimited trust is not beneficial in all circumstances.

A journalist in the Norwegian newspaper *Dagens Næringsliv* recently wrote, "If you're not paranoid, you have too little information" (Eckblad, 2014). The journalist had recently discovered the amounts of information one of the large media companies in Norway had about him, and seemed to suggest that if people would know how much information companies of the same sort have about them, their supposed trust would vanish.

In this section I have pointed to some possible threats of general trust in the online sphere, and how the information privacy debate seems to encourage less trust and more protection in general. In the next section I discuss trust and the welfare state.

2.6.3 Trust and the Welfare State

The privacy debate in itself offers enough material to cover this research project and many more. However, to understand the reasoning behind the privacy paradox it has been of interest to look at the role of trust. Therefore, I have in the previous section discussed trust in the online sphere. Furthermore, the aim of this research project has been to explore the Norwegian respondents' relationship to information privacy. Norway is a welfare society and trust seems to be a vital part of this type of society (Jensen and Svendsen, 2009).

According to the Oxford Dictionary of English, a welfare state is: "a system whereby the state undertakes to protect the health and well-being of its citizens, especially those in financial or social need, by means of grants, pensions, and other benefits." (Stevenson, n.d.) Mjoset writes about the goals of the welfare state being: "Full employment, an egalitarian income distribution, and general social citizenship through universal pension schemes and provision of social services" (1992, p. 652). Based on these two quotes, it seems as though a welfare state is concerned with its inhabitants having equal opportunities and obligations. In the OECD-report on trust, the authors found that higher equality in income in a country seemed to affect the level of trust. In countries with less hierarchy and distance between the "classes", the trust levels were higher. Seeing that Norway is in the top range of countries with income equality (OECD, 2011, p. 91) it is reasonable to assume that the inhabitants are inheritably trusting towards others. According to Jensen and Svendsen "[s]ocial trust [is] the belief that most people can be trusted" (2009, p. 3). They go on to claim that "a high level of GT [generalised social trust] i.e. trust in individuals outside the family and friendship sphere, is a precondition for universal welfare institutions" (2009, p. 3)

In Jensen and Svendsen's article, they write about how trust is fundamental in the Scandinavian welfare states. This is exemplified by how the inhabitants of these state accept high taxes. The authors call it "giving money to strangers". Their main question is how can the taxpayers know that their money is being used for the good of the welfare state? On the basis of generalised social trust. Furthermore, Jensen and Svendsen points out the effects of positive feedback, when people in general experience that their trust is not misplaced (2009, p. 3)

In the previous chapters I have given an account for a part of the general research on privacy. Additionally I have discussed trust and the welfare state in relationship to privacy. The aim of this research project has not been to merely conduct yet another study on people's opinion on information privacy in general. However, it has been of interest to explore if the lack of correlation between statements of concern and behaviour may be explained in terms of the privacy paradox. Additionally, it has been of interest to explore if the privacy paradox can be found in Norway and if it is linked to general trust. Therefore, in the following section, I provide an overview of some of the research conducted on the privacy paradox and so-called "actual disclosure".

2.7 Previous research

It is evident that information privacy is a much-researched field of study, and as the development of new technology continues, the aspect of information privacy also seems to be of interest to many researchers. When studying people's attitudes towards information privacy, it seems as though the default focus of measuring attitudes have been to measure people's concern for information privacy (Smith et.al., 2011, p. 998) The degree of concern about information privacy, and the factors affecting this concern have been researched to great lengths and have provided several findings. For instance, one project found that women were more concerned about privacy than men (Smith et.al., 2011, p. 999). Another study found that the degree of concern for privacy were likely to be higher amongst "young, poor, less educated, African-Americans" (Smith et.al., 2011, p. 999). Furthermore, research has found that the concern about privacy is connected to the opinion of information privacy, which varies based on several factors, such as context, belonging a certain group, age and many other aspects (Norberg et.al., 2007, p. 102).

It seems apparent from previous research that many have studied the level of concern, reasons for concerns and factors connected to this. However, Norberg et.al. points out that there seems to be little research on the actual measures taken to protect information (2007, p. 103). In the following section I discuss so-called "actual disclosure" and case studies conducted in the attempt to explore measures taken to protect information.

2.7.1 Actual disclosure

In this case study on information privacy, the ultimate goal has been to explore if what the respondents of the interviews say correlates with what they do, and if the lack of correlation may be connected to levels of trust. The privacy paradox suggests that there is a general lack in correlation. However, the aim of this particular thesis has aimed at studying a part of the Norwegian population to explore if it applies to them. Ever since the privacy paradox became a puzzle, it has been of interest for researchers to explore the factors that motivate people to act upon their concern for their information privacy. This action is what Norberg et.al. call "actual disclosure" (2007, p.) Studies of what motivates action in protecting information privacy have led to research on the relationship between the privacy paradox and trust. However, Norberg et.al. noted in 2007, that the amount of research done on actual disclosure and privacy was lacking (p. 103). The exception Norberg et.al., found was that Sayre and Horne had conducted research that found that "consumers would freely trade personal information in exchange for small discounts at a grocery store" (2007, p. 103). Even though it is seven years since Norberg et.al. published their studies, it seems as though there are still few case studies, exploring actual disclosure and information privacy today. As I will discuss in the method chapter, it is arguable that when studying a phenomenon, asking "why" and "how, it is of value to explore a smaller portion of a population. Therefore, I have in this research project studied a part of the Norwegian population. When studying the variable of trust in the privacy paradox, I have also studied a part of the German population. In the following section I discuss some of the previous research on information privacy in the Norwegian population, and possible justification for further research.

2.7.2 Norway

It would seem as though Norway is one of the countries where new technology is apparently being adopted at a high speed, and the public seem open to new solutions. According to Flam, Norway is in the very top when it comes to adaptation of new technology such as "smartphones, tablets and internet protocol television" (2013). However, as argued in the introduction, the technology that is being adopted often collects information in databases out of reach of the protection of Norwegian laws (Datatilsynet and Teknologirådet, 2014). In Norway, the Norwegian government aims at protecting its inhabitant's privacy by several means. The Norwegian Data Protection Authority (NDPA) is an institution that "shall facilitate protection of individuals from violation of their right to privacy through processing

of their personal data" (Datatilsynet, n.d.). The NDPA cooperates with the Norwegian Board of Technology (NBT). NBT is "an independent body for technology assessment established by the Norwegian Government" by the purpose of exploring "societal impacts and options of technology and science; stimulates public debate on technology; and advises the Norwegian Parliament (Stortinget) and other governmental bodies on technological issues" (Tenøe, 2013).

The recent years, these two bodies cooperate to explore the current situation and future trends on information privacy in the Norwegian population. The recent report on information privacy from NBT and NDPA (Datatilsynet og Teknologirådet, 2014), uncovered that there had been a rise in concern for information privacy amongst the Norwegian public in general, during the last years. Some of this concern might be traced back to the fact that 94 per cent of the respondents in the study had heard about the Snowden-leaks (Datatilsynet and Teknologirådet, 2014, p. 20) However, the report also pointed out that the Norwegian people did not seem to want to act upon their concerns, the actual disclosure of information online was higher than expected. Many stated that in a hypothetical situation were they knew that they were under surveillance; they would not change their online habits (Datatilsynet and Teknologirådet, 2014, p. 33) The authors of the report could be argued to have couched this finding by saying that it could seem as though the Norwegian people are not able to relate to the issues at hand and thus producing no action. It is clear that surveys like these are of great value in order to map out attitudes in the population. However, as Scrhøder et.al. argue, a quantitative method alone cannot portray the whole picture (2003). When the NBT and NDPA finds that the Norwegian people are concerned about the issue of information privacy, but cannot fully relate to the issue, it is of value to ask why. The value of this research project lays in the continuing research on the topic of information privacy in Norway, and that it aims at aquiering a more in-depth understanding of why the Norwegians are concerned about information privacy, but cannot fully relate to the issue.

In this section I have reviewed a part of the previous literature on information privacy in the Norwegian population and provided justification for why this research project is of value. It is my argument that to understand more of information privacy, actual disclosure and the privacy paradox, more qualitative in-depth research is of value. In the following section I discuss the methodological approach of this research project, and why it is of value. I begin by discussing quantitative methods versus qualitative methods.

3 Methodologies

3.1 Qualitative vs. Quantitative

When making an attempt to understand a population, quantitative methods, including questionnaires, seem to have proven to be of great value. They are generalizable, hence creating a greater overview of the opinions of the population. Moreover, these types of methods are able to quantify the opinions of the population, which may indicate in which direction a population leans. As described in the previous section, the NBT & NDPA published a report of such a questionnaire conducted in Norway earlier this year (2014). The report aimed at mapping out the people's attitudes towards information privacy. The study found that a large portion of the population was concerned about information privacy. However, it also noticed that the actions that should follow that concern is lacking.

The debate of the effectiveness of qualitative versus quantitative research is a long-standing, well-known and on-going debate amongst researchers. Bernard and Ryan acknowledge this debate, and points out how different types of methods are valuable in different types of research (2014). In any kind of research, a mass of data in all shapes and forms are gathered, and to make sense of those data, a method of research is of essence. According to Bernard and Ryan, quantitative data is formed, when data is recorded as numbers, frequency, volume and so on, and qualitative data describes the process in which data focus on words, pictures and so on (2014, p. 5).

> In the social sciences, we are interested in people's behaviour, thoughts, emotions […] When we reduce our experience of those things to numbers, the result is quantitative data. And when we reduce people's thoughts, behaviours, emotions […] the result is qualitative data. (Bernard and Ryan, 2014, p. 5)

Using NBT and NDPA as an example, they have reduced people's experience of information privacy into numbers and have made an overview of how many people that for instance are concerned about information privacy (Datatilsynet and Teknologirådet, 2014). The NBT and NDPA report joins an array of studies done on people's concern for information privacy (Smith et.al.,). However, as researchers have found, it is common for people to have an opinion or concern without acting upon those and many have attempted to research and

explain why there is a lack in correlation and how it may be remedied (Norberg et.al., 2007). However, even though generalization has been impossible, the few qualitative studies on information privacy and actual behaviour seem to have proven fruitful (e.g. the project described in the literature chapter, where researchers found that consumers were willing to trade personal information for small discounts at a grocery store (Norberg et.al, 2007, p. 103)). Therefore it would be reasonable to assume that regardless of the complexity of the topic, it is of value to conduct qualitative case studies on information privacy, even if they only were to uncover a fraction of the picture. In the following section I discuss surveys versus qualitative case studies, and further argue for the value of the chosen method, which I will discuss in the chapter thereafter.

3.2 Other surveys

Baek is of the opinion that

> [a]lthough large scale opinion polling is often considered the most scientific estimate of what people are thinking and what they want on a particular issue, public opinion researchers suggest that such polls provide a picture of public opinion that is superficial (2014, p. 34).

The average individual might find it easier to answer yes to a question in a survey than to a person sitting in front of you. Furthermore, the person in front will be equipped with the ability to ask follow-up question, possibly making the answer more correct. It seems as though there have been conducted a great deal of surveys, and less qualitative research within the Norwegian population. In surveys, Baek points out, it is easy to answer "yes" or "no" to a simple question on a screen, without giving it much thought (2014). I am not discrediting surveys. However, as I will discuss in the method chapter, I believe that by talking to a smaller group of people, and adding that information to the already existing information collected through surveys, there might be additional interesting findings in the current state of information privacy in people's minds. According to Schrøder et. al. (2003) all that any form of method, quantitative or qualitative, can ever do is present a piece of the puzzle. No one method can tell the whole truth. It is of value to continue to study the topic of information privacy. One of the reasons that van der Hilst points out is that if consumers in general are unaware of how data is collected and used, they could be at higher risks of someone taking advantage of that ignorance (whether it be surveillance or identity theft) (2013).

This project was conceived by the want to understand why the Norwegian people could seem to be concern for the information privacy of their information, and not act upon that concern. "If you want to know how people understand their world and their lives, why not talk with them?" (Kvale & Brinkmann, 2009, p. xvii). It seems as though regardless of the method chosen, a sacrifice of either scale or depth has to be made choosing either one of the two umbrella terms of methodologies for this project. Even though two interviews with all together 12 people could not be representative for the whole population, it uncovered valuable information that would not be discovered in a survey.

In the following section I discuss case studies and thereafter, qualitative group interviews.

3.3 Case Study

According to Kvale and Brinkmann, methodologies should be found as a result of asking the question "what do I want to know" (2009). Furthermore, "the purpose of the qualitative research interview […] is to understand the themes of the lived daily world from the subjects' own perspectives." (Kvale and Brinkmann, 2009, p. 24). With the aim of acquiring more in depth on the reasoning behind people's actions regarding information privacy, it was necessary to conduct conversations with a smaller group of respondents. Yin states that a case study research method "is used in many situations, to contribute to knowledge of individual, group, organizational […] and related phenomena" (Yin, 2014, p. 4). With the aim of researching the everyday behaviour of a small group of people, a case study, including two group research interviews seemed like a fair approach.

This project is not the first to research the phenomenon of the privacy paradox, nor the first to research Norwegians relationship to information privacy. However, in a field as large as information privacy a case study researching a more narrow case might contribute to more knowledge about the field. Many have studied the larger picture of information privacy; in this project I have studied a smaller portion of information privacy, the context being students in Norway, using mobile phones and applications. As discussed in the introduction, I also conducted an interview with a group of German students. This was to form the basis for an argument on whether Norwegian's level of GT (general trust) (OECD, 2011) could be argued to impact the Norwegian respondents relationship to trust. As discussed in the literature

chapter, it would seem as though people that trust the provider of an application seem to be more willing to provide personal information to make use of the applications (Norberg et.al., 2007). To study whether the trust and information privacy might be linked in the Norwegian group of respondents, the idea was to find a group of respondents that would be from a somewhat similar society, however, with a substantial lower level of trust. After speaking to a few German friends, it became evident that this population, which scored much lower on the OECD scale of trust, might prove useful in this discussion (2011, p. 90).

Finally, as discussed in the chapter about stimulus materials, the application ValYou was added to this case study to assist the respondents in the focus of the interview. By introducing a new application, ValYou, which is as previously explained a cashless and card less banking application, I wanted to trigger some thoughts on information privacy that have not been triggered with the application the respondents are familiar with. The application in itself is tested and secured by the providers. However, it presents a new function and thus possibly a new thoughts on the topic of information privacy.

In this section I have accounted for the characteristics of case study research, and the components of this particular case study. In the following section I account for the rationale of choosing a qualitative group interview, what it is, and how they were conducted in this project.

3.4 Qualitative Group Interviews

Eli Skogerbø is a professor of the Department of Media and Communication at the University of Oslo, have experience with research, and teach method at the University. According to Skogerbø, the topic of information privacy may be researched in both a qualitative and quantitative manner. As previously discussed, research conducted with different methods is of value. However, as I wanted to present an actual application as a part of the project (ValYou), and this particular application was new and unfamiliar, a more in depth interview was expected to provide interesting results. Focus group interviews are often utilized in marketing before a new product is to be released into the market, to test initial reactions and opinions (Barbour, 2014). Furthermore, Skogerbø was of the opinion that the Norwegian people in general had developed impatience with forms, and that a quantitative survey might cause negative results (personal communication).

Seeing that the tendency seemed to be that people in general did not have much knowledge about information privacy, in addition to impatience with forms, group interviews could prove to be a more effective method for this project. When the expected answers might not be satisfactory, due to lack of knowledge it was important to capture non-verbal cues, and to have the ability to rephrase or clarify on both ends during the interview, to ascertain quality data. Furthermore, it was important to be able to detect reactions when discussing information privacy, and when presenting the visual stimuli (ValYou).

In the following section I discuss the characteristics of a group interview versus a focus group interview.

3.4.1 Focus Group Interviews vs. Group Interviews

Judging from the literature on focus group interviews and group interviews, there seem to be differing opinions on the difference between the two. Even though most literature focus on focus group interviews, and there are many similarities between the two, there are also differences and a reason to why I chose a group interview. According to Cohen et.al., both types of interviews are so-called collective interviews. As the names reveal, the interview does not focus on an individual, but a group of people. The difference between the two interviews becomes visible in both the role of the researcher and the focus of the analysis (2011, p. 432).

A focus group studies the interaction between the respondents. In this setting, the researcher works as a moderator who initiates conversation, whilst the respondents, to a greater extent, lead the conversation. The relevant data is retracted from the interaction between the respondents. On the other hand, the relevant data in the group interview is derived from the respondents' answers to the researcher's questions. Never the less, the researcher has to pay attention to the interaction between the respondents in the latter interview as well. The focus is less on the interactions between the respondents in terms of content, and more on assuring that possible dominant or non-dominant respondents does not affect the answers negatively (Coen et.al., 2011, p. 436).

When asking a specific question, as was the case in this research project, the thoughts and opinions of the respondents seemed to be of most importance. I.e. RQ1;

Does protection of information privacy affect users in their everyday use of new technology? E.g. does the lack of a privacy policy in an application affect their decision to download it?

This question was asked in a manner that sought a concrete answer to how this possible effect of privacy policies is visible in the respondent's everyday life. The desired data for analysis was answers to questions from several respondents. This kind of data could also be acquired through individual research interviews. However, according to Cohen et.al "a group interview […] can generate a wider range of responses than in individual interviews" (2011, p. 432). Seeing that the general knowledge about information privacy was expected to be low in this at least the Norwegian group of respondents, the idea was that by having several respondents in a group, the chance that some of the respondents would know more was higher. Furthermore, the hope by conducting a group interview was also that by listening to the conversation of the others, the respondents that for some reason did know less about information privacy would be inspired to comment and add some of their opinions during the interviews. This particular expectation was met in both interviews, which will be discussed in a later chapter. In the following section I account for the interview guide that was created for the interviews.

3.4.2 Interview Guide

As previously discussed, the group interview was chosen as a method specifically because of the interest of the respondents answers to questions, not because of their interaction between each other. However, the actual answers were not the only interesting data to be found in the interviews. Considering that the research leading up to the interview gave an impression of little general knowledge about information privacy in the population, it was important to create an interview guide that would aid the respondent's reflections on the topic. However, it was also of importance to see where the conversation would lead once it had started, so I made use of a semi-structured interview guide, to make sure the conversation would flow, with less help from the questions. Kvale and Brinkmann recommend a type of semi-structured interview guide, when the aim is to study the perspective of the respondents (2009, p. 47)

After a short while of small talk and warming up, both interviews started off with the same question “what do you consider as private information” and the discussion went on for a while there in both interviews. According to Kvale and Brinkmann it is of importance that the questions are short and simple, aiding the respondent in answering (2009, p. 134). Therefore, in creating the interview guide I tried to create questions that would be easy to answer regardless of the level of knowledge (Kvale and Brinkmann, 2009, p. 141). After the first question, the interviews went in different directions, and the interview guide got more fluid. Nevertheless, as Barbour predicted, when one of the groups kept venturing off topic, it was of much help to have a guide, ticking off topics as the interview proceeded (2014). The conventional school of research interviews argues that in order to protect the validity and reliability of the research interview, it is important to keep the interview questions in check, This is to assure that there are no leading questions, or the likes, that may sway the respondents. However, in an interview covering a topic as complex as information privacy, it was of necessity to employ creativity in the conversation to aid the reflection process. Some leading questions were consciously made use of to test if they would cause a reaction and proved to of great value of the project. In one of the questions I asked if the fact that the stimulus material (ValYou) was created by a large Norwegian corporation, would change their decision to use or not use the application. This was clearly of a question of a “leading” nature. However, it was of importance to see if trust was a factor in making use of an application or not. Barbour argues that the balance in leading and non-leading questions is essential to a good interview, but that there is room for those kinds of questions (2014, p. 117). Furthermore, she also argues that the interviewees might not be as easy to sway, even with leading questions (2014, p. 117). The latter notion is arguably visible throughout both interviews, the respondents was not necessarily led, even with leading questions (Appendix 2 and 3).

Considering that the interviews were of a semi-structured nature, some topics were only covered in one of the groups. During the coding and analysis of the data material, it became evident that some of the topics discussed in one group were of value to ask the other group about too. Therefore I asked a few follow-up questions to both groups of respondents via Facebook (Appendix 5).

Questions about the application ValYou was also presented in addition to the demonstration of an application. This is what Barbour describes as stimulus materials and will be discussed in the next chapter (2014).

3.4.3 Stimulus materials

Seeing that information privacy could be viewed as a part of their basic human values to some, it could prove to have many potential tracks, from which it could derail. With a topic that could easily be derailed, a way of stimulating or focusing discussion may be of help (Barbour, 2014, p. 142). One type of stimulus is presenting an actual product, which I did by presenting "ValYou" in the interview. After a general discussion about information privacy, I ended the interview by presenting a smart phone with the application and demonstrating how it worked, to see if there was a reaction with regards to privacy of information. As discussed in the section on case studies, the application was used as a stimulus to help the respondents come at the topic from a less familiar angle.

ValYou is an application making use of a technology named "Near Field Technology" (NFC) that enables two devices to transfer information between each other through a light touch (Figure 1).

Figure 1: The function of ValYou (Source: Zachariassen, 2013)

ValYou is not the only application making use of this type of technology. However, it is the first in the Norwegian market to make use of it in mobile payments, or the so-called "mobile

wallet" (Mobeyforums, 2011). In Norway, this type of mobile payments has not been in use until autumn 2014 (Mobile Payments, 2014). However, judging from the media it is expected to become an important application (Amundsen, 2014). As mentioned in the introduction, ValYou is an application that is relying on it being standardized, that people in general will make use of it, or else the stores and banks will not be interested and the application may be argued to be a flop. Even though the application has been tested and the producers have it on good merit that it is secure, the consumers may be concerned merely because of lack of knowledge and experience with this kind of technology.

When discussing information privacy it might be easy to answer theoretically, or thinking in possible scenarios. However, by presenting an actual product, the aim was to start a reflection process.

In the next section I account for how I recruited the 12 respondents in the two group interviews.

3.4.4 Sampling

The German group was recruited through the message board of a Facebook-group for international exchange students in Oslo, through the Erasmus programme. A simple message was posted, explaining the nature of the interview. A reward of free dinner was offered to the participants of the interview. Many students volunteered for the project. However, seeing that I was interested in both male and female participants and most of the interested was female, I also recruited one respondent through a friend. In the German group, there were four females and two males present, four of them were students at the University of Oslo (UiO), and two of them at the Norwegian Business School (BI).

The Norwegian group was also recruited through Facebook, but with a slightly different approach. After several failed attempts at recruiting respondents through messages in Facebook groups, such as the group for Political Sciences at the UiO, the group for Pedagogy at Oslo University College (OUC), and through many friends, I had to rethink my method. I reached the final successful attempt by searching for Norwegian students on Facebook and addressing them directly. After many messages, a number of people responded positively. Furthermore, a colleague recruited some fellow students at UiO. In the Norwegian group

three girls and two boys attended the interview. Four of the respondents were students at the UiO, one was from OUC, and one was from BI.

The interviews was held at the University of Oslo on September 10 and 22, 2014, and lasted for 80 and 75 minutes. The interview guide was of a semi-structured nature, hence the two sessions varied some in discussion topics, seeing that I was interested in where the discussion would lead. Most of the respondents was recruited through Facebook, a few was recruited through friends.

In the following section I account for how I have coded the data material from the interviews and justify some of the choses made in the analysis process.

3.3.4 Codebook

According to Kvale and Brinkmann; "[c]oding involves attaching one or more keywords to a text segment in order to permit later identification of a statement […]" (2009, p. 202). Coding is also used in order to quantify the frequency of statements in a text, which is often used in "content analysis". During the transcription and the read through of the interviews in this project, codes were attached to segments of text. This is what Kvale and Brinkman calls "data-driven coding" (2009, p. 202). Seeing that I wanted to explore attitudes and behaviours of a case, there were only a few concepts that might have been determined before the data was collected. "Concept-driven coding", which entails formulating specific concepts before the interviews were transcribed, could have made the process after transcription less demanding. However, it would not have been sufficient for this project, because I had no clear idea of what I was looking for on the outset.

The codes for this project are made based on a combination of different topics mentioned in information privacy literature, such as "control" or "the right to oneself", and the research questions. Considering that it was of interest to have a discussion, a semi-structured interview guide was used. Not all questions were answered, and the groups did not receive all the same questions. Therefore, the codebook is a result of studying and analysing the topics in discussion, both introduced by myself as the researcher, but also introduced by the respondents as the discussion moves along.

As is apparent the coding of this project is both a form of what Kvale and Brinkmann call "meaning condensation", taking long segments of text and attaching a few words to them based on what is stated in that text. Furthermore, the codes are also based on "meaning interpretation". In meaning interpretation "the interpreter goes beyond what is directly said to work out structures and relations of meanings not immediately apparent in the text." (2009, p. 207). An example of meaning condensation is the code "privatlivet" which puts the topic of some of the statements where the respondents discuss the issue of having information privacy, by the simple reason of wanting to be let alone. On the other hand, some of the codes and categories are also based on non-verbal communication and clues picked up during the interview. This may be exemplified on how I compared the two groups of respondents level of knowledge and concern about information privacy on a combination of what they said, and what they did not say. As I elaborate on in the discussion chapter, the fact that the Norwegian respondents talk minimally about surveillance and large-scale issues of information privacy, whilst the German respondents quickly arrive at that point in their discussion, underlines an essential point of the thesis. The fragility in this codebook lies in the fact that I, as the researcher have done all the work, from the transcription to the coding and interpretation of findings. The latter example of attaching codes to non-verbal communication that I myself have interpreted as meaningful might be entirely wrong. However, seeing that information privacy seems to be an issue that is highly current, whilst the general population seem to know little about the topic, I would argue that it allows for a wider analysis of the data at hand. In this study, it is of interest to explore the possible rationales of the issue. The fragility of being the only researcher analysing the data could to some extent be remedied if I would recruit another person to analyse the data. If the second person would arrive at similar conclusions as myself, it might ensure intercoder reliability (Mouter and Nordergraaf, 2012). Even though I did not have the time and resources for recruiting another person in this project, it would be of value in a possible further research of the topics in this project.

I have in this section accounted for the coding of the data material from the interviews. In the following section I justify the research project by looking at its reliability and validity.

3.5 Finding truth

The main rationale for all research may be argued to be to discover the truth. In all discussions on methodologies the ultimate question could be: does this method discover the

truth? One of the major questions in the discussion between the quantitative and qualitative camps has been regarding how we make sure our findings are true, sound and reasonable. The degree of truth in a research project is often discussed in the terms of validity, reliability and generalizability. Especially qualitative research has been in the crossfire in this aspect, considering that there is an argument that claims it is more difficult to find valid, reliable or generalizable results from qualitative research, because of its exposure to human error (Kvale and Brinkmann, 2009). However, Schrøder et. al. argues that all research methods may bring an addition to a large picture, and that no single method are superior to another in that sense (2003). The two terms could be argued to complement each other and that has been the aim of this project as well, a qualitative method that compliments the previously conducted studies making use of quantitative methods.

3.5.1 Generalizability

In its most frequently applied form, generalizability is not discussed in connection to qualitative methods, mostly due to the sampling process. This type of generalization is often referred to as statistical generalization (Yin, 2014, p. 40). There are certain criteria that have to be met if research is to be generalizable to a population. One is the amount of respondents in the sample and the other is the way in which the respondents are requited. To represent a national population, a sample of 1000 people is necessary (Cohen et.al., 2009). Furthermore, to recruit that sample a type of random selection has to be employed. It is thus evident that per this definition, findings from qualitative studies, which are known to be smaller in sampling a non-random, it cannot be generalizable to a whole population. In the qualitative interviews the intention is to find a non-random sample, in the group interviews preferably a homogeneous group, compared to another homogeneous group (Kvale and Brinkmann, 2009). This has also been the intention for the group interviews in this project, and thus they are not generalizable in this sense. However, as Yin argues, there is a second form of generalizability that is more frequently used in qualitative case studies, called analytical generalizability. This type does not attempt to generalize across a large population, rather it looks for "lessons learned", to possibly adapt into a new study (Yin, 2014, p. 40-41). These lessons learned, may transfer to be analytical generalizations, which might "form a working hypothesis, either to be applied in reinterpreting the results of existing studies of other concrete situations (that is, other cases or experiments) […]" (Yin, 2014, p. 40-41). As I comment on in the summary chapter of this thesis, it could be argued that some of the

findings could form an analytical generalization, which again could form working hypothesis for another study (e.g. the possible connection between foundational values of the Norwegian society and their view of information privacy).

3.5.2 Reliability

When discussing reliability, the procedure of collecting and analysing the data material is in question. It asks whether the data is trustworthy, and the analysis finds reasonable conclusions (Gentikow, 2005, p. 57) To ensure that the findings of the interviews were reliable, I made use of two different tape recorders whilst conducting the interviews. In case of poor quality on one of the recorders, I made use of two differing types. By testing the sound from various positions in the room, I also made sure that the recorders would pick up all respondents. The recorders picked up everything the respondents said. The respondents were anonymous, and seemed to be answering in a truthful and open manner. One example was how the respondents in both groups admitted to stream content illegally online, which could attest to that they were not holding back because of the recorders. Furthermore, seeing that it was a group interview, there would have been a risk of a lack in data by some of the respondents being shy or some other being too dominant for others to talk. In both group interviews almost all of the respondents answered frequently and in a seemingly open manner, with the exception of one respondent in the German group and two respondents in the Norwegian group. In both groups there were also at least one dominant respondent, more often raising their voice and opposing the other's opinion. This was not as evident in the German group as it was in the Norwegian group, were one of the respondents often interrupted or commented critically on the other respondent's statements. However, most of both the groups answered and kept the discussion going regardless of the dominant participants.

To make the data found in the analysis reliable I transcribed both interviews as it was spoken. To ensure non-verbal cues I included symbols to explain pauses, body movements and interruptions. When I have cited a respondent directly in the analysis I have altered the text to make it understandable for a reader that was not present in the interview. However, when making alterations I have made sure not to alter any more than absolutely necessary to make sure the meaning of the data was not altered. Furthermore, when the respondents referred to a topic that might not be familiar to the reader I included an explanation in

brackets (i.e. when the German respondents refer to “Ruter” I have put it like this: Ruter [an application for public transport in Oslo]).

It is evident that if another researcher were presented with the same results as I have found in the data material I have collected in the group interviews, she will not necessarily arrive at the same results. However, I have attempted not to draw conclusions based on single statements, I have rather looked for patterns and attempted to put those into context from literature, previous research and so on. Finally, even though the interviews were semi-structured, they were transcribed in full and the respondents were anonymous. Therefore it would be possible for other researchers with special consent from the respondents to view the follow-up questions and direction of the two interviews. This could ensure the ability for another researcher to replicated the interview to some extent, thus increasing the reliability of the findings (NESH, 2006).

3.5.3 Validity

Questioning validity is questioning whether a study has accurately captured that which it intended to investigate, how “true” the findings are according to the starting point (Gentikow, 2005). The projects method and analysis was conducted on the basis of the research questions, which aimed at discovering if the Norwegian respondents’ everyday use of new technology was affected by protection of information privacy and if that could be connected to trust. Knowing the complexity of information privacy, questions such as “what is private information to you” was asked to ease the respondent into the topic. The following questions asked what kind of applications they used and if they had rejected an application in fear of what the providers would do with their information. These were some of the ways of uncovering if there would signs of actual behaviour. These questions and their answers constitutes to what I find a high degree of validity seeing that they help answering the research question. Furthermore, as will be discussed in a later chapter, the questions employed were of a more indirect manner in the way that they do not firstly ask if the respondent protect his or her information privacy, but more what information privacy is to them. In this way, it could be argued that the respondents have given more genuine answers, which was the aim the project. However, seeing that there was fewer questions asking directly if the respondent protected their information, the answers to the research question have been answered by my analysis to a higher degree than if the answer were given

"directly" by a number of respondents. Seeing that other researchers might arrive at other conclusions with the same data material, the latter notion might be argued to decrease the validity of the project. However, I am of the opinion that without the indirect questions, the respondents would not have provided the answers as they did. Those answers then again provided useful findings that could be of interest in further research.

I have in the previous section attempted to justify the findings of this research project. In the following section I operationalize the central terms used.

3.6 Operationalization of Terms in Use

In this thesis I have posed the following research questions:

RQ1

Does protection of information privacy affect people in their everyday use of new technology? E.g. will the uncertainty of what an application will do with personal information about an individual, hinder that individual in making use of it?

RQ2

Is there any reason to believe that the privacy paradox is a reality in Norway and can it be traced back to the high levels of trust amongst the population?

In this chapter I operationalize the variables of those research questions. In the sections thereafter I provide an explanation of other central factors of this thesis, such as "smart phones".

3.6.1 Information privacy

Even though I have discussed information privacy in the literature chapter, I want to clarify that information privacy is the type of privacy that is discussed throughout this thesis.

3.6.2 Smart Phones

In the interviews I asked the respondents whether or not they had "smart phones". In this report, a smart phone is a phone with the ability to download applications through a mobile network. I decided to limit the case of everyday information privacy to the use through smart

phones and applications due to the limitations of a master project and the fact that ValYou, is an application created for smart phones. Årnes & Nes define a smart phone in the following:

> Smart phones are mobile phones that offer more advanced data processing and better connections than conventional mobile phones. In fact, smart phones are small handheld computers, on which small programs, or applications – popularly known as apps – can be installed. (2011, p. 7)

A smart phone brings a whole array of new information privacy issues to the table. Baase puts it colourfully, but truthfully in this way "a Masai warrior with a smartphone and Google has access to more information than the President did 15 years ago" (2013, p. 25) and "as a side effect of cellphone use and the sophistication of smartphones, researchers are learning an enourmous amount about our behaviour." (Baase, 2013, p. 26).

3.6.3 Applications ("apps")

In this project, the reference to "applications" or "apps" means all programmes installed on a smart phone from an external provider – or the use of existing application. An example of an external provider is the SNS Facebook. An existing application means one of the applications on the phone's desktop by default and an example of an iPhone existing application would be the Internet browser "Safari". According to Årnes and Nes,

> Apps are available via the different platforms' app stores, the top two being Apple's App Store and Google's Android Market. The number of apps available from these stores are growing enormously: Apple has approved 500.000 apps for sale at its App Store, while around 300.000 apps are available on the Android Market. Ten billion apps had been downloaded from App Store as of January 2011. (2011, p. 7)

3.6.4 Everyday life

In RQ1 I ask if people are affected by information privacy concerns in their everyday use of new technology. As discussed in the introduction it seems valid to claim that when asked about concern for privacy in connection to surveillance and Snowden-leaks many would state that they indeed are concerned. By asking about everyday use of new technology I mean in this project all activity conducted online on a frequent basis. Such as downloading and using applications.

3.6.5 Affect

When asking about "affect" in RQ1, the intention was to find if there were actions related to probable concerns for information privacy. When an individual is downloading or making use of an application in his everyday life, will he decide not to download and use the application if he is unsure of what the information the application receives about him is used for? Will uncertainty on how the information is managed and protected affect the individuals decision to download an application?

3.6.6 Trust

Trust is a broad term, and within new technology it has a wide spectrum of meanings and associations. Countless books have been written on the topic, and it would be possible to write this whole report on trust's role in information privacy. However, in this report trust is treated as a variable, attempting to explain the privacy paradox in Norway. According to Norberg, Horne and Horne the willingness for people to give out their information is higher with higher levels of trust (2007, p. 102).

The foundation of this variable is the OECD-report on trust claiming that Norway is in second place on the barometer of trust, whilst Germany is in 15th place (2011, p. 91). Trust is defined in the trust section of the literature chapter. Furthermore, as noted in the literature chapter (pp. 25-26), I refer to general social trust (GT) as described as a part of the welfare system by Jensen and Svendsen (2009), which is the general state that people are trustworthy.

3.3.5 "Norwegians" and "Germans"

When I speak of Norwegian and Germans as a people, attempting to explain a part of the study, I am not studying the whole culture of the two people groups. I recognize and fully admit that cultural identity, as well as personal identity, has a lot of affect on their answers. However, I chose not to discuss it in detail, for the sake of the projects length and resources. Furthermore, seeing that I wish to discover Norwegians relationship to information privacy in their everyday lives, I intentionally discuss the Norwegian culture and background more than I do the German. The data from the German group of respondents' functions more as a control group than a group I study in detail. In both countries I take into account the respondents relationship to their peers in the way of trust.

I have in the current section operationalized the central terms of this thesis. In the following chapter I reflect upon some of the limitations of this research project and thesis.

4 Limitations of the project

This research project has its limitations. In the previous section I discussed how the findings of the research could be argued to reliable and valid in addition to possible flaws. Gentikow is of the opinion that where a qualitative research project might lack in validity due to human bias, a transparent and reflected process make up for the loss (2005, p. 37). In this chapter I account for some of the possible limitations of the project and how it could be remedied. I start by reflecting upon the data collection in the following statement.

4.1 Group Interviews vs. Individual Interviews

We will never know what respondents might have revealed in the "privacy" of an in depth interview but we do know (through focus groups) what they are prepared to elaborate and defend in the company of their peers. (Barbour, 2014, p. 137)

When gathering a group of strangers and asking them to speak in front of each other, several factors that might play a role in the result. Factors such as their background, upbringing, personality, associations with venue, event, people, fears and so on may affect their response, or make them not respond at all. More specifically, the fear of being ridiculed by answering a question with an honest opinion might hinder a respondent from adding valuable data to the project. Furthermore, a dominant respondent may monopolize on the conversation and hinder others from answering, or interrupt. However, an uninspired respondent in an individual interview might be just as harmful to a research project. Barbour points out that regardless of the method, it is impossible to know what "could have been revealed" with another method (2014, p. 137).

4.2 Interview Guide

For an interview to be reliable it is of importance that another researcher may be able to conduct the same kind of research and arrive at similar conclusion as the original research (Kvale and Brinkmann, 2009, p. 245) To reproduce an interview without having attended the original, it is vital to be able to copy the original interview guide (Kvale and Brinkmann, 2009). Considering the interest in the respondents' attitudes and actual disclosure regarding information privacy, it was important to create an interview guide that avoided narrow questions in the beginning. It was vital to ask a question with a wider frame of interpretation,

to observe what the respondents would discuss with minimal stimulation. Hence, even though the interview guide was followed to a certain degree, the conversations went in different directions, and the two interviews produced different results. This is a possible limitation of the project, because when the questions are not posed in the same way in both groups, it is not possible to compare answers. However, as I discuss at length in the discussion chapter, much of the information may be found in what the respondents did not mention. The fact that the Norwegian respondents did not mention surveillance once during the interview, whilst the Germans mentioned it early on, might say more than their actual answers to some of the questions. Then again, when critical data for the findings stem from my analysis, my bias might produce results that other researchers might not find. I attempt to argue why the findings are nonetheless valid in the discussion chapter. Furthermore, as recommended by The National Committee for Research Ethics in the Social Sciences and the Humanities (NESH) I attempt to make clear what are my own interpretations and what the respondents actually said through out the following discussions (2006).

Seeing that the topics of discussion are varied in the two interviews, it is not possible to quantify the frequency of all statements. Even though it is taken into account the statements that is mentioned several times in both groups, the data is not analysed in frequency of statements, but on the meaning of the statements it has not been as important to clarify which person that said what, and in some instances "the group" is used as a loser term. This might be a weakness, due to the fact that it is more difficult to know if this is the whole groups opinion or not. In the instances where "the group" has been used, it talks about a discussion where all or most of the group have been significantly involved in "active listening", agreeing on what the speaker has been saying (it was especially visible in Interview 1, German group).

4.3 Recruitment

The recruitment and composition of the groups might also be a limitation of the project. Due to limitations in time and resources for this project, I decided to interview student groups in the Oslo area. Whilst recruiting German students living in Oslo proved to be quite uncomplicated once I found the right forum, the Norwegian group could not be recruited in the same manner. Hence, I had to recruit the group through various methods, e.g. through a colleague, and through addressing people directly on Facebook. By using "graph search" on Facebook it is possible to filter users that are students and live in Oslo. Therefore, it is a

possibility that the German respondents might have answered out of interest for the topic, whilst the Norwegians might have agreed to participate due to the fact that I approached them directly. However, all of the respondents were presented by the same initial information, and not all of the German respondents seemed to be very interested in the topic. Furthermore, one of the German respondents was also recruited through a colleague.

In this project there are several possible limitations, and the ones discussed in this chapter are merely a few. However as I attempt to argue in this chapter, the limitations are also possibilities for further understanding of the topic of information privacy in the Norwegian population. In the discussion chapter I try to argue the findings of this research project on the basis of previous research and theory as discussed in the literature chapter. In the following chapter I begin the account and analysis of the data retrieved from the interviews.

5 Findings and analysis

In the previous chapters I have discussed the methodologies, operationalization and limitations of this research project. Before I begin the account and analysis of the findings in the interviews I give a brief summary the background for the interviews and the research questions.

In the interviews for this project I conducted two group interviews with male and female students in the age between 20 and 30 years. The interviews were held at the University of Oslo, at September 10 and 22, 2014, and lasted for 80 and 75 minutes. One group consisted of German students and the other group consisted of Norwegian students. The reasoning behind the different nationalities of the students was to test whether it could be argued that Norwegian students are less interested in information privacy and that it could be argued that it is because they are more trusting to people in general, than the German students. Thus, as mentioned in the operationalization chapter, the German group functioned more as a control group to the Norwegian one. To focus the conversation in the interviews I made use of the application ValYou as a so-called stimulus material.

In the following chapter, I report and analyse the findings of the interviews conducted.
I attempt to answer the research questions posed in the beginning of this report:

RQ1

Does protection of information privacy affect users in their everyday use of new technology? E.g. does the lack of privacy policies in an application affect their decision to download it?

RQ2

Is there any reason to believe that the privacy paradox is a reality in Norway and can it be traced back to the high levels of trust amongst the population?

Furthermore, I will review the expected findings that was discussed in the introduction, and considering that the application ValYou has been used as a stimulus material in this project, I also aim at answering whether the respondents are concerned about information privacy when considering taking it in to use.

In the following sections I start by reporting the findings, and continue to analyse them.

5.1 Private information

As mentioned in the introduction and the method chapter of this report, there have been conducted several representative surveys claiming that people in general are concerned about information privacy. The last survey conducted in Norway arrived at similar conclusions; people are worried about the privacy of their information. However, when asking about information privacy, the NBT and NDPA seem to connect the questions to surveillance and cases such as the "Snowden-leaks". However, the reason why the NSA was able to conduct surveillance was according to them due to what has previously been termed self-surveillance. This term describes how people disclose information about themselves through various online channels (Clark, 2014, p. 18) Therefore, in these interviews, the aim was to study the respondents' attitudes towards information privacy in their everyday use, in the form as it is operationalized in chapter three. To achieve this goal it was vital to begin the interview with an open question that did not require knowledge: "what do you consider to be personal information?" (Appendix 1).

When asked about what information they consider personal, both groups had some reservation about giving out their full name, or real e-mail address. However, the German group were the one where most of the respondents consider their full name and address private information (Appendix 2, Interview 1, German group, p.1). Most of the respondents in both groups found medical journals to be the most private information that they would not want broadcast online. However, the Norwegian respondents discussed how they had heard that the Norwegian patient journals were to become e-journals and that it was a positive aspect. When one of the respondents retorted that "any doctor will be able to go and look it [the journal]", the other responded by saying "yes, doctors may see it, but that doesn't mean that others will see it" (Appendix 3, Interview 2, Norwegian group, p. 4).

The Norwegian respondents also found their personal identification number to be personal (Appendix 3, Interview 2, Norwegian group, p.1). In the German group, almost all the respondents had a second e-mail address that they used for matters of less importance, or when they did not want to receive unwanted e-mails, this e-mail would most often not contain their full name: "I have a second e-mail address, without my name in it, so if I don't

care about the website, I just put this in [when required to disclose personal information] and spam goes to this address. " (Interview 1, German students, p.2)

In the Norwegian group, only one of the respondents reported having a second e-mail address to avoid unwanted e-mails (Appendix 3, Interview 2, Norwegian group). Furthermore, the German students on the other hand said that they would make up false names if they were about to register for a website or anything similar that they were not very interested in. Half of the group of the Germans reported that they did not have their actual names on Facebook (Appendix 2, Interview 1, German group), whereas the Norwegian group all had their actual names on their profiles (Appendix 5).

I don't actually [have my real name displayed on Facebook], my last name, the last name I have on Facebook is actually my middle name, so it's like, I test if someone knows my real name, [if they don't] they'll not find me actually. (Appendix 2, Interview 1, German group, p. 5)

The German group also mentioned several times that their pictures, the ones they posted online were the ones that they were most afraid of losing control over or them being misused. Therefore, they would not let applications access their smartphones photo album, and so on.

Pictures as well, those I think is quite private. So if I have a Facebook […] like you have all the pictures there, and you only want your friends to see this, and then you like Google your own name, and all of a sudden, there's like pictures of you on Google, that's like, accessible to anyone, that might be… quite --- yeah, like if you have a picture where you're drunk or something and your employer sees it or whatnot, that's, um, very bad, I think (Appendix 2, Interview 1, German group, p. 5).

One of the Norwegian respondents did not mind having applications access her phones images, seeing that she would use several applications that needed access to her pictures. However, she would be more careful allowing an application access her phones microphone in fear of that being misused, whereas two of the other respondents agreed that they would not let applications access their microphones.

Yes, but then I accept [to let the application access the photo album on the phone], otherwise it's no point. But—not that I post that many pictures on Instagram, but, microphone I'm a bit more sceptical of. If they [the application] asks to access the microphone. With pictures I don't mind that much,

because I don't have that much interesting [on my phone], but with the microphone I say no, and then I'll delete that application. (Appendix 3, Interview 2, Norwegian group, translated, p. 22).

When I asked the respondents if they would consider IP addresses or the coordinates of their locations (made available online when making use of location services), most of them admitted to not knowing how that could be used against them. A few, one in the Norwegian group and one in the German group admitted to being uncomfortable with other people being able to see and possibly make use of their IP-addresses and location information. However, one of the same respondents admitted to not caring too much about it anymore, because she did not know what to do about it. Furthermore, when one of the respondents asked what an IP address could be used for, and another participant in the group responded by saying "they can get you when you're streaming" (Interview 1, German students, p. 2), many of the respondents in the group then said that they would consider the IP address as private information. Regarding GPS coordinates (location services), some of the respondents in the German group did not know what it meant. When another explained, they did not see the harm in using it. Later in the conversation one of the respondents remarked that he would use location services when the application had to make use of it to work properly, such as Google Maps and Ruter [application for public transport in Oslo]. Only one of the respondents in the German group and one in the Norwegian group had reservations as for using location services. The respondent in the German group admitted to thinking it was "creepy" that someone could watch her (Appendix 2, Interview 1, German group, p. 21).

Neither the German respondents nor the Norwegian ones would consider their religious beliefs or political opinion as personal information: one of the Norwegian respondents even stated that she thought it was important to be open about her beliefs. However, in the debate about whether political views should be considered personal information, the Norwegian group discussed whether or not they thought that it should be allowed to be anonymous online, and possibly post strong and possibly controversial or abusive opinions. One opinion was that it is better with anonymous people causing harm, than forcing people to give their full name, and in that way risking that people do not to speak at all (Appendix 3, Interview 2, Norwegian group).

During the interview the German group of respondents initiated a discussion on how they had heard how it was possible to see how much their Norwegian neighbour earn, by only

knowing their name. Most of the German respondents considered wages a private matter, even though one respondent thought it would be valuable for equality (Appendix 2, Interview 1, German group).

In the following section I analyse the findings accounted for in this section.

5.1.1 Protecting the address, using location services

On a general note, it could seem as though there is little information that the respondents in both the Norwegian and German group consider personal. That could be because they find it hard to imagine personal information without being questioned directly about specific topics. However, of the topics the respondents themselves produce and the ones I ask about, it seems as though little information are considered to be personal to the extent that the respondents take precautions to protect it. Besides this general note, judging from their answers, the German respondents seem to be the group that are most concerned about their information privacy, this assumption is made by comparing the overall impression of the interviews. This group are more alert to possible threats and issues regarding how their information might be used and possibly violated online (Interview 1, German respondents). Furthermore, they are more aware of current issues on information privacy, especially through media. The German respondents frequently refer to incidents were people have experienced violation of their information privacy. Judging by the intensity of the conversation and how the respondents keep interrupting each other in sometimes a quite loud manner, it seems to be a topic that engages the respondents. The latter notion might also be explained by natural factors, other than merely their interest in the topic. First and foremost, there might be that the communicative culture in Germany is louder and more forward in comparison to the Norwegian communicative culture. It may also be that in the recruitment phase I located a group of respondents with a particular interest in the topic, as discussed in the chapter about the project's limitations. However, seeing that the answers to the questions seemed less informed than expected, I am uncertain as to how involved the respondents were in information privacy at first.

As discussed through the previous chapters of this thesis, the aim has not first and foremost been to discover if the respondents are concerned about their information privacy, but whether they act upon that concern or not. As expected it seems as though the German group

of respondents consider more information about themselves personal than the Norwegian group, but what is more interesting is that they seem to go to greater lengths to protect that information. The German group of respondents do take more actual precautions in protecting their name and address by not disclosing the correct ones when they are unsure of the intentions of the recipient (e.g. the example of names on Facebook and false e-mail addresses (Appendix 2, Interview 1, German group).

In contrast to the German group of respondents, the Norwegian group show little concern or restraint on actual disclosure of personal information. As in the German interview, this could be caused by that the respondents find it difficult to imagine personal information without direct questions. However, from the answers they provide there seems to be little information that the Norwegian group want to protect. The respondents do find their medical journals and personal identification numbers personal information. However, when asked about the precautions they might take to protect that information, they do not do much about it. The Norwegian respondents found their medical journals personal, whilst simultaneously viewing the transition into e-journals as valuable progress. The respondents are comfortable with various doctors viewing their medical journals, and do not seem to concern with their information being online. As accounted for in the previous section, one of the Norwegian respondents are aware that other doctors than her own may see her patient journal, and does not seem to be bothered about that. Furthermore, she even says that even though doctors might see it that it does not mean that others will see it. The latter notion can arguably be connected to the respondent's general trust in people, and that it is based on the values of her society. In reality, even though the doctors that could see the respondent's journal would not have the intentions of "leaking" information to others, they are merely human and thus prone to error. This was exemplified when a doctor in New York accidentally leaked 6,800 patient journals, by a technical mistake (Boulton, 2014). It would seem as though the respondents the respondents' background makes her trust people, almost unconditionally, even though the realities might not portray the same image.

The argument of this section has been that the German respondents seemed to be more concerned and take more precautions for the sake of their information privacy than the Norwegian respondents did. However, when I asked about whether the groups regarded electronic identification, such as their IP-address or GPS coordinates provided by location based services (LBS) as personal information, only one respondent in the German group saw

the possible threat. As mentioned in the introduction, LBS may not only show the place you live it shows were you are at all times. Many smart phones have their location services switched on by default (Apple, 2014). Recent studies of location data showed that due to the predictability in human movement patterns, it is only necessary to collect four different points of location and time to identify an individual (Palmer, 2013). In a group, such as the German group, that took actual measures not to reveal their full name and address in many cases, reason would expected that they would be especially cautious when making use of LBS. However, as accounted for in the previous section, several of the German respondents did not know what LBS was. Furthermore, the majority of the German respondents seemed to be of the opinion that information stored about them in servers were only analysed by computers. The combination of not knowing what LBS was and then not believing that any human being would make use of LBS information provides reasonable explanation as to why the German respondents take care not to reveal name or address, whilst making use of LBS.

In this section I have accounted for what the Norwegian and German respondents considered personal information, and if and how they protected that information. At this point of the thesis, the argument is that based on the interviews alone, the German group of respondents are more concerned and act more upon that concern than the Norwegian group of respondents. In the following section I continue to account for findings on how the respondents in the two groups protected their information, and analyse the findings thereafter.

5.2 Protecting information

To answer the question of whether the respondents were affected by protection of information privacy in their *everyday* use of applications, I asked several questions with the aim of uncovering if the respondents' actual disclosure of information. As accounted for in the previous section, especially the German group tried to conceal their online identity to some extent by using false name and e-mail addresses. The Norwegian group of respondents did little to protect their information, besides not allowing applications to access the microphones on their smartphones. Furthermore, one respondent admitted to being especially cautious when downloading material illegally from the Internet. He would use another PC whilst downloading, in addition to a proxy server [a computer that works as a station between the user computer and the Internet, as a safety precaution].

A topic that was discussed by the Germans was that several of the respondents had covered the lens of the web camera on their laptops with a sticker or something of that sort, in fear of their cameras being hacked. This seemed to some extent to be caused by an example of a girl being watched in her own room by a person that later proceeded to post what he had seen, online. The girl committed suicide (Appendix 2, Interview 1, German group). In the Norwegian group of respondents, only one reported of having done this. However, most of the respondents had heard about the phenomena (Appendix 5).

Another topic that also was discussed by the German students was that they were cautious about pressing the "like-button" on anything on or outside Facebook, in fear of information about them, their pictures or their views would be spread further, or that Facebook would be able to track them "outside" of the site. One of the respondents talked about the example of not wanting to press "like" on any news articles because of this (p. 29, Interview 1, German group). Another of the respondents said that he did not want to press "like", in fear of other people seeing what websites he visited, even though he claimed not to visit any illegal or frowned upon sites. The like-button was invented as a way of giving positive feedback on a post of any sort. It was originally invented by Facebook, but has spread to countless other sites (Facebook Developers, n.d.).

In the same spirit, the group of German respondents expressed scepticism when they talked about the possibility of Facebook and other companies such as Amazon collaborating and being able to create specific advertisement that address them directly.

[…] but if they would target me directly – I guess, and ad on the side is one thing maybe, but if I would get a direct e-mail, that would again be on step—[too far] (Appendix 2, Interview 1, German group, p. 25).

The respondents discussed the possibility of an online provider knowing about their personal relationships and make direct suggestions to them based on that knowledge, such as sending an e-mail suggesting that the recipient buy his girlfriend a gift.

[…] Like I would get an e-mail [from a business or organization] then, "Hey, send your girlfriend.." – like wait, who are you? Who's talking to me, how do you know I have a girlfriend, how do you know it's her birthday tomorrow? (Appendix 2, Interview 1, German group, p. 25)

Some of the respondents from both groups said that they would rather use their computer than their smart phone whilst for instance using online banking. One of the Norwegian respondents was also careful to update the application "Java" [security system frequently used in online banking], to make sure it could not leak information (p. 10, Interview 2, Norwegian group). One of the German students admitted to that regardless of it was grounded in reason; the feeling of being inside of a room in for instance her home, made it feel like it was safer to go online (p. 9, Interview 1, German group).

One of the German students had also changed her e-mail-provider to a company that was committed to not spread her information, due to concern for her information privacy (Appendix 2, Interview 1, German group).

To uncover whether the respondents acted upon concern for their information privacy, I asked if the respondents had rejected applications that had asked to access their information. Some of respondents in the Norwegian group had declined to download an application due to concern for the privacy of their information. The rest had either not experienced this, or they had declined downloading an application for reasons such as "I did not want it anymore" or due to lack of capacity on the phone, or a last one did not download that many apps at all (Interview 1, Norwegian group). One of the German respondents admitted to rejecting applications if they asked to access information about her. When asked about why she would not download some applications and give them access to her information, she said "[I]t's just so weird if someone like, access, and I can't control it, so that's why I say no, and because I don't know what to do with it if they did [access personal data and misuse it]." (Appendix 2, Interview 1, German group, p. 7).

A few of the Norwegian respondents talked about how they disliked having some applications run on their phone without them having control over it, and their solutions were in those cases to drop the applications and enter the website through a browser or the likes. When asked if they would accept an application to enter their photo album or microphone some of the respondents said that they would not allow it. The rest of the group said that it depended on the application, seeing that some of the applications would not be of any use without access to e.g. photo album (such as Instagram).

When the application ValYou was presented and it was discussed whether the respondents would make use of it, one of the respondents in the German group, said that “I think as long as the convenience is caused by such apps or whatever are bigger than the fears of people getting your information, this system will work.” (P. 9, Interview 1, German group).

Furthermore, in the discussion whether the respondents would give their information to an application the German group stated that it depended on what kind of application it was. When the example of “Ruter” [public transportation application in Oslo] or “Amazon” [online book store] was brought up, several of the respondents in the German group stated that they had given all their information, including their credit card information, due to the fact that it would not work without it. One of the respondents ended the discussion by stating that

[Sighs] To be really honest, I would probably just allow it, because I'm a bit careless like that, but what's the difference, on the one hand it's a necessary part of the app, whereas on the other hand it's an unnecessary part of the app, and I don't know what they want with that information, but yeah, like I said, I would probably just push "okay" so I'm maybe the wrong one to ask about that case [laughing] (Appendix 2, Interview 1, German group, p. 11).

In the discussion on the use of applications and their functions, several of the respondents expressed how they thought that it was positive that services such as Facebook, Spotify and Netflix filtered information, based their searches on the information available about that person and personalized results. One of the respondents admitted to appreciate how Facebook would help him sort through all the information that was available (Appendix 2, Interview 1, German group, p. 14). The same respondent also appreciated how music streaming services such as Spotify could suggest new music based on what he had previously been listening to. Another respondent appreciated the convenience of making use of LBS to e.g. help him get home on time.

In the following section I analyse the findings of this section.

5.2.1 Information privacy versus convenience

The example of how one of the respondents felt it safer to venture online whilst inside a physical room, instead of outside on e.g. a smart phone, seems to be the extreme of the

general point I take from the findings in the previous section. The extent to how the respondents protect the privacy of their information it seems to be sporadic and often based on the value found in the convenience of the application. There is a possibility that the questions were not sufficient to uncover how they protect themselves, or that the respondents did not reflect upon what could be seen as protecting their information. However, considering both interviews as a whole, the image of sporadic and non-logical protection seems to be the common denominator. As discussed in the introduction, the information flow in today's society is ever increasing, and with a complex topic such as information privacy, that might be a part of the reason why the respondents in the two interviews are cautious about aspects such as covering the web camera lenses on their laptops to avoid hacking, and not allowing applications to access the microphone on their phones, whilst willingly using location services and applications such as Instagram, which was accused of having a too free privacy policy on the users' pictures (Paul, 2012).

Whilst, some part of the protection is natural, such as some of the respondents being careful when they are streaming content illegally, the other measures taken seem to be of a somewhat random nature, often based on the media or what other people do online. Especially in the German group, several of the reports of the respondents taking action to protect their information come as a result of a story in the media. An example in the German group was when the chat application "WhatsApp" was bought by Facebook, and many of WhatsApp's users moved to another application to protect their information privacy (Dredge, 2014). However, after a week the new application shut down, because so many WhatsApp's users never left. Another example was when Facebook changed its information privacy policies many Germans reacted by writing an information privacy statement on their profiles, refusing to let Facebook violate their information privacy (according to one of the respondent in Interview 1, German group) (Figure 1).

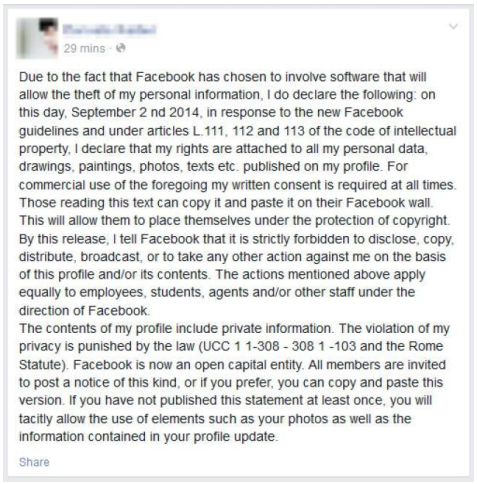

Figure 2. "Privacy Notice". (Source: Emery, 2012).

Even though the measures taken to protect information privacy seem sporadic, one common denominator seems to be captured in the German respondent's statement about the convenience of the application being what motivates people to take it into use. The value of the application seems to be measured against the value of information privacy when choosing to make use of it. If the application is attractive enough, it seems that there are little limitations to what kind of information the respondents will give it (such as Amazon or Ruter). Very few of the respondents express set principles when it comes to information privacy and evaluate the application on its usefulness when deciding if it should be allowed access to components of the mobile phone. The two exceptions seem to be pictures for the German respondents and the microphone for many of the Norwegian respondents. The Germans express unease on the topic of pictures of them spread and used in the future: some of the respondents mention if an employer should see them, or even some future enemy that could use the pictures against them. When I asked the Norwegians about whether they let applications access their microphones, they seem to express the same unease as the German respondents do about pictures, a sort of fear that someone could hack their microphones and listen in on them. Even though the reactions in both cases are interesting, it may just as well be random, based on previous experiences, something that happened, a scandal in the media and/or a very small sample.

Based on the findings and analysis presented in this section, it seems valid to continue the argument that the German respondents are more concerned and restrict the disclosure of information based on that concern to a greater extent than the Norwegian respondents do. In the interviews, the Norwegian group of respondents show little concern and thus little action

in protecting their personal information online compared to the German group of respondents. A note to take from this particular section is that in regards to applications, it would seem as though several of the respondents are willing to lower their demands on information privacy as long as the application is convenient. In the following section I account for the findings based on a question I asked in an attempt to uncover the respondents' willingness to protect their information.

5.3 Willingness to pay

One of the questions the NBT and NPDA report asked was whether the respondents would consider paying a monthly fee of NOK100 instead of giving their information when using applications. The majority of the respondents in the survey responded negatively to this. However, as the authors of the report noted, the suggested amount could have been too high to get a positive response. In a further attempt to uncover the respondents' willingness to protect their information, I asked this question in the interviews for this research project as well. The only difference was that I lowered the price. When I asked if the respondents would be willing to pay a small fee for using application without giving out information, several of the German respondents were positive. When I proposed NOK50 a month, most of the respondents would consider it. However, they stated that they would be more willing to pay to a provider that needed the money to develop an application than a provider that would take a fee not to use their information. One specific example of this came from one of the German respondents saying that she would not like to pay for Facebook. However, she would be willing to pay for newspapers or journalists, needing funding to survive (Appendix 2, Interview 1, German group). Furthermore, some of the German respondents seemed more willing to consider the possibility of paying for the application, and thus avoid disclosing their personal information, at a later point in life.

When the same question was asked to the Norwegian group of respondents, the majority would be willing to pay a small amount for the use of an application; however they linked their willingness to the type of application, whilst also saying that they would only be willing to pay for it one time, not monthly. One of the respondents would be willing to pay for an application for the increased convenience of not having to enter all his information before taking it into use. Another person expressed disbelief in it having anything to say for her personal information, seeing that she was of the opinion that if someone wanted to get her

information they would find it on the Internet regardless (Appendix 5).

Almost all the respondents positively received the solution of paying for not disclosing their information. Therefore, it could seem as though they were interested in protecting their information in that manner.

As I have discussed in the previous sections, the concern and actual disclosure of information seems to be sporadic and grounded in multiple factors in both groups of respondents. Furthermore, it is evident that in a complex topic such as information privacy, the challenge lays in extracting clear answers. In both conversations with the two different groups, it proved to be a challenge to stay on focus of what they actually did to protect their information. As discussed in the methodologies chapter, I had anticipated this factor, and brought in a stimulus material. In the next section I present the results from introducing the ValYou application and thereafter analyse the findings.

5.4 ValYou

In the end of the interview I presented a smart phone and demonstrated how the application ValYou worked. The aim was to stimulate a reaction, enabling the respondents to consider the protection of their information privacy. One of the questions I asked was basically if they would consider making use of the application. The respondents that were most concerned for the privacy of their information when making use of the applications were the Germans. However, not many of them would consider not making use of the application because of that. Several of the respondents reacted positively to the application in itself and would consider it. To try to uncover if the respondents would alter their decision to use or not use the application based on whether they trusted the provider or not. I then asked about whether they would change their opinions when they got to know that it was a major telecom company that had created the application, some of the Germans responded positively. In the Norwegian group, the majority said that their decision would not necessarily be altered if it were Telenor that provided the application. Their focus would rather be on if the provider would have enough funds to reimburse them if they lost their money. They responded in no particular way when learning it was Telenor that was the provider, besides one of the respondents. She expressed that she would not take it into use if Telenor were the provider, due to a previous negative experience. When the German group heard that is was a

Norwegian telecom company, some of them said they would consider making use of the application if a Norwegian provider made it, contrary to an American or Chinese provider.

Another aspect of the conversation that was particularly visible in the Norwegian group of respondents was that it was of more interest whether the provider would be able reimburse them if their money was lost, than if their information privacy was lost. The German group was less concerned about their money and more about the information, whereas the Norwegian group derailed into a conversation about whether they brought their credit cards on vacation or not. When being presented this application after one hour of conversation about information privacy, few of the respondents in either group asked questions about information privacy, but talked about what would happen to their money, and other security issues.

Both groups quickly linked the use of ValYou to the use of a regular credit card, and did not see any harm in that. However, the German group mentioned that they would not use credit cards as much as the Norwegians do, and they were more sceptical to an application such as this, but mostly due to the fact that they feared that it would make them spend more money. Furthermore, when asked about what the German group would be most worried about, most of the group except one respondent were more afraid of losing their phone, than losing their information through the Internet from their phone (Appendix 2, Interview 1, German group, p. 20).

In this section I have described the findings regarding ValYou. In the following section I analyse those findings.

5.4.1 Privacy vs. security

In the discussion on about the implications of loss of information privacy it seems as though it was difficult for the respondents in both group to grasp how that would harm them. For instance, when discussing what could happen if people look into their bank account, the only risk they considered was whether people could get their money or not. They did not seem worried about the threat of someone using that information for their own benefit. I introduced the applications “quick pay” function, which allows the user to touch the phone in question on a NFC-ready terminal for any amount up to NOK200 without having to enter a code. After the introduction of the application, the first question from both groups was if it was possible

to alter the security settings on the application to lower the amount that could be used in the "quick-pay" function. In other words, the initial reaction did not entail information privacy issues, but security issues, and worry for small amounts such as NOK200.

To test if trust in the provider had an implication on the respondents decision to use the application or not, I asked if it would be of any difference to their use when they learned that the provider was a large Norwegian telecom company (Telenor). The majority of the Norwegians said that it would not. However, the important aspect for the Norwegian respondents seemed to be if the provider would be able to reimburse them if their money was lost. In the German group, the fact that the provider was Norwegian and not American or Chinese made some of the respondents more positive to the application. Even after discussing information privacy for an hour, the initial responses to a new application was whether they could make sure they would not lose money or not. The German group even stated that they would be more afraid of losing their phone than having the privacy of their information invaded through the Internet (Appendix 2, Interview 1, German group, p. 20). The lack of connection to information privacy through ValYou might be explained in many ways; one of them is that the providers might have created an intuitive application that helps the consumer understand it easily based on previous knowledge of applications. Another reason might be that compared to the protection of their money, protection of information might be less important.

At this point in the account and analysis of the data from the interviews it seems as though the reactions to the application did not vary at any length between the groups. Both groups reacted similarly by discussing how secure the application was, and the possible repercussions of a lost phone. It is interesting that after 45 minutes of discussion on information privacy and applications, none of the respondents besides one in the German group would be concerned for the protection of her information privacy when making use of ValYou. In the Norwegian group of respondents, this was the one topic were it could be argued that they were less trusting than on other topics. This might be due to the possibility of losing money. These are of course only speculations. However, in the German group of respondents it could be argued that they would trust a Norwegian provider of an application. Referring to RQ2, it could be argued that in this topic the privacy paradox could be a reality in the German group of students. When the respondents trust the Norwegian provider, they

would make use of the application if it was convenient enough. I discuss this further in the concluding chapter.

In the discussion of attitudes and actions in information privacy, I asked the respondents if they were aware of possible threats of losing their information privacy of information. There was a reoccurring difference between the German and the Norwegian Group in how they answered those questions. In the two following section I account for those findings. I start with the discussion in the German group.

5.5 Fear of future consequences

The individual rationale for information privacy may as discussed in the literature chapter vary on several levels (personality, culture, experience etc.). If an individual is aware of possible threats of loss of information privacy, it could be argued that their attitudes would be different than those of an individual that are not aware of any threats. In this thesis the question has been if the attitudes (such as concern) affect the individual's everyday use of new technology such as applications. However, as discussed in the literature chapter, the essence of the privacy paradox is that there is often a lack in correlation between what people say they are concerned about and how they respond to that concern. To discover if the privacy paradox is a reality in Norway (RQ2) a vital discovery was whether the respondents were concerned or not. Based on this, I asked if the respondents were aware of possible threats of loss of information privacy. By "loss of information privacy" I mean when any measure of personal information is made available online to one or more people that the respondents would not want to have that information.

During the conversation with the German group of respondent a reoccurring topic was how the loss of information privacy might affect them in their future, or if their lives would go in a certain direction. Several of the respondents discussed how loss of information privacy could affect them if they in the future were to hold a powerful position. As accounted for in the section on what they regarded as personal information, the German group expressed that the pictures of them online was personal and not for other's use. It was also with regards to personal pictures, the majority of the German respondents saw the possible future threat of being targeted by someone with malicious intent, by an opponent or an "enemy". The group started discussing the possibility of deleting information online, and some of the respondents

thought that a service that deletes information about them would be of necessity one day. In the same discussion I brought up the saying that claims “nothing to hide, nothing to fear”. Even though the group did not have anything to hide, they expressed that they would want be able to have the opportunity to hide something. Two of the respondents said that even though they did not have anything to hide now, they might have something to hide later in life. Yet again the example of pictures that had been posted online was brought up. This time the threat was that it might be misused in a future setting, and hinder employment opportunities.

Just if you have a picture […] and there is a guy, that don’t like you, because you did [something] and he’s good with Photoshop [photo editing service], he can do anything with a photo. And in the end, even if you didn’t do it, and you can prove you didn’t do it, […] you get trouble, just because he has a picture. (Appendix 2, Interview 1, German group, p. 4)

One of the other respondents in the German group noted that she would be more afraid of how her information is used right now, than how she might end up in a scandal in the future. She was of the opinion that there was some irony in discussing possible future threats, when she felt that everything she did online could be seen today. Following this statement, two of the other respondents reattributed with: “I think a lot of them do like, they know you like these things, [or that] you may like these things, that's just advertising, I don't have a problem [with that]” and “This is a simple computer program, “you bought this”, “[an] other person bought this”, “maybe you like this”, it's a simple computer program, it [has] nothing to do with me [personally].” (Appendix 2, Interview 1, German group, p. 13)

The Norwegian gro up also discussed the notion of information being used against them. Referring to how politicians might experience that information about them might be used against them at some point. In this discussion one of the respondents stated that; “In general, I’m not afraid of giving out personal information about myself, but it is about how it might be used and how it may be misused later. I.e. when is it deleted? Is it ever deleted?” (Appendix 3, Interview 2, Norwegian group, p. 8)

When asked about the possible information privacy related threats of downloading and making use of applications, one of the respondents in the Norwegian group said that he did not download applications for e-mail, because he had heard that the application could read his information. In the same discussion, several of the other respondents had heard that

Facebook's Messenger application [chat application] could read their messages. However, none of the respondents reported any restrictions towards the application.

When the German group of respondents discussed possible ramifications of loss of information privacy, they kept mentioning "them" and "they". Therefore, a natural follow-up question was who they wanted to protect their information privacy from. Their immediate response was "Big Brother" or "Google, Facebook" and "Silicone Valley" (Appendix 2, Interview 1, German group, p. 14). In the Norwegian group, the mention of "them" or "they" did frequently occur. When I asked about who they wanted to protect their information from, none of the respondents had an immediate reaction. After a while, two of the respondents answered that it would be a hypothetic individual that would want to harm them.

In this section I have accounted for the findings from asking if the respondents were aware of any threats by loss of information privacy. In the following section I analyse the findings accounted for in this section.

5.5.1 Reasonable fear?

The fact that only two of the respondents can identify one possible threat of loss of information that could happen at in the present time, might attest to several factors. First and foremost, it could be argued that since none of the respondents in both groups identify a particular threat, that none of them have experienced any particular violation of their information privacy. In an attempt to estimate the fraction of famous people in the world, Arbesman, calculated that based on the number of living people that have their own page on Wikipedia, 0.000086 or 1 in 10 000 people could be argued to be famous (2013). Without going into the discussion of what constitutes a powerful person and if a famous person is a powerful person, this number suggests that few people enter into that category during their lives. Thus the predominant perceived threat of loss of information privacy in the German group could be argued to be a future and less likely threat. The reasoning for these answers might be a sign of how the respondents find it hard to relate threats to their everyday use of new technology and applications. Furthermore, based on the German respondents want to be able to hide something in the future, and possible delete online information might also suggest that they envisioned a future with responsibilities beyond what they had at the time of the interview. This future might include responsibilities towards a workplace and a family

amongst others.

Among the Norwegians, the discussion of threats of loss of information privacy did not spark a lot of response. After a while of thinking, one of the respondents answered that it would have to be individuals with the intent of harming her. One of the respondents also mentioned a future possibility of harm if he were to become a politician. Thus, the Norwegian respondents spoke little of "they" or "them" when addressing possible threats. Furthermore, possible threats were not a reoccurring topic in this conversation. In comparison to the German group of respondents, the Norwegian group seemed very little concerned about possible threats. The respondents admitted that lack of knowledge about protecting information privacy, and disbelief in how they could be harmed guided their attitudes on information privacy. The Norwegian group's response in this topic seemed to be confirming to the general impression of the group. They were not as concerned about information privacy and their actions seemed to correlate with this. This could in turn illuminate the argument that the Norwegian attitudes and behaviours seem to be connected with their trust in other people in general.

As accounted for in the previous section, the German group of respondents were quick to identify "Big Brother", "Facebook and Google" and "Silicon Valley" as the ones that could invade their information privacy. In the Norwegian group only one of the respondents had a clear answer, and she thought that a hypothetical individual would be of harm. In the two interviews there were many differences. However, there were some main differences, and the view on "who" could harm them was one of them. In the German group they linked information privacy to topics that is popularly discussed in the surveillance debate on privacy. Big Brother, Google and Facebook are all terms and organisations that could be argued to often be associated with surveillance, especially after the Snowden-leaks (Datatilsynet and Teknologirådet, 2014). Silicon Valley is the area of business for many of these technology companies, such as Facebook and Google, and has popularly been used as an umbrella description for this bundle of organisations (Wikipedia, 2013). According to NBT and NDPA, 94 per cent of Norwegienas above the age of 15 years old had heard about the Snowden-leak (Datatilsynet and Teknologirådet, 2014, p. 20). With this in mind I find it interesting that, "Big Brother ", Snowden and the other topics connected with surveillance are not mentioned once in the interview with the Norwegian group of respondents. There might be several rationales in the discussion on why this is, some of them in which I discuss in a

later section in this chapter.

So far in this chapter on findings it seems as though the Norwegian and the German group of respondents do little to protect the privacy of their information. As discussed earlier, it is evident that the German's are more concerned and to some extent do more to protect their information privacy than the Norwegian group does. Furthermore, it could be argued that the German group of respondents know more about current topics on information privacy in the Norwegian group of respondents. However, there were respondents in both interviews that admitted to not protecting their information due to the fact that they did not know why or how. I account for the findings on this topic in the next section.

5.6 What can they do with my information?

When asked about what they did to protect their information, some of the Norwegian students admitted that they did not know enough about what could happen with their information, so they did not do anything about it. "I don't know how to protect myself, so I just don't do anything" (Appendix 3, Interview 2, Norwegian group, translated from Norwegian, p. 9). Very few of both the Norwegian and German group read information privacy policies, and most of them used applications and disclosed their information willingly. Similarly, in the German group one of the respondents admitted to not take many precautions, because she thought that there was so much to protect herself from that she did not know where to start. In addition to not knowing what to do, one of the opinions that seemed to be repeated often in the Norwegian group, and sometimes in the German group was that it was irrelevant what kind of information that was about them online. This notion was made visible through several statements that were repeated by almost the majority of the Norwegian group, and by some in the German group. This statement captured one of the opinions that frequently reoccurred in the Norwegian group: "when it's electronic [information in general] it's no longer private" (Appendix 3, Interview 2, Norwegian group, translated from Norwegian, p. 3). Furthermore, several of the Norwegian respondents claimed that it was uncomplicated to look them up online, and therefore they did not bother to do protect themselves. One of the Norwegians specifically said that "what I do online I feel like everybody is already able to see, so I don't think that in itself is a problem" (Interview 2, Norwegian students, translated from Norwegian, p. 7).

Further on in the conversation about their online presence, several of the Norwegians expressed that they did not see what anyone could have of interest in their information. Thus they did not protect their information to any length. Several of the respondents in the same group protected themselves by counting on that no one would want to "find them" online and invade their information privacy (Interview 2, Norwegian students). One of the German respondents thought that there was a general lack of interest:

Because nobody really cares! It's like you're more like, against the principle behind it [providers such as "WhatsApp" seeing information], but then again, like you said well, what if they know about your messages to your friend, like "Hey, want to meet up at five" "Okay"? Who, who cares really? (p. 7, Interview 1, German respondents).

The majority of the German group of respondents believed that it did not matter what information could be found online about them. They believed that information collected about them were analysed by a computer program and not human beings: "But like, […] I think that all the data that's out there, that's maybe not a picture or something, is all randomized, so they'll have an idea about you as a person, but they don't know who you as a person are --." (p. 23, Interview 1, German students)

When presented with the possibility of Facebook tracing them online and offline, some of the German students said that they did not mind. Their rationale being that it had already existed for a while through companies like Visa and such (Appendix 2, Interview 1, German group, p. 26).

5.6.1 Good faith

In the Norwegian group of respondents a sense of apathy or "just go a long with it" seemed to seep through many of the topics. The group seemed to not think that anyone would want to use their information, and therefore they did not mind their information being online. The majority of the Norwegian respondents were of the belief that nobody would want to search for them, thus not protecting themselves at any length. Even though most of the respondents seemed to be aware of some future danger, only one of them discussed the possibility of his information being used by advertisers or other commercial interests as a threat. In the German group, the majority seemed to be of the opinion that the fact that their information helps to personalize technology was more beneficial than the opposite. Nonetheless, one of

the respondents seemed to have reflected upon the fact that they trade information privacy for convenience.

Few of the respondents in the interviews seem to be able to connect threats of loss of information privacy to themselves in their current situations. As discussed in the previous section, most of the respondents spoke either philosophically or about the ”what-ifs” of their future when they discussed possible repercussions of loss of information privacy.

In this section it becomes evident that there are levels of lack of knowledge, one in which the respondents claim themselves and one in which that the respondents are not aware of. The possible threats to their information privacy when making information available in databases, as discussed in the literature chapter, seems to be a topic that the respondents are not aware of to any lengths. According to the literature on information privacy, it is also evident that there are levels of unknown lack of knowledge. It seems as though the respondents defend their lack of protection by not believing that anyone could want to use their information for anything. Especially in the Norwegian group, the respondents seems to operate in good faith and to some extent trust people in general to not want to find them and use their information harmfully. The German group’s trust seems to lay in the computer program’s lack of humanity. They seem to feel safe in the “haystack”. Referring to RQ2, it would seem as though the attitudes in both groups are connected to trust at some level. In the Norwegian group it could be argued that the trust are more in people in general, whilst the German group seem to trust a computer. However, it could be argued that the German group of respondents are more ambivalent in their take on information privacy than the Norwegian group. The Germans talk about possible threats, and how they protect a part of the information about themselves, whilst simultaneously expressing that nobody cares and that it is no problem that their information is available in databases. This could mean that the privacy paradox is connected to trust for the German group of respondents. Furthermore, it could seem as though the privacy paradox is more real amongst the German group of respondents than in the Norwegian group. I will discuss this at length in the discussion chapter.

As previously mentioned, during the analysis of the findings of these two interviews it seemed as though there were some reoccurring differences in how the two groups viewed information privacy. In the following section I discuss this from the perspective of the Norwegian group of respondents.

5.7 The right to information privacy

A topic that was unique for the Norwegian group was how some of the respondents wanted privacy for the sake of privacy. They did not want to hide anything, but they consciously avoided sharing some aspects of their life. Their point of reference was the increasing amount of people sharing large part of both minor and major aspects of their life in SNSs (Dzjik, 2013). Several respondents expressed a need to keep something for themselves:

[I]t's not that I want to hide the fact that I work out, or that I eat healthy now and again, but there are some parts of my life I want to keep private. I don't want to share that with the whole world and that is not because I want to hide anything, but it is because I don't want to share anything of it (Appendix 3, Interview 2, Norwegian group, translated, p. 11).

As previously mentioned, some of the Germans also wanted to have the possibility to "hide" something, but their reasoning was more because they might want to hide something in the future, or that some of their information may be the cause of harm in the future. One of the respondents also mentioned a desire to keep information about his personal relationships to himself, and that he would feel violated if some organisation or the likes approached him with this kind of information (Appendix 2, Interview 1, German group, p. 25).

Another aspect that was only discussed in the Norwegian group was their view on information privacy of their medical journals. When asked about what information they would consider private, both groups mentioned their medical journals. However, in the following discussion in the Norwegian group, some of the respondents were positive to the Norwegian journals now becoming electronic. The respondents were aware that it was possible for other doctors to look at their journal, and did not mind.

As I have discussed throughout the previous sections, it would seems as though especially the Norwegian respondents attitudes and behaviours are connected to trust. In the following section I elaborate on the possible connection between the social context of the Norwegian welfare society, trust and information privacy.

5.7.1 Privacy in the welfare society

During the interviews and the analysis of the findings, several indicators on how information privacy might be linked to the values of the Norwegian welfare society appeared. In the findings discussed up until this point, it could seem like the Norwegian group of respondents are less concerned about the information privacy than the Germans. As discussed in the previous chapters, this thesis explores whether this has anything to do with trust. Judging from the latter findings, there could be indicators pointing to that the Norwegian group of respondents are in general more trusting due to their background. One example was the medical journal being considered personal information. However, the respondents discussing this topic seemed to find it natural that other doctors might view it. Another example could be some of the respondents desire to keep a private space and withhold information from the public. In the Norwegian conversation there were few topics that the respondents expressed that they wanted to keep private, other than this "private life" (Ess, 2013, p. 10). However, the contrast to this statement is that even though the respondent does voluntarily post information on what she is doing, her smart phone's LBS could provide involuntary information. Hence, even though the respondents do not share details about herself voluntarily, she might be sharing them after all. Where the German group of respondents were aware of several topics and probable issues that could occur with loss of information privacy, the Norwegian group of respondents could identify few of those issues and are thus less worried.

As discussed in the introduction, one of the common denominators for a welfare society is high general social trust (GT). Judging from the Norwegian respondents take on inforamtion privacy up until this point in the discussion, it could seem as though high general trust creates a relaxed relationship to information privacy and possible loss of information privacy. However, the relaxed relationship might be a somewhat naïve relationship. When talking about whether it is okay that information about them is available online, two of the Norwegian respondents answers that it is okay as long as they regulate it, as long as they have given consent. Simultaneously, the respondents admit to use applications without reading the privacy policies and have most likely given consent to much more than they are aware of, i.e. by using Facebook. The following quote is retrieved from Facebook's privacy policy.

For content that is covered by intellectual property rights, like photos and videos (IP content), you specifically give us the following permission, subject to your privacy and application settings: you grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook (IP License). This IP License ends when you delete your IP content or your account unless your content has been shared with others, and they have not deleted it. (Facebook, 2013).

In short: the Norwegian respondents seems to sometime be of the opinion that the only information that is out there about them is the information they have consented to give out, and if someone got a hold of any other information, they would not care to do anything about it. It would seem as though the theorist claiming that information privacy is a value or a right would gain some grounds in Norway, judging from the indicators from the interview with the Norwegian group compared to the German group.

Another example of how information privacy might be linked to trust in the welfare society is found in how the Norwegian respondents speak about posting online anonymously. When asked about whether religion or political opinion should be private, the respondents discussed the topic of "internet trolls" who are people often anonymously causing harm on the internet by slandering or behaving in an offensive manner. Whilst in the UK the debate has been going on how the trolls should be punished (BBC, 2014), some of the respondents in the Norwegian groups expressed an opinion that it was better to let people keep posting comments anonymously, even if that meant they would cause harm, because the option of people not wanting to write at all because of the fear of the consequence of being "outed", would not be favourable. This might be an argument that the Norwegian levels of trust in general might be high enough for this respondent to trust these so-called "trolls" not to overstep boundaries. However, an argument might be that the freedom of speech are higher values than punishing people that act in a certain manner.

As discussed in the literature chapter, privacy is said to be important for the core thoughts of a democracy, because it aids people in developing an autonomous individual capable of forming and making independent choices. Without privacy, the theorists fear that people will be afraid of exposing themselves to the public's scrutiny, and therefore decline to express their opinion. Furthermore, Nissenbaum connects these notions to information privacy as well. It is clear that the group of Norwegian respondents to some extent agree with this

notion, that regardless of the risk of information privacy enabling criminal or offensive behaviour, that it is more important to ensure a society where people are free to speak and have their own opinions. This could be argued to portray a notion grounded in the Norwegian constitution, that all Norwegian citizens are entitled to have freedom of speech. Furthermore, this might seem to be rooted in trust in the society and humanity in general, which according to OECD (2011, p. 91) is a phenomena seen in society with high equality. This topic was not brought up amongst the German students. However, considering that Germany scored lower in the OECD trust survey (2011), it could be assumed that the German group of respondents are more critical to this point of view due to the lack of trust in the government in general again due to less equality in the society.

In this section I have accounted for and analysed the findings suggesting that information privacy in Norway is linked to values found in the welfare society. In the following section I summarize the main points of the analysis before I continue to discuss the findings on the basis of literature and previous research in the discussion chapter.

5.8 Summary of the analysis

According to the report from NBT and NDPA, the average Norwegian's concern for the information privacy of their information has increased during the last few years. It even seems like the young population (15-29 years old) are more concerned than the average (Datatilsynet and Teknologirådet, 2014, p. 9). However, the report notes that it does not seem like their acts correlates with their concern. One of the main aims of this project has been to further investigate this notion, also called the privacy paradox. In attempt to explore this phenomenon more in-debt I have conducted an exploratory case study. In this case study, I have conducted group interviews of two groups, one with Norwegian students and one with German students (between 20-30 years old). In the interviews, I expected to find that the Norwegian group would express concern for their information privacy, however that they would not act upon it to any lengths. In the German group I expected to find a more visible scepticism which in turn affected their everyday use of new technology. My initial thought was that one of the explanations for this difference between the nationalities was due to a high level of trust in Norway, and a lower level in Germany (according to the OECD trust index (2011)). In the exploration of this I wished to see if the concern translated into actions in the groups, hence my first general research question**:**

RQ1

Does protection of information privacy affect users in their everyday use of new technology? E.g. will the uncertainty of what an application will do with personal information about an individual, hinder that individual in making use of it?

One of the conclusions from the NBT and NDPA report (Datatilsynet and Teknologirådet, 2014, p. 32) was that the respondents were concerned, but did not act accordingly because they found it difficult to grasp the issues at hand. With the motivation of wanting to explore the actual disclosure of information versus admitted concern, research question one asked about the everyday use of new technology. Furthermore, to go more in-depth on a case, I wanted to see if the privacy paradox were a reality in Norway, and to test one possible rationale:

RQ2

Is there any reason to believe that the privacy paradox is a reality in Norway and can it be traced back to the high levels of trust amongst the population?

In the following section I discuss the analysis of the findings based on the literature and previous research.

5.8.1 General remarks

One of the first thoughts that entered my mind after the two interviews was conducted, was that there was a significant difference between the German and Norwegians in their area of focus, level of knowledge and stated action. This notion was based on the interviews as a whole, not just what was said, but also what was not said. It was evident that both groups were concerned for the privacy of their information. However, I did not find any indicators that it was due to experience. It seemed particularly evident in the German group of respondents that their opinions stemmed from media and from peers. Another common denominator was that none of the groups seem to act on a cognitive principle, determined to protect their information privacy. The Norwegian group did as expected little to protect their information privacy, and what the German group did was of a sort of sporadic nature, not necessarily in any pattern. However, a possible pattern could have been considering the

convenience of the application before the protection of information privacy. It seemed like the German group of respondents made a more conscious trade-off, exchanging information privacy for the convenience of an application. The Norwegians was mostly quite open with the fact that they either did not know enough to protect themselves or that they did not see the harm in having their information online. Even though the Norwegian group of respondents could have been argued to trade information privacy for the convenience of an application, the trade-off seems less conscious when the respondents do not fear the consequences of loss of information privacy. What was evident was that the Germans seemed to have more interest and knowledge about the topic. As discussed in the chapter on the limitations of this project, there were a number of possible reasons for the latter observation. The sampling of the groups, where the Germans was recruited through a message in a Facebook group, allowing those who were interested to attend, and the Norwegians was recruited by directly addressing them (also on Facebook), might have made the groups more uneven. However, the difference in knowledge and interest might also have been to the fact that the German group of respondents expressed more caution when discussing information privacy.

5.8.2 In the beginning

The construction of an interview guide for a project such as this was a challenge. The major challenge was to create questions that would help the respondents reflect on questions they did not necessarily have too much knowledge about. I wanted to ask questions that had no "easy" answer. This is of course could be a challenging task even for a professional. However, based on a tip from my supervisor, the first question in the interviews was "what kind of information do you consider personal" (Appendix 1). This question seemed to have helped respondents into a focus were "surveillance" did not dominate the discussion on information privacy and the protection of it. Without having any information on how the study reported by the NBT and NDPA was presented to the respondents, the "Snowden-leaks" was mentioned and asked about, which might have created a focus on surveillance in a larger scale. As mentioned in the introduction, when somebody is asked about if they are worried that foreign governments are watching their moves, many would have answered yes. However, in the interviews I conducted, I never mention Snowden or cases of surveillance. I started the interviews on a very general basis. Reviewing the interviews it would seem as though this question set the bar lower when talking about information privacy. Furthermore, it would seem as though it allowed for the respondents to think more about their everyday use

of technology. This seemed to reveal how little they connected their everyday usage to large scale surveillance or other instances. When it came down to their everyday activities, few of the group of Norwegian respondents reported of much concern or actions taken to protect themselves. Through the account of the findings and analysis through the previous chapters, it could seem as though the group of Norwegian respondents trust people in general to a degree that they have trouble believing that anyone would harm them. Furthermore, it could seem as though the Norwegians did not connect their everyday use of applications to large scale operations and surveillance.

In the following section I summarize the main findings of the analysis on the German group of respondents.

5.8.3 Privacy paradox amongst the respondents

In the conversation on possible loss of information privacy, the German group of students seem to focus on how it could harm them in the future, either in their search for employment or even if they would gain power and someone would make use of information about them (Appendix 2, Interview 1, German group). In the same discussion with the Norwegian group of respondents, they showed disbelief in that anybody would want their information. However, the German group showed real concern that someone would use their information (such as private pictures) to harm them in the future.

Contrary to my initial reflections, the German group seemed to be the ones that could conform to the privacy paradox. Considering that some of their reflections around possible threats of having their information privacy violated were real, they took fewer precautions than expected. Three of the respondents even express how they would rather risk their information privacy for the use of convenient services, such as Spotify (Appendix 2, Interview 1, German group). As reported in the previous chapter, the German respondents admitted to both trading information privacy for convenience and some of them reflected upon the fact that if it were convenient enough, the application in question would be popular (Appendix 2, Interview 1, German group).

The German group clearly stated how they saw the risk, and that they at some point would want to protect themselves (such as paying for an agency to delete online information about

them) (Appendix 2, Interview 1, German group, p. 5), but they seemed to see that more in the future. It could seem as though these notions were thought of in a time where they were had the responsibilities of jobs and families. The interview with the German group indicated a lower level of trust in general, they express several possibilities and examples of information privacy invasion and show fear of that something could happen. However, their actions seem to be more connected to what the media and masses do, rather than principles of information privacy.

In contrast to the German group of respondents it would seems as though the Norwegian group are not affected by the protection of their information privacy to any extent. They do not consider possible threats when making use of applications. This might not say that they would not express concern when asked about surveillance or "Snowden-leaks". However, when it comes to their everyday use of new technology, they do not see the harm in having their information available online. The latter notion might be based on "social trust" (Jensen and Svendsen, 2009) or trusting people in general. However, it cannot be said for this group that the information privacy paradox apply to them at any great lengths because they do what they say, even if that is not caring too much about information privacy.

It would seem as though the German group are affected by protecting their information privacy in the everyday use of new technology. However, according to the level of their concern, it might be argued that the information privacy paradox is more relevant in the German group than in the Norwegian group. The former group are concerned, but do not act upon that concern to a great extent. It would seem as though most of the German respondents trust that it is a computer that store and analyse their data, and not a person that would target them directly, which could argue that the privacy paradox is connected to trust.

In the previous section I have summarized the analysis of the findings. One of the main arguments against qualitative methods is how they are exposed to human error, and one may argue the validity of that argument. Therefore, I will in the following chapter attempt to place the findings of the analysis into the context of theory and previous research in the area of information privacy and trust, as discussed in the literature chapter. When I review the findings in light of theory, I am not making a claim that the findings are generalizable for the whole Norwegian or German population.

6 Discussion

In the study on information privacy and related behaviour, it has become evident that there are no black and white answers. In qualitative research in general it is vital to keep a humble attitude towards the data material in the attempt to ensure that no conclusions are drawn wrongfully. Reasonably, in the study of behaviour in human beings, the need for humility is even greater. Therefore, a reminder of that the findings presented in this thesis might be biased and exposed to human error is of value. However, in this chapter, I attempt to limit the chance of overanalyses by connecting the findings to the privacy literature and previous research. In the following discussion the main focus is on answering the research questions in relationship to the Norwegian group of respondents. As discussed in the introduction of this thesis, the group of German students acted as a sort of control group to compare the findings in the Norwegian group of respondents. I start the discussion with revisiting some of the literature discussed in the literature chapter.

6.1 Context-based information privacy

In the literature review of this report we have seen that notions of privacy vary from the fundamental conceptions of it being the need for "breathing room" to develop as an individual (Cohen, 2012) and the room to develop as an autonomous individual and thus making sound decisions and co-exist in society (Nissenbaum, 2010).

As a guideline for the interviews on information privacy I have made use of Westin's definition of information privacy, which is: "The claim for individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." (as cited in Solove, 2008, p. 24).

However, reviewing and analysing findings from the interviews it becomes clear that in the clutter of conceptions and definitions of privacy, one definition does not cover the scope in which the respondents in the interviews view information privacy. If information privacy is connected to fundamental human values (Nissenbaum, 2010), it is only natural that views on information privacy will vary from person to person. However, if information privacy is indeed connected to fundamental human values, it could be argued that they would be more consistent in the holders of those values.

Even though it is frowned upon to make bold claims in a research report such as this, it is evident from the two interviews conducted with young students, that their view of information privacy is context-dependent. Some aspects of their personal information seem to be of less importance to keep private, whilst others are not for anybody else to see. Other than being context driven, the views on private information vary from person to person. One example that could be of relevance is from the interview with the Norwegian group of respondents. Their view on patient journals being personal, and still allowing for other doctors to see it, might be due to a number of social context factors. Referring to the discussion on contextual integrity in the literature chapter, it could be argued that it is within the norm of the Norwegian social context that a medical journal is personal information that can be shared in some cases (Nissenbaum, 2010).

It seems reasonable to argue that Nissenbaum's contextual integrity could be a suitable theory to base several of these two groups of people's approach to information privacy. They accept different types and levels of information privacy in different settings. Nissenbaum argues that it's nothing peculiar about caring deeply for information privacy and simultaneously sharing information generously if the sharing conforms to the norms of the channel (2010, p. 127). As I discussed in the analysis chapter, this theory might explain the attitudes and actions of the German group, that care more for information privacy than they act upon. Furthermore, in addition to the OECD findings of Norwegian trust, and the GT from Jensen and Svendsen (2009), the theory might simultaneously offer an additional explanation for the Norwegian groups. The norm of trusting their peers in general could be argued to translate into trusting people and thus new technology providers in general. In the following chapter I discuss the social background of the welfare society, in an attempt to offer an explanation for the Norwegian attitude towards information privacy.

In this section I have revisited some of the privacy and information privacy theory, as discussed in the literature chapter, and started the connection with the findings of this study. In the following section I connect the findings from the Norwegian group of respondents to theories from the value-based school of privacy thought. I continue by briefly comparing the results from the Norwegian group and the group to each other.

6.2 Value-based information privacy conception?

Even though the Norwegian group does not seem to care deeply for information privacy in general, they seem to care for the protection of their "private life". This notion is a distinct notion of information privacy. One of the respondents who talks about protecting the information privacy of her private life talks about how she wants something for herself (Appendix 3, Interview 2, Norwegian group, p. 11). She is not actively hiding it, but she is making choices not to share it online with everyone. Rachels talks about this notion of the desire for privacy, not to hide anything, not because it would be embarrassing to show what went on in the private sphere, but simply because "it is nobody else's business" (1975, p. 325). Rachels continues to explain this notion by using an example of a married couple not wanting anybody to see or hear when they are having sex. This is not because what they are doing are not natural, it is just a private part of their lives (1975, p. 325). According to the respondent's statement, it does not even seem to be that she wants to hide intimate experiences such as these, but also daily activities.

These notions of privacy are somewhat basic, and will surely be found in many types of cultures, not only in welfare societies. However, for the Norwegian group of respondents it seemed as an important aspect of life. As Ess points out, this desire for "privatlivet" is a common social backdrop in the Norwegian culture (2013). The respondent claimed that this sphere was not hidden, but she expected others to respect the boundaries of it. According to the contextual integrity, the norms of the Norwegian view on "privatlivet" dictates that this sphere is being kept private. However, the respondent did little to protect her private life other than not publish pictures online. Hence, for this space to exist, the respondent could be argued to be dependent on her peers not to violating it. This kind of trust seemed to correlate with what Jensen and Svendsen's GT (2009) which entails believing that people in general are trust worthy. To draw the connection one step further; according to the author, this type of trust is the necessary foundation of a welfare society (2009). Another example of this kind of trust seemed to be found in the same respondent's reaction to Norwegian patient journals becoming electronic. As discussed in the findings and analysis chapter, the respondent did not mind that several doctors looked at her journal, because she was confident that it would not be available for others to see. As further discussed in the same chapter, these rationales could be argued to be more based on fundamental values than real life. As exemplified by the New York doctor that accidentally published 6,800 patient records online, even possibly

trustworthy people make mistakes. In other words, as mentioned in the analysis, it would seem as though the Norwegian respondent's attitudes on information privacy at least correlates with trust.

In the Norwegian case, the not wanting the public to see their "private life" did not necessarily imply distrust, as the respondent said "I just want a space that is only for me" (Appendix 3, Interview 2, Norwegian group, p. 11). As discussed in the literature chapter, information privacy in itself can be argued to encourage scepticism. Eckblad, the journalist who found the media giant's files on him, even encouraged paranoia (2014). "Control over information" and "limited access" would not necessarily be actions taken by a person trusting people, it is in general actions taken by a person that do not trust other people to not take advantage of their information (Nissenbaum, 2010). If an individual trusts people in general not to take advantage, why would she want to protect her information?

A comparison that might argue why the Norwegian group of respondents could have a more value-based orientation on information privacy is the findings from the German group of respondents. As discussed, this group had more knowledge and had reflected on the possible issues of new technology and information privacy. Where the Norwegian group of respondents did not see much harm in making use of applications without concerning about privacy, the German group of respondents did. Furthermore, they also took some precautions in controlling what information that could be spread about them, such as not revealing their name on Facebook, or creating a false e-mail address. As discussed in the literature chapter, the German group seemed to trade their information privacy for convenience in a more conscious manner than the Norwegian group of respondents.

If it was of value to place the groups within the schools of thought on information privacy as discussed in the literature chapter, it could be argued that the German respondents would lean more to the cognate-based conceptions and the Norwegian group to the value-based school of privacy conception. In the literature chapter I discussed how the cognate-based school of privacy focused on privacy as a state of being, a more conscious decision of withdrawal or control. It could be argued that Westin's definition of information privacy could theorize on the rationales of the German group of respondents. Information privacy according to Westin is "The claim for individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." (as cited in Solove,

2008, p. 24). It is evident that the German group to some extent determine for themselves what information about themselves that are communicated to others. Furthermore, as I have discussed in the analysis chapter, and continued in this section it would seem as though the Norwegian group of respondents intuitively connected questions on information privacy to what they viewed as human values. As discussed in earlier chapters, topics such as freedom of speech, informed consent and the right to be let alone were unique topics of discussion in the interview with the Norwegian group of respondents. Without going into a lengthy discussion on all of these topics, it could be argued that the focus of the Norwegian information privacy debate, correlated to central human values in Norway and Europe (according to the Norwegian law on privacy, and the EU Human Rights Convention).

As commented on in the introduction, even though the social context of the Norwegian welfare society encourages trust in people in general, and most Norwegians seem to have those values, it does not mean that people outsider of Norway would honour those values. It could appear as though the German group of respondents did not possess those values to the extent that the Norwegian group of respondents did. It could be argued that when Norwegians trust each other, and the positive feedback mechanism continues, the rationale for employing measures to protect information privacy would be less visible. However, the fact that a vast amount of personal information about the Norwegian population are stored and analysed by foreign servers (Datatilsynet and Teknologirådet, 2014, p. 23) is arguably a reason to continue researching and working towards protecting the Norwegian's information privacy. As asked by the NBT and NDPA: how close to our private lives does the information privacy violations have to come before we react? (Datatilsynet and Teknologirådet, 2014, p. 3).

In this section I have discussed how it could seem as though the Norwegian respondents' views and actions regarding information privacy is more based on fundamental values of the Norwegian society, and how the German group of respondents does not seem to have that same trust as the Norwegian group. Furthermore, I have argued that trusting other people in general might not be altogether positive, when the Norwegian people's personal data often is stored in countries that are not protected by the Norwegian law. In the following section I discuss the possible ramifications of trust.

6.3 Does trust keep us safe?

Jensen and Svendsen describe how positive feedback mechanisms drive the welfare society (2009). When an individual trust the leaders of a society with their money (through taxes) to keep the welfare system running, and then see that it is working, the individual will keep paying taxes and so the welfare society will continue to thrive. In the analysis I speculated in if trust could be the reason why the Norwegian respondents claim that they do not believe that anybody would bother to harm them, or show disbelief in that anybody would want to harm them through what information about them was available (Appendix 3, Interview 2, Norwegian group). Many critics of information privacy have claimed that the protection of it hinders innovation and the spontaneity of technological advancements. A simplistic reasoning could be that as long as the provider is trusted not to violate people's information privacy, and privacy policies are seen as a hindrance to the convenience and experience of a good application, further work to protect information privacy would hinder growth. Furthermore, as long as the mechanisms of positive feedback of being able to make use of application and not experience any "attacks" on information privacy are working, there seems to be little reason for change. However, in the next section I argue why it could be of essence to studying and protecting information privacy.

According to Lagerspetz (2014), Baase (2014) and other authors, the development of new technology and personalisation continue to excel. Lagerspetz points out that in addition to the information the user voluntarily disclose to an application, the amounts of information that might be harvested from the mobile phone's sensors and its history go beyond the voluntary disclosure. Based on the combination of these sources of information, the application is able to provide a detailed image of the holder of the mobile phone (2014). As described in the literature chapter, researchers who had access to location data from a large group of people were able to identify an individual based on four locations on time alone, calling it a sort of "fingerprint". The majority of the Norwegian respondents stated that they did not know enough to protect the information privacy of their information and one of the respondents in the Norwegian group interview stated that she did not see how anybody would want to know what she searched for online (Appendix 3, Interview 2, Norwegian group, p. 10). This suggests that the respondents did not know what kind of information is "out there" about them. Årnes and Nes confirms this notion in their study on what kind of information the applications had about its users (foreign and Norwegian applications) that the application

users were not adequately informed about "which data [that] is collected about them, what it is collected for, or how the data may be reused" (2011, p. 24).

When the information about the users does not harm them, the positive feedback mechanism will arguably work. Users invest their information into a system that is providing the desired outcome. However, as technology advances and new technology increasingly receive more information about the users, new issues will arguably arise. According to Karagiannis, there will be more mobile phones than there are people in the world by the end of 2016 and mobile internet traffic which has grown from below one per cent of all traffic in 2009 to more than 10 per cent today are expected to have an annual growth of 78 per cent. Furthermore, it is estimated that the average Norwegian's information of many sorts are stored in between 700 – 1000 databases (Johansen, 2011). According to Nissenbaum (2010) and Baase (2012), these factors could be argued to cause threat to information privacy to a greater extent. This threat was materialized when Edward Snowden revealed that the NSA had been conducting surveillance on the Norwegian people (amongst others), through their e-mails and Facebook-messages. However, as the report from NBT and NDPA suggested, many people were concerned, but only eight per cent of the respondents admitted to this having motivated them to change their online habits, whilst 62 per cent said that the case had not altered their actions (Teknologirådet and Datatilsynet, 2014, p. 29).

In the last two sections I have discussed how it could be argued that the Norwegian group of respondents could be basing their decisions and behaviours regarding information privacy on more fundamental values, such as trust, than on actual knowledge and precautions. This becomes more evident when comparing the group to the German group of respondents. Furthermore, I have in the last section argued why there could be argued to be a threat on the information privacy of Norwegians, due to the rapid increase in new technology thus threats, and how it could be of value for this group of respondents to take precautions. In the following section, I continue the discussion of why there might be ramifications for not protecting information privacy. Furthermore, I comment on how it could seem as though the Norwegian group of respondents does not connect everyday use of applications to larger threats such as surveillance.

6.4 Surveillance and self-surveillance

Countless databases have information on people that are online, and the owners of those databases sell information to other companies that make use of it for various reasons (Nissenbaum, 2010). It is evident that there is a threat of loss of information privacy for anybody who operates online. When asked about their concern about information privacy in relationship to surveillance, the majority of the Norwegian respondents state that they are concerned (Datatilsynet and Teknologirådet, 2014). However, in the interview with the Norwegian respondents for this project, the fewest of the respondents express some sort of concern or actions. It could be argued that there is a lack in knowledge about the connection between the everyday use of applications, and the threat of their information being used in e.g. surveillance.

The evident danger of the information society could be argued to be that it is not a difficult task for a government, organisation or even individuals with the right skills to conduct surveillance on a vast amount of people. According to the NBT and NDPA, the reason why the NSA was able to conduct surveillance on people in the manner that they did was because people conduct self-surveillance (Datatilsynet and Tekonolgirådet, 2014). As discussed in the literature chapter, this concept explains people in general disclose enough information online for almost anybody to conduct surveillance on them (Smith et. al., 2011). Comparing the interview with the Norwegian group of respondents to the German group it could be argued that the Norwegian group were not aware of the connection between surveillance and self-surveillance. As commented on in the analysis chapter, where the German group quickly connect questions on what they regard as personal information and how to protect that to larger issues such as surveillance, the Norwegian group does not mention the latter issue at all. It could seem as though in terms of when the Norwegian respondents in the NBT and NDPA survey are asked about surveillance, the privacy paradox is a reality. However, as my study have shown, when asked about information privacy in their everyday use of applications, the majority Norwegian respondents in the interview for this project do not see the necessity to protect their information at any length. This was further exemplified when I did a simulation of the application ValYou. Some of the Norwegian respondents hesitated to take it into use due to security concerns. However, none of the respondents considered the application a threat to the privacy of their information.

Up until this point in the discussion, I have argued that information privacy in the Norwegian group of respondents could be connected with their fundamental human values. This notion is in accordance with Nissenbaum's conception of contextual integrity. Viewing information privacy in accordance with freedom of speech and the right to a private life could be argued to be the social background in Norway. Furthermore, it could be argued that trust in people in general is a social norm in Norway as well, thus making it somewhat appropriate to disclose as much information as the Norwegian respondents do, without showing too much concerned about their information privacy. It could be argued that the respondents in the Norwegian group did not seem to be affected by the protection of information privacy in their everyday use of applications. However, when confronted with larger issues such as surveillance they would be concerned. Furthermore, in the analysis, I argued that due to the definition of the privacy paradox, it did not seem that this particular group of respondents, in the context of their everyday use of applications conformed to the privacy paradox. Basically, they seem open about their lack of protection. In research question two, I asked if the privacy paradox could be traced back to the levels of trust in the society, and for this particular group, the answer would be no, because of the absence of the privacy paradox. However, their behaviour regarding information privacy in general could at least be connected to trust.

In this section I have discussed how the respondents in the Norwegian group does not seem to connect so-called self-surveillance to major surveillance, and thus are neither concerned or behave in manners to protect their information privacy. In the next section I discuss possible rationales for the privacy paradox.

6.5 The privacy paradox and trust

In the quest to gain insight into whether the existence or non-existence of the privacy paradox in Norway could be linked to the levels of trust in society, I interviewed a group of German students. As previously discussed, the data from the German group of students was mainly used as a point of comparison to the data from the Norwegian group of respondents.

The reason why I chose to compare two countries with different levels of trust, was somewhat due to a study cited by Norberg, Horne and Horne, where researchers found that higher level of trust in an organisation increased the likelihood of the individual's willingness to disclose information (2007, p. 103). In the OECD report on trust, researchers found that

whilst Norway was in second place in trust levels in the country, Germany was in 15th place. When speaking of trust I have used the OECD's question "do you find people in general trustworthy" (2011, p. 90) and Jensen and Svendsen's definition of general social trust (GT) as trusting people in general, even those other than family and friends (2009).

Even though, findings could attest to that in the German group of respondents the privacy paradox could be connected to trust at some level, there could also be other rationales. According to Baek, one of the proposed explanations to the root of the privacy paradox is "the public's low level of knowledge or literacy (e.g. the public do not know how personal information is processed on the Internet)" (Baek, 2014, p. 34). Another explanation could simply be that most people are ready to "trade online privacy for the benefits of personal information disclosure" (Baek, 2014, p. 34). As is visible in the findings and analysis chapter, these rationales could be argued to have grounds amongst the two groups of respondents in this study. Both groups admit to not know enough about information privacy, and also to trade their information for applications.

As discussed in the analysis, the German group of respondents were the ones that seemed to have more knowledge, judged by their responses to e.g. what could happen to their information online. This group were aware of the fact that organisations collected information about them, and to protect themselves, most of the group had altered their names on Facebook, and were careful about their pictures. However, the protection did not seem persistent, and their knowledge was often based on examples from the media. In comparison to the Norwegian group, who all had their real Facebook name, and did barely mention how organisations could store information about them, it seemed as though the German group knew more and acted upon it, which would support the first explanation of the privacy paradox, i.e. that a higher level of knowledge lead to higher level of protection of information privacy. Another support of this notion would be, when presented with the application ValYou, few of the German respondents were sceptical towards what it could do with the information and when they figured out some of the security questions they did not hesitate much on taking it into use. As described in an earlier chapter, most of the Germans did not believe that the information about them in databases could cause them any harm, and did not hesitate much to use convenient applications. One of the respondents in the German group commented that as long as the application was convenient enough, it would be popular, thus

supporting the second claim to explain the paradox; most people are ready to trade information privacy for the benefits of an application.

This picture of the German take on information privacy might be oversimplified. However, as I have discussed earlier in this report, it would seem like the German group of respondents conform more to the privacy paradox than the Norwegian group does, and it could both be explained by lack of knowledge and just the desire for a convenient application. When the German group heard that it was a Norwegian telecom company that provided the application, ValYou, they also stated that it they would be more inclined to take it into use knowing it was Norwegian and not American. This could be an indicator that trust had something to do with the willingness to use a new application. Furthermore, the fact that many of the German respondents put their "trust" in the fact that their information was stored and analysed by a computer program, and not people, might add to the theory of trust being a component of the privacy paradox.

In the Norwegian group the paradox seemed less present, because the respondents did not express too much concern, or behaviour of protecting information privacy. However, as commented on in the previously commented on, it could seem as though the Norwegian group did not connect their everyday activities with applications to major issues such as surveillance. Hence, it could be a natural explanation as to why the privacy paradox did not seem as present in this group. If the group would have been confronted with surveillance, the paradox might have been more visible. Furthermore, with several groups and a larger sample, the result might have looked different as well.

When interviewing the German group of students I expected a group that would be more sceptical to new technology's alleged invasion of information privacy. I had been speaking to young German friends who meant that in comparison to Norway, they were cautious with their information privacy. When I interviewed the group of Germans they were more cautious, not always in action, but they were aware and sceptical towards the possible ramification of their information privacy being violated.

In the next and final chapter of this report I summarize the findings and discussion in the light of the research questions, and suggest future research.

7 Summary

If I were to summarize the findings of this study in two points, I would say the following: Firstly, the Norwegian respondents' views of privacy seem to be governed by a connection to fundamental human values found in the Norwegian society. Amongst those values is trust in other people. Secondly, I would say that both groups seem to trade information privacy for the convenience of an application. However, the German group could be argued to be doing the conscious choice of the trade-off. Translated into answering the research questions, I would argue that the respondents in the two groups are more or less unaffected by the protection of their information privacy in their everyday life use of new technology in the form of applications. Even though it could be argued that the group of Norwegian respondents' attitudes regarding information privacy could be connected to high levels of trust in the society, it cannot be argued that the privacy paradox is a reality in this group of the Norwegian population. In what follows I provide a more detailed summary of this study, before I end the thesis with suggesting further research.

If you have read the newspapers during the last few months in Norway, it could seem as though there has been an increase in stories about people who claim to have had someone intrude the privacy of their information. A recent example was reported by the Norwegian newspaper *Aftenposten*, where a young mother was one of several people who responded with shock when she learned that the picture she had posted on the SNS Instagram, of her two small children and herself, had been used for an article created by the website based on so-called viral news, *Buzzit.no* (Hagen, 2014). This story exemplifies what some argue to be a trend in the world of new technology, more people will experience breaches on the privacy of their information. When NBT and NDPA asked the Norwegian population, the majority of the respondents were concerned about their information privacy. However, when asked about what they would do if they knew they were under personal surveillance, the majority stated that they would not change their online habits. In this thesis I have discussed that the respondents in the Norwegian group could be argued to not connect their everyday use of new technology and the following disclosure of information to larger scaled issues such as surveillance. In the two interviews, I started off asking what the respondents considered as personal information. Where the German group of respondents quickly connected the questions to surveillance related issues, the Norwegian group of respondents did not mention any related topics. In this thesis I have asked the following research questions

RQ1

Does protection of information privacy affect users in their everyday use of new technology? E.g. will the uncertainty of what an application will do with personal information about an individual, hinder that individual in making use of it?

RQ2

Is there any reason to believe that the privacy paradox is a reality in Norway and can it be traced back to the high levels of trust amongst the population?

One of the aims of asking these research questions was to uncover if information privacy was of concern to Norwegian people in their everyday use of new technology, and more specifically applications. As discussed in this thesis, it could be argued that the Norwegian group of respondents are not affected in their everyday use of technology by protection of information privacy. There are few signs of precautions taken to protect their information privacy when downloading and making use of applications. Even though the German group does not take many precautions when making use of new technology, it is evident that they are more concerned and act more to protect their information privacy.

Another aim of asking these questions was to make an attempt to understand why the respondents are concerned for their information privacy, and still not acting upon it. By this I wanted to explore if the privacy paradox is a reality in Norway and to see if it was somehow connected to trust.

After talking to all together twelve students from Norway and Germany it is clear that not knowing much about what our information is used for, and how to protect it, is not a Norwegian phenomenon, at least not for these two groups. It might be at a higher degree in this country. Clearly, the German group of respondents knew more about the topic of information privacy and the possible threats of it, and they did take more precautions to protect their information. They also seemed to have a more pressing fear of what could happen to their information in the future. With that said, the German group knew more, but did not act in accordance, which have led me to believe that of these two groups the German group of respondents would be the ones that could comply more with the privacy paradox in general. Furthermore, as discussed in the analysis chapter, the Norwegian group did not

admit enough concern to be said to comply with the privacy paradox. They were not as concerned, and thus did not take any specific concerns to protect their information privacy. However, I am of the opinion – an opinion supported by the research undertaken and reported on in this thesis – that the information privacy situation in Norway has to do with trust. It would seem as though the value-based school of privacy could at least partially offer an explanation of the Norwegian respondents' view of information privacy. Norway is a welfare society with high GT, which seems to affect how they view information privacy. The Norwegian people trust people in general to a degree, and for this group of respondents, that means that they do not see how they could be harmed. This leads to one of the more significant findings in this project, a finding that is visible in both groups of respondents: they do not seem to connect larger issues of surveillance and collection of data to their own use of applications.

As the NBT and NDPA report notes, when surveillance was conducted on e.g. the Norwegian people, it was user data stored with Google or Microsoft that made it possible for the NSA to conduct the surveillance, i.e. the everyday use done by Norwegian inhabitants. However, none of the groups seem to be aware of this connection. One of the examples was how the Germans expressed that the information they find private is their name and address. However, when asked about the use of LBS, few of the respondents recognize that as private information. In the Norwegian group the notion of not seeing how what they search for online can be of interest to anyone, whilst not being aware of how the very phone they use every day may provide an array of information besides what they search for online.

The application ValYou did not produce much concern for the groups' information privacy either. It was evident that when the application was presented as a mobile wallet, the respondents were more concerned about the security of the application and possible reimbursement if their money was lost. There was little evidence of concern for information privacy as possibly hindering the respondents' use of the application. However, when asked about if the respondents would change their decision based on the knowledge that the Norwegian telecom company Telenor were the provider; the German respondents would consider a Norwegian company trustworthy. The Norwegian respondents were more interested if the bank in charge of the application could reimburse them if necessary.

7.1 Further research

When exploring this topic of information privacy in the context of Norwegian consumers, a whole array of possible future research opens up. The further I got into the research, the more questions I had. This did not only make it clear that this type of case study on information privacy deserves a larger format than a master thesis: it also created a major challenge in deciding what to pay attention to and not. Hence, during the course of this master project, the end product became broader than what was planned. However, without exploring this broader scope of information privacy in context, I would not have discovered several interesting topics to possibly move further with. In this research project I have had to make several decisions as to what to include and further discuss from the data material due to time and other resources. In this section I will mention a few of the topics I would have considered to pursue if time and resources were allowed.

The main finding among the Norwegian respondents seemed to be that there could be a connection between how the Norwegians viewed information privacy, and fundamental values found in the welfare society of Norway. As discussed in the chapter on finding truth, this finding might constitute as analytical generalizability. It would be interesting to conduct several individual or group interviews with different segments of the Norwegian population and further study the possible connection between attitudes and behaviour on information privacy and the population's fundamental collective values. Those segments could for instance be groups of young people compared to an older segment of the population. It would be interesting to see if this general trust in new technology is a factor of the younger generation or if it transcends the generations. Another segment that would be of interest in measuring if these fundamental Norwegian values could be connected to attitudes and behaviour would be ethnic Norwegians versus recent immigrants. Furthermore, another interesting study could be to look at the possible gap between how the respondents view surveillance and their evident concern, versus their lack of concern in their everyday use of applications. In this type of study, I would start by exploring how the respondents in both groups that were interviewed did not connect any information privacy concerns when I presented the application ValYou, even though we had discussed the topic for an hour before.

Another interesting area of study could be the media's role in attitudes and behaviours on information privacy. In the German group, it seemed as though several of their attitudes and

behaviours were inspired by stories from the media. The Norwegian group of respondents mentioned few examples from the media in their reflections on information privacy. It would be interesting to conduct a comparative study on major news outlets from the two countries, and explore if the degree of media attention on information privacy could be argued to affect both attitudes and behaviours on information privacy.

A final interesting study that could be conducted would be to study Facebook and information privacy. In the German group of respondents, Facebook were frequently exemplified as the "bad guy" in the privacy debate. Why is that? Is the generalization correct or is it media made?

Even though the findings of this thesis are not generalizable for a population, it would be interesting to see if some of the findings could be applied and expanded on in further research.

Bibliography

Amundsen, G. (2014, 13.10). Tøff kamp om hjerteslagene dine (The Battle for your Heartbeats). *Aftenposten*. Retrieved from http://www.aftenposten.no/ digital/T off-kamp-om-hjerteslagene-dine-7739952.html

Amundsen, G. (2014, 29.09). Kampen om mobilbetaling hardner til. *Aftenposten.no*. Retrieved December 10, 2014, from http:// www.aftenposten.no/digital/Kampen-om-mobilbetaling-hardner- til-7721564.html

Apple. (2014). Apple Watch Overview. *Apple.com*. Retrieved December 11, 2014, from http://www.apple.com/watch/overview/

Apple. (2014) iOS 4: Understanding Location Services. *Apple.com*. Retrieved December 11, 2014, from http://support.apple.com/en-us/HT201674.

Arbesman, S. (2013, 22.01) The Fraction of Famous People in the World. *Wired Science Blogs.com*. Retrieved December 11, 2014, from http://www.wired.com/2013/01/the-fraction-of-famous-people-in-the-world/

Baase, S. (2013). *A gift of fire: social, legal, and ethical issues for computing technology* (4th ed., International ed. ed.). Boston: Pearson. Pp. 5, 23, 25, 26, 42, 127, 357, 360,

Baek, Y. M. (2014). Solving the Privacy Paradox: A counter-argument experimental approach. *Computers in Human Behaviour, 38*(2014), 33-42. P. 34

Barbour, R. (2014). *Introducting Qualitative Research a Student Guide* (Second ed.). London: SAGE. Pp. 117, 141, 142, 147

Bernard, H. R., & Ryan, G. W. (2009). *Analyzing Qualitative Data*. California: Sage Publications. P. 5

BBC. (2014, 19.10). Internet trolls face up to two years in jail under new laws. *BBC News*. Retrieved November 6, 2014, from http://www.bbc.co.uk/news/ uk-29678989

Boulton, C. (2014, 09.05) Patient Data Leak Leads to Largest Health Privacy Law Settlement. *The Wall Street Journal*. Retrieved December 14, 2014, from http://blogs.wsj.com/cio/2014/05/09/patient-data-leak-leads-to-largest-health-privacy-law-settlement/.

Clark, D. (2014). The Role of Trust in Cyberspace. In Harper (Ed.), *Trust, Computing and Society* (pp. 17-37). New York: Cambridge University Press. Pp. 17-20,32. Pp. 17, 18,

Cohen, J. E. (2013). What Privacy is For. *Harvard Law Review, 126*(7), 1904-1933. P. 1905

Cohen, L., Manion, L., & Morrison, K. (2011). *Research Methods in Education* (7 ed.). USA & Canada: Routledge. P. 432, 436

Datatilsynet. (n.d.). The Norwegian Dataprotection Authority. *Datatilsynet.no*. Retrieved December 11, 2014, from https://www.datatilsynet.no/English/

Datatilsynet and Teknologirådet. (2014). Personvern. Teknologi og Trender. 2014. Oslo: Teknologirådet & Datatilsynet. Pp. 23, 29, 30, 32, 33, 36, 37

Dijck, van. J. (2013) The Culture of Connectivity. Oxford: Oxford University Press. P. 7

Dredge, S. (2014, 24.02) Messaging app Telegram added 5m new users the day after WhatsApp outage. *TheGuardian.com*. Retrieved December 11, 2014, from http://www.theguardian.com/technology/2014/feb/24/telegram-messaging-app-whatsapp-down-facebook.

Easypaisa (n.d.) About Easypaisa. *Easypaisa.com.pk*. Retrieved December 10, 2014, from http://www.easypaisa.com.pk/en/about/about-easypaisa.

Emarketer. (2014, 16.01). Social Users in Norway Smile for Snapchat and Instagram. *Emarketer.com*. Retrieved December 11, 2014, from http://www.emarketer.com/Article/Social-Users-Norway-Smile-Snapchat-Instagram/1010534

Ess, C. (2013). *The End of Privacy? New research apps, new research ethics?* . Paper presented at the Nordmedia 13, Oslo, Norway. P. 6, 10, 17

European Comission Directory C (2007). *Opinion 4/2007 on the concept of personal data*. Article 29 Data Protection Working Party. Retrieved December 11, 2014, from http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf.
European Convention of Human Rights (2010). *Convention for the Protection of Human Rights and Fundamental Freedoms*. Strasbourg. Pp. 1,5

Everett, E.L. and Furuseth, I. (2012). *Masteroppgaven*. *Hvordan begynne og fullføre*. Oslo: Universitetsforlaget.

Facebook Developers (n.d.) Like Button for the Web. *Developers.Facebook.com*. Retrieved December 11, 2014, from https://developers.facebook.com/docs/plugins/like-button .

Facebook (2013). Data Use Policy. *Facebook.com*. Retrieved December 14, 2014, from https://www.facebook.com/about/privacy/your-info.

Fenwick, M. (2014, 09.07) Harefield Hospital first UK centre to routinely use 'beating heart' transplant technology. *Transmedics.com*. Retrieved December 10, 2014, from http://www.transmedics.com/wt/page/pr_1405011124

Garcia-Retamero, R., & Cokely, E. T. (2013). Communicating Health Risks With Visual Aids. *Current Directions in Psychological Science, 2013*(22), 392.

Gentikow, Barbara (2005): *Hvordan utforsker man medieerfaringer? Kvalitativ metode*. Kristiansand: IJ-forlaget AS. Pp. 37, 57

Hagen, A.W. (2014, 03.07) Klonet Buzzfeed fikk klikkrekord. *DN.no*. Retrieved December 11, 2014, from http://no.wikipedia.org/wiki/Silicon_Valley

Harper, R. (2014). Reflections on Trust, Computing and Society. In Harper (Ed.), *Trust, Computing and Society*. New York: Cambridge University Press. Pp. 4,18

Hildebrandt, M., & de Vries, K. (2013). *Privacy, due process and the computational turn: the philosophy of law meets the philosophy of technology*. Abingdon: Routledge. P. 1

Hilst, R. v. d. (2013). *Putting privacy to the test: how counter-terrorism technology is challenging article 8 of the European Convention on Human Rights*. Oslo: Faculty of Law, University of Oslo. P. 53

Hornby, A.S. and Cowie, A.P. (1990). *Context*. Oxford Advanced Learners Dictionary. Oxford: Oxford University Press. P. 254

Johansen, P.A. (2011, 21.10) 700 databaser har deg. *Aftenposten.no*. Retrieved December 15, 2014, from http://www.aftenposten.no/nyheter/700-databaser-har-deg-6579879.html.

Jensen, C. and Svendsen, G.T. (2009) Giving Money to Strangers. *International Journal of Social Welfare 20(1) 3-9*. Pp. 3

Justis- og beredskapsdepartementet (2013) Lov om behandling av personopplysninger (personopplysningsloven), LOV-2013-01-11-3 C.F.R. (2013). §1.

Karagiannis, T. (2014). The New Face of the Internet. In Harper, R.H.R. (Ed.), *Trust, Computing and Society* (pp. 38-67). New York: Cambridge University Press. Pp. 39, 60-61.

Kvale, S., & Brinkmann, S. (2009). *Interviews. Learning the craft of qualitative research interviewing*. USA: SAGE. Pp. IX, 24, 47, 141, 202, 207, 245

Lagerspetz, O. (2014) Trust: Assessing the Debate. In Harper, R.H.R. (Ed.), *Trust, Computing and Society* (pp. 120-143). New York: Cambridge University Press. P. 123.

Landau, E. (2008, 09.12). Google uses search terms to detect flu outbreaks. Retrieved 09.10, 2014, from http://edition.cnn.com/2008/HEALTH/conditions/11/11/google.flu.trends/#cnnSTCText

Lanier, J. (2013). How Should We Think About Privacy? *Scientific American, November 2013*(309), 64-71.

Lekanger, K. (2013, 13.02). Norge i verdenstoppen på bruk av smartmobiler. *Tek.no*. Retrieved November 16, 2014, from http://www.tek.no/artikler/ norge-i-verdenstoppen-pa-bruk-av-smartmobiler/116802

Lewis, J. G. (2014, 25.02). Internet trolls are also real-life trolls. Retrieved November 6, 2014, from http://www.theguardian.com/science/head-quarters/2014/feb/25/internet-trolls-are-also-real-life-trolls

Mobeyforum. (2011). Mobile Wallet Whitepapers Part 1: Definitions and Vision *MobeyForum*. Retrieved December 10, 2014, from http:// www.mobeyforum.org/whitepaper/mobile-wallet-whitepapers-part-1- definitions-and-vision/

MobilePayments. (2014, 01.12). Norway's fist NFC Wallet use's Gemalto's tech. *Mobilepayments.com*. Retrieved December 10, 2014, from http:// www.mobilepaymentstoday.com/news/norways-first-nfc-wallet-uses- gemaltos-tech/

Mojoset, L. (1992). The Nordic Model Never Excisted, But Does it Have a Future? *Scandinavian Studies, 64*(4), 652. P. 652

Mouter, N. and Noordegraaf, N.V. (2012) Intercoder reliability for qualitative research. *TRAIL Research School*. Netherlands: Delft University of Technology.

Nayab, N. and Edwards, G. (2014, 24.10). How communication has evolved with new technologies. *Bright Hub PM*. Retrieved December 10, 2014, from http://www.brighthubpm.com/methods-strategies/79052-exploring-how-technology-has-changed-communication/

NESH. (2006). Guidelines for Research Ethics in the Social Sciences, Law and the Humanities. In NESH (Ed.).

Nissenbaum, H. (2010). *Privacy in Context*. California: Stanford University Press. Pp. 1, 19, 70, 75, 76, 105, 127, 128, 129, 132

Njie, R. A. (2014, 06.08). - Facebook overvåker "offline"-livet ditt. *Aftenposten.no*. Retrieved from http://www.aftenposten.no/kultur/--Facebook-overvaker- offline-livet-ditt-7657531.html#.U-NErKhMrFY

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The Privacy Paradox: Personal Information Disclosure verus Behaviours. *The Journal of Consumer Affairs, 41*(1, 2007),100-126. Pp. 102, 103

OECD. (2011). Trust. In OECD (Ed.), *Society at a Glance 2011: OECD Social Indicators*. OECD Publishing. Pp. 90 and 91.

Paul, I. (2012, 18.12) Instagram updates privacy policy, inspires backlash. PCWorld.com. Retrieved December 11, 2014, from http://www.pcworld.com/article/2021285/instagram-updates-privacy-policy-inspiring-backlash.html

Rachels, J. (1975). Why Privacy is Important. *Philosophy and Public Affaris, 4*(4), 323-333. Pp. 2,3

Remling, A. (2014, 21.09). iCloud Nude Leaks: 26 Celebrities Affected in the Nude Photo Scandal. *International Business Times*. Retrieved December 11, 2014, from http://www.ibtimes.com/icloud-nude-leaks-26-celebrities-affected-nude-photo-scandal-1692540

Ribeiro, J. (2014, 16.09). Apple Watch's privacy details under scrutiny by Connecticut attorney general. Retrieved November 10, 2014, from http:// www.pcworld.com/article/2684132/apple-watch-under-scrutiny-for-privacy- by-connecticut-attorney-general.html

Simpson, T. (2014). Computing and the Search for Trust. In Harper (Ed.), *Trust, Computing and Society* (pp. 95-119). New York: Cambridge University Press. Pp. 99.

Skogerbø, E. (2014, 20.01). [Hjelp til metodevalg masteroppgave].

Smith, H. J., Dinev, T., & Heng, X. (2011). Information Privacy Research: An Interdiciplinary Review. *MIS Quarterly*, *35*(4), 989-1015. Pp. 993, 994, 998, 999

Solove, D. J. (2011). *Privacy, information, and technology* (3rd ed. ed.). New York: Wolters Kluwer. P. 41

Solove, D. J. (2008). *Understanding privacy*. USA: Harvard University Press. P. 24

Statista (2014) Number of active Facebook users worldwide from 3rd quarter 2008 to 3rd quarter 2014 (in millions). *Statista.com*. Retrieved December 14, 2014, from http://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/.

Stevenson, A. (Ed.) (n.d.) *Privacy*. Oxford Dictionary of English. Oxford: Oxford University Press.

Stevenson, A. (Ed.) (n.d.) *Trust*. Oxford Dictionary of English (Third ed.). Oxford: Oxford University Press.

Stevenson, A. (Ed.) (n.d.) Welfare state. Oxford Dictionary of English (Third ed.) Oxford: Oxford University Press.

Tenøe, T. (2013). About us. *Teknologirådet*. Retrieved December 11, 2014

University of Toronto. (2011). A Global Overview of Digital Wallet Technologies. Retrieved June 10, 2014

ValYou. (n.d.). ValYou. *ValYou.no/en*. Retrieved December 11, 2014, from http://valyou.no/en/

Walker, A. R., & Miller, D. B. (2013). *Mobile devices: privacy risks & protections*. New York: Nova Science Publishers.

Warren, S. and Brandeis, L. (1890). The Right to Privacy. *Harward Law Review*, IV (5) , 193-220.

Wikipedia. (2014). Positive Feedback Loop. *Wikipedia.com*. Retrieved December 11, 2014, from http://en.wikipedia.org/wiki/Positive_feedback.

Wikipedia. (2013) Silicon Valley. Wikipedia.com. Retrieved December 11, 2014, from http://no.wikipedia.org/wiki/Silicon_Valley.

Yin, R.K. (2014). *Case Study Research*. *Design and Methods*. California: SAGE Publications. P. 4.

Zachariassen, E. (2013, 01.10). Siste frist for banker til å bli med på mobilbetaling. *TU.no*. Retrieved December, 10, 2014, from http:// www.tu.no/it/2013/10/01/siste-frist-for-banker-til-a-bli-med-pa- mobilbetaling

Årnes, A., & Nes, C. (2011). What does your app know about you? Data protection challenges in the mobile applications market. Oslo: Datatilsynet. P. 7

Appendix 1: Interview Guide

For the purpose of this interview I will begin by asking general questions about the respondents perception of privacy and their relationship to it. I will ask some of the same questions that would be asked in a survey. However, I will use the opportunity to ask follow-up questions. Following, I will ask questions about the respondents' use and relationships to applications and new technology. I will then present a prop; a new application that lets you download your credit cards to your phone. I will then ask if they would consider using it and if they have any hesitations. Either as a follow-up question or a new segment of the interview, I will ask whether or not privacy is a concern when downloading this app, and if they would consider not using it if they were unsure about the safety privacy policies.

The purpose of these interview questions is to answer two research questions:

RQ1

Does protection of information privacy affect people in their everyday use of new technology? E.g. will the uncertainty of what an application will do with personal information about an individual, hinder that individual in making use of it?

RQ2

Is there any reason to believe that the privacy paradox is a reality in Norway and can it be traced back to the high levels of trust amongst the population?

Finally, the questions listed below will function as a guide for the interview, seeing that I am interested in a conversation. It is not important that all questions are asked and answered categorically, therefore, there might be a bit more questions than needed listen beneath.

Questions:

For the background questions, such as age, gender, occupation, nationality and area of residence, I will have the respondents fill out a form before the interview starts.

Attitudes about information privacy:

Q1. What is information privacy to you? How would you describe it?

Q2. On a scale from one to ten, where ten is the highest value, how high do you value privacy of information?

Q3. Do you take any specific measures to protect that privacy?

Attitudes towards applications and information privacy:
Q3. Do you download applications (either on your phone or on your PC)?

Q4. When you visit a web site or download an app, do you pay attention to the providers ”privacy policy”?

Q5. How much of your personal information are you willing to give for the use of a application? I.e., information about you, or the use of location services, etc.?

Q6. Is there a difference between the applications? Would you give some more information than others? Why is that?

Q7. Do you take any precautions when it comes to the downloading and use of applications in your everyday life?

Q8. Have you ever decided not to download or make use of an app because of concerns for what the provider will do with your information?

STIMULUS: At this point, I will demonstrate a new application, called ValYou, which allows the consumer to use their smart phones as credit cards. I will not reveal who the provider is, just the application, and record the initial reactions.

Q9. Would you download this application if it were to be made available for you?

Q10. What kind of considerations would you make before downloading it? Would you consider privacy?

Q11. When you are to download an app, do you consider what the provider will do with the information about you?

Q12. Are you aware of any threaths involved in downloading and making use of applications?

Appendix 2: Interview 1, German group

Research interview 1/2
Conducted September 10, 2014, at the University of Oslo, Institute for Media and Communication.

Interviewer: Hanna Kaupang
Respondents: Six German students
Time: One hour, twenty minutes
Place: Group room at the Insitute for Media and Communication

---

This transcript has gone through minor editing to ensure that it is understandable to readers that were not present in the interview. I have let as much of the originial statements, pauses and hesitations, to convey the actual interview as well as possible. Words that were not uttered by the respondents in the interview, but was added to the transcript clarify are put in [brackets].

Codes in use

--	As if they change their minds about what they are to say
--.	Interrupted by somebody else
…	Pause, thinking
(…)	Something missed on the recording
umm hmm	Agreeing
hmm	Not agreeing/uncertain

Hanna: So-- ehm --- when we talk about privacy, it's a lot of different kind of opinions about what it is and nobody can actually define it, so I'm going to start with a question that is very general -- uhm --- and I'm asking, what kind of information about you, do you consider private. What would you be uncomfortable, kind of, giving out, in a way?

N: Yeah -- should we like just –- [looking at Hanna]

H: Yeah -- just -- when you're -- when you're ready

N: Okay

R: Just like definitions […] I would say privacy is well information I wouldn't tell everybody

H: umm hmm

R: Yeah, so

H: So, do you have an examples, would you -- umm--

J: Information on my bank account

H: Umm hmm

S: Or things I just tell the doctor, for example, about some conditions I have I just (...) private [at this point, one of the other respondents start to scribble loudly on his information sheet, which makes one word impossible to catch]

H: Yeah

F: I see as private family issues, or, boyfriend issues. Yeah, that's for me private, but, but, but, bank account is for me not so -- in Germany it's often that it's a problem to talk about salaries, and -- I don't get why so, I have not a problem to talk about it, but most people have.

H: Okay. --- So you are okay with […] name, and address, and --.

J: Hmm

N: Somethimes, I don't even like giving like -- if I'm on a website, and they just -- like some random website -- you don't really care about, but they ask you to state all your information anyways, and if you like think that okay I'm going to visit this website maybe once, then I'm just -- most of the time, I just make up like some weird name, and especially e-mail address, (J and S: Yeah, yeah) --.

S: -- so, I've --.

N: because, otherwise you get like spammed, and stuff

S: I have a second e-mail address, without my name in it, so if I don't care about the website, I just put this in and spam goes all to this address

H: Okay -- that's very clever. I will do that, [laughter]

[Group laughs]

F: Yeah -- I think also the address, is, like, what I don't want to give out, because it's very -- if you think about who like -- that people know where you live, and -- or, it's not even people, you don't know even who that is who knows it so, yeah, [voice getting increasingly high pitch, F smiling as she talks about this]

H: umm hmm. Any other opinions about the address? What about, ehm … lets say your IP-adress, you know what an IP address is? [One person says "uhm"] Do you -- is that okay, if everybody -- if that is public, and out there, and --.

J: I'm not sure what can you do with, with, ones IP address? --.

N: They can get you when you're streaming [laughter] -- or when you're downloading--. [laughter]

J: Then probably -- I'd have a problem with that

[laughter, several "yeahs"]

A: Me too

H: What about, ehm, religion? Would you like that to be -- would you tell that to anybody?

A: I'm not religious [laughter], so, [laughter]

N: Neither am I,

R: If everybody, eh, [knew] I would have no problem with it

H: No?

H: Yes, good. Umm…

F: But, for the IP-adress, I think I got this mindset that I started to not care anymore because, there are so much trouble on the internet, and it's like, so complicated, that I think: "okay, they already know, like who I am, what I buy, where I buy it and where I travel to, what ever". So, I started to think like, okay, like actually, I have no secrets, so … yeah, I think it's, like, kind of, I started not to think anymore about it, which is I think not good, but yeah.

N: There might also be that like even in Germany, in the beginning, I remember on Facebook, when Facebook changed the AGBs all the time, like the privacy settings, and everybody was like outraged, and like everybody posted this like long things like, "I hereby declare Facebook, don't you know, bla, bla, bla, bla", nowadays, like … nobody really cares anymore, it seems, you know, everybody is like okay, you know, like you said, they know everything anyways, so why bother really, and also---.

R: lost of people would just say they have nothing to hide, so why should (…) but, umm, I think it's, yeah it should not be like this because, if you have something to -- you want to hide, it should be able to hide it, yeah ---.

J: Yeah, I mean that's not the point, the point is that… people should respect, re-respect your privacy, and even if you don't have to hide, umm, anything ---.

R: Yeah, that's what I mean, because, um, if I would want to hide it, so I would be able --- eh, I should be able, bit I, I, umh ---.

J: Yeah, you should be able to.

R: …often I'm not able to hide it

N: Pictures as well, those I think is quite private. (Julia: Yeah). So if I have a Facebook, easiest example I guess, like you have all the pictures there, and you only want your friends to see this, and then you like Google your own name, and all of a sudden, there's like pictures of you on Google, that's like, accessible to anyone, that might be… quite --- yeah, like if you

have a picture where you're drunk or something and your employer sees it or whatnot, that's, um, very bad, I think,

J: Yeah

F: I also hate it, when it comes through -- you want to download an app and then the app says that you, umm -- that it gets access to your, um, pictures, and messages, and I'm like, "no, okay" and then I -- actually I don't download it anymore, because always when I read that it scares me so much because then I'm like: "yeah, no" [smiles].

H: So do you, uum, R. you said something about if you have nothing to hide, it's no problem, that --.

R: Yeah, a lot of people say that it's no problem, but I think it's a problem because, it should be -- you should be able to hide something if you want, because they also things that are, um, not criminal just want not a lot of people to know it, so. You should be able to hide (…)

F: Yeah, I think especially, they use that for economical reasons like, that is weird stuff, yeah, used as, yeah for economies.

H: Umm, so everybody agrees that that's not a valid term, that -- you don't agree with this, if you don't have anything to hide, it's no problem with everybody seeing into your private stuff.

S: No, because, it can change,

J: Yeah! As we know mindsets can change very quickly (: Yeah), and then it could -- a problem could appear. (N: Umm hmm. S: Yeah).

S: So you never know what, (J: Yeah), what will happen to you, what you will hide, maybe later (J: Yeah)

R: Just if you have a picture, umm, and you don't -- and there is a guy, that don't like you, because you did anything, [laughter], and he's good with photoshop, he can do anything (Julia: yeah), with a photo and in the end even if you didn't do it, and can you can prove you didn't do it, eh, you like, eh (Niklas: in trouble), yeah you get trouble, just because he has a picture.

H: umm

A: Yeah, and you friends can like it as well, um

J: I think, for me, it's kind of a problem that there are some information that you can probably or possibly never delete from the internet, yeah,

H: So, do you know that, if, if it's any organisations in Germany that's, that allows you, or helps you to delete your, (J: yeah), internet history, is that --.

J: I've heard about that, it sounds very good and helpful, maybe --. In the future

H: Would you use that sometime?

J: Maybe, yes.

N: Never heard of it.

S: There was a recent case, that Google lost, um, against German court, that they have to delete things just like the general statement is that Google has to delete things if someone wants to delete it

J: Searching things

N: But isn't it like almost, didn't they also say that it is almost impossible, because, like if you have your stuff somewhere in the net, and then it's like connected and retweeded, and bla, blablablablabla (S: yeah). It's like --.

R: I think, what they have to delete is if you will type in your name or maybe, let's say, a famous football player, his name, and then they make some guesses for you, what you want to type in (N: right!), they have to delete this, because, (N: the autofill thing) yeah, the autofill. Because, yeah if there was a scandal they have to delete because normally there's, um, Christiano Ronaldo has a crash in, with a woman or something like that [laughter], so the have to delete the autofill (N: okay). Not the website itself, yes, because they have no control of the website (N: okay).

H: That's interesting. -- So, do you, I know that you have your normal names on Facebook, but, do you --.

N: I don't actuall, (H: you don't?), my last name, the last name I have on Facebook is actually my middle name (H: aah, okay!), so it's like, I test if someone knows my real name, they'll not find me actually,

S: Yeah, so for me, it's I have a double last name, and the first name is very common, the last not, and I just have the first one, so there are, more (Julia: there are several), there are several with this name, but there is only one person with my name, so …

H: So, this is because you don't want anybody to be able to search for you and find you, or--.

S: Yeah, for me it's very nice to do, it's very easy to do it, because I just left out a long second name, and, um, yeah, maybe also for this --.

N: I actually don't remember, I think I changed it, like, couple of years ago, to that, because there was like, this thing going on, you know, with the, um…, data security and like, people can see through your web cam on you, and there as a general paranoia, I don't know [laughter] But, I never changed back, but like, I don't know,

H: My roommate has a sticker [pointing to the webcam on an iPad] [several agreeing "yes"].

J: Me too

N: I do so too [laughter]

J: Many Germans have ---.

S: Since I Skype, and now I -- I Skype often, I -- I just had to

J: But it is very creepy, isn't it?

S: Yeah! When I'm back in Germany, I will put it back on [laughter].

F: Um, I just recently changed my name, it was in, I don't know, I just had the feeling, because Facebook is, since I'm in Norway, more in my life than before, because I have the feeling everything goes here through Facebook. All the student societies, the Erasmus people, everything is through Facebook! It's incredible, and what is also interesting that everyone -- um, it is like, um, expects that you are on Facebook, and I have friends in Germany who are not on Facebook, and I -- just one of my friends here, she just got Facebook for this semester, and, um, yeah, so I changed my name into, um, like a short name "F", and my surname is "W" [not certain how the surname is spelled correctly], but I changed into the question "Why?", the English question "Why?". So, because of what like -- "why do they have to know my real --?" or like "why is -- should there be my real name?", because it's just in a fake thing, so, yeah

H: But it's not like that, that Facebook is used for everything in Germany? You're not used to that, or?

F: Not at least in organizations, like, um NGOs, stuff, where I was active … you do, you try also to hide some informations. Like -- and really try to use safer e-mail things, yeah.

[N is scribbeling, which causes background noise]

R: I think also there was something that the teacher put out the homework in Facebook, and then there was a court that said "no, it's not allowed". Because, you force the students, or the, um, pupils to go on Facebook and so teacher was not allowed to use Facebook for these things.

H: Okay. So, why would you use other names, or protect your information? What is it to be protected from?

N: Hmm. Umm … Good question. [Laughter].

A: I didn't choose my name -- I didn't change my name, so --.

J: Me neither --.

N: I don't like I -- I think back that when I actually did change it, there was just some general … yeah, like almost paranoia going on because it get -- back then Facebook came more more and more up in Germany, I guess. And, um, so many people did it, and then like the ball was just rolling, and everybody kind of goes with it.

J: So, it was not really your personal decision…?

N: [Sighing]. Yeah, it was at some level, but like, I wasn't actively scared of, like, some person in specific, finding out things about me. Just that, umm … yeah -- yeah, I'm not really sure. It was just like some general feeling as to, okay, something -- you know, maybe even something like anti kind of thing like, "okay, well, everything is so public these days, I'm going to make something against it, I'm going to change my last name, you know [laughter]. Smallest little protest.

J: But, I mean, only, the people I'm friends with can see my information on FAcbeook, so I can still decide, when someone's adding me, if I confirm them or not, so I'm not that worried about, um, yeah, about people knowing too much about my Facebook profile.

H: You mentioned, F, you, um, when Facebook asks you, to download a new app and says that this will access your photo's, you don't do that. What are you nervous about, or scared about, what --.

F: It's just so weird if there is someone like, access, and I can't control it, so that's why I say no, and because I -- if they -- I don't know what to do with it if they did. I think for me, it's not the fear that an individual person sees pictures, it's more like if this huge company, a global player, has it, and that is a problem I think, because I don't want to support Facebook or WhatsApp, or --.

S: So you don't have WhatsApp?

F: Unfortunately, I have it, but I use also Telegram [Messenger App that are focused on privacy: https://telegram.org/], and I have on -- do you know Telegram? It's anoter … it's like WhatsApp, but it's safer, it's safe, at least that's what they say, and you can have there, um, like a safe chat and [smiling at S] do you want to say something against it [laughing]?

S: No

F: But, yeah, um, and when, um, eh, when -- it was just some months ago when a WhatsApp thing came when it was bought by Facebook -- so, -- and then in Germany, many people, um, got -- what is it, freema?

S: Yeah, alternatives for Whatsapp. It was like, for one week, everybody was thinking, leaving Whatsapp, but then after one week it closed down because everybody stayed ---.

N: Exactly, that's the thing

S: And --.

N: Because nobody really cares! [Several "nos"] It's like you're more like -- and like, against the principle behind it [J: yeah], but then again, like you said well, what if they know about your messages to your friend, like "Hey, want to meet up at five" "Okay"? [R: It's like --.] Who, who cares really?

R: You would prefer if everybody has the other thing, but because not everybody has, it's much more easier to stay at What'sApp [J & S: Yeah], so , you don't lose so much if you stay at What'sApp --.

S: And why put another account on another thing, and you don't know if it's really safer. They just, they do an ad with it, so they advertise that they're safer, but …

J: But if you consider that especially women, I think, um, write almost everything to her friends using What'sApp [A say's "nah" and laughs].

F: But for me for example, I have a long distance relationship to Ghana. And, um, my friend, my boyfriend has a smartphone and we, of course What'sApp was our solution, like how we can keep in touch but that is crazy because like What'sapp has all our messages so, I'm really -- but yes I have What'sapp, but at least I try not to get more of these horrible apps [smiling]!

J: Yeah, it is!

N: That is actuallt super sca-- like, What'sApp and even scarier Skype I think. Because tha-- at one time it went around that like Skype, or like, it was possible that every minute or so, a screenshot was taken [Several "whoa"'s] of, while you were Skyping, and if you have a long distance relationship [laughter] or something, eeeh, that might get super dangerous, you know, if then some -- and then there's like stuff leaks all the time and like hacker get so and so many naked pictures, just last week of all these --.

R: It doesnt' have to be the company [N:Exactly!], these are random people that has a security gap, and then sees your picture -- your na -- your messages --.

N: Wasn't it just last week, all these like naked pictures of all of these like Hollywood stars [Several: Yes!]. That would be the worst [bangs the pen in the table], that would be terrible if that happens to you.

S: Also, there was a case from the girl in the US, where [J: Yeah] a boy from her school hacked in to her computer and watched her through her webcam, and then I think she... she did kill herself? [J: Yeah, she did]. Because he , yeah,-- her laptop was open, and she was in her room, and he watched her and published pictures probably, and, um, so this is also a reason why people put something for the camera.

H: I can see why, maybe I should do that too. [Laughter]. Okay, um, let's move on to smart phones. So, do you all have a smart phone, either here in Norway, or at home?

All: Yep, yes

H:Yeah? All use it? So, do you use it every day? Many times a day? [J:Yes]. For lots of different things, yeah? So do you download applications on it?

J: Some

N: Not really

A: I didn't know how it worked [laughter], so I did, um, didn't want to ask anybody [laughter][J: You can ask me] [laughter] And actually, I don't have What'sApp, so, [F:Cool], yeah. I have Facebook and I think it's enoguh, and, um, now I've read that, um, What'sApp

can control everything, your camera, your pictures, everything, I think Facebook can too, but, yea, it's enough

H: So you decided not to download the other apps, because of -- you don't know what they will do .. ?

A: Yeah, I don't need so many apps, just one for training, um, and for weather [laughter]. I don't like to play with my smart phone, like Angry Birds or other games, und, um, yes, it's okay. I don't know why I have a smart phone [laughter] but it's good to look at Facebook when you need it, but it's not that important for me, and I think it's good, and since I'm in Norway it's really good, because I don't have wireless LAN, and Ijust have my, um, internet at home and I can't walk through the flat using my phone and something, and yeah, it's really relaxing, you can talk to others [laughter], and yeah, I think it's great [laughter].

H: But everybody else, download applications?

S: I have not too many apps, but just some necessary or just he-- some helpful ones

J: Yeah, like, for example, news [Everybody:yeah], websites magazines from Germany

J: Or the Ruter App [laughter]

N: Tinder! Everybody has Tinder [laughter]

S: No

N: Not yet [smiling]

S: Um, or dictionary, yeah

H: SO, do you have bank applications, or --.

N: Yes J:Yes S: Yes

A & F: No

H: Would you have it if it was available to you?

F: No, I don't want t-- no.

H: No, why not?

F: Okay, I do online banking, but only on my laptop or computer, cause I think I don't want to do it like somewhere, somehow, like, I don't know.

S: So, I have a bank, um, banking application, but I don't do online banking things, I just check my, check my account

J: [Looking at F]. But do you think it is really more secure to do it on a laptop than on a mobile phone? --.

F: No, yeah, I just thought it at the minute I said it, that I get -- I'm sure it's not more secure to do it on the laptop than on the phone, I guess it's the same thing, but for my feeling it is more secure to be in a closed room, my room, that to do my bank stuff [laughing while talking].

R: I don't have problems on my banking on the phone, because I think it still, if someone makes it then sees my bank account, it's -- yeah, I don't want it, but if someone does it, it's -- I don't lose money, because if you want to do a transaction you still need a (...) or something like that that, so he can't do these things, so, I don't see what really happens. Maybe you can see my balance, yeah, but, okay, so he has my balance.

F: Yeah, but when I, okay I also checked before, when I was in Ghana I had a simple phone, but it was able to go in to the internet, it had a screen. Like, it was not a smart phone, but a bit smart, [laughter], and once I also checked my account, because we had no internet there, but I just checked it. I wouldn't download an app that Ijust use once in a month or something, I don't do that.

H: So you don't, um, you think about it when you download an app, you don't just press "okay" and then --.

S: But, I have also, not enough space

F: Yeah

S: I don't have enough gigabyte to download everything

H:So, when you visit a website or download an application, do you think about the information you give out, or leave, is that a part of the decision process?

J: I think --. [N interrupting, letting J speak]. Um, when, they're especially asking for information, I think about it, but I'm not, um, thinking about what could happen, or what could they be interested in without especially asking me.

[Silence]

H: So, what about information like location services, are you familiar with that, do you use that?

N: Location services ... ?

S: Google Maps

H: Like, Ruter [public transport application in Oslo], um, they can, they can, they ask you to use the plcae where you are at right now, and they activate the GPS in your phone [N: Oh, locations, yeah, right], and then get some information about you.

N: That's totally alright with me, like Google Maps, also if you have a navigation system, they ask you "can we use your location", yes obviously, you have to. [A: Or weather app] Also, Ruter, you know, when it's necessary, like when I use Ruter, and I want to know how to get quickly home, "can we use your location", "yes, of course, go ahead", but if it's like some

random app, asking me for it ... hasn't happend yet I guess to me, because I don't use apps so often, but then I would maybe be a little more careful with it...

H: Why is that? What's the difference between the apps?

Niklas: [Sigh] To be really honest, I would probably just allow it, because I'm a bit careless like that, but "what's the difference", on the one hand it's a necessary part of the app, whereas on the other hand it's an unnecessary part of the app, and I don't know what they want with that information, but yeah, like I said, I would probably just push "okay" so I'm maybe the wrong one to ask about that case [laughing]

H: You're not alone at least

[laughter]

J: I think I'm having a problem with Facebook, posting a map of the spots I've been during the last, I don't know, year

N: But do they do that?

H:They have this function, and --.

J: They can do that, yeah

S: Yeah, where pictures were tagged with you, so and you have the map and the pictures

N: Do they post it like publicly, or for you, because I actually think that's kind of cool, like knowing your routes, thats um, okay,

S: But, they generate it from the content you have posted

J: Yeah, I think they just post it on your profile [S: Yeah, so]

R: YEah, but only if you want to do it, they don't do it by their own,

J: I'm not sure actually

S: I think there's always a map were you can click on it and see where the pictures were taken. But maybe there's also of -- the thing that you can, say no, and then they'll do it --.

J: Yeah, but those are not your everyday life, um, ways, spots, they're just the spots you, um I don'† know, you posted something when you been there ...

N: Hmm ... Can be a little sketchy, like when they would do that, and then it turns out you've been at that strip club a lot of times, and like posted in front of the door, and that's not so nice, um ...

H: No

N: What we always talked about, when we're discussing these things, it's like, maybe right

now, you're not concerned about all these kinds of information, however, in 25 years, when you might be some politician, or some person in whatever position, that might come back to you, because these things don't disappear you know, from the internet by themselves

R: Yes, it is like, if you get a powerful person, like politician, in economy or something, and you also have a -- today you a friend or something that also get powerful and then they your textes, and you are just making fun of this other person and it get's out, so then you have a problem, in the mom, in the moment I don't have something to hide, but I don't know what happens, so

H: But does it change what you do today? Would it change it?

N: You know, it might actually, because like, when it came the -- there was a lot of scandals like especially during the financial crisis, when all of the sudden there was like e-mails popping up from like some managers, like, "omg I just sold this bullshit thing to this old lady, bla bla bla" you know. And then you go "omg, an e-mail is actually not just a face to face conversation, you know,there's traces of this in the web for ever, you know. And then I guess you get more careful about --.

R: I think it's just, if you're here you would be careful, but a week later you --.

N: I don't know! Like, also, in the -- it's probably like a learning process you know. In the beginning you treat internet and like Facebook and messages and stuff like, you don'† really know how to behave and all of a sudden a guy goes to jail because he like -- Internet mobbed his girl, calling her names and stuff --.

S: Anonymous, and then they find out from the IP [Niklas: Exactly!] for example, so they think they're safe, but in the end it will come back to them --.

N: And then other -- oh snap! I have to be careful, like, you know, what ever I post, and write, you know --.

S: Of course you have to be careful when you mob people on the internet. [laughter]

N: No, but not just that! No, but for example, there was this, there was a teacher in my school, and he is like a left wing guy, and he posted on some, there was some political discussion on Facebook, with a picture and there was like an article, and people like commented. And then, he posted his opinion, with his Facebook account, and he had a pretty strong, opinion about this specific topic, and then, um, a mother or father of one of the children, commented under there, like "hey, mister so and so, you know you might want to keep your personal opinion out of here, you're the teacher of my son and what-not, you know, and he-- this father was probably the opposite opinion of -- as the teacher had, you know. And even in the smaller things, you know, like you have to see "okay, this is available for many people, I have to be careful".

J: Yeah, I think we should care about that a little more, because if I was a powerful person, um, I would make of such a company deleting that site from the internet, because, if you are powerful, there are people looking for scandals, from your past, and it could completely ruin your career.

F: I think it's funny that we are more talking about these personal fears about security, than what they do with the data, like not in the scandal direction, more in that they have like profiles of people, like what they buy, where they go, what they do, where their hobbies are, what ever. Because, for me, that is more scary than, um, a naked picture of me, then because I would say, "hey, I mean you're crazy to post that". I think scandal is also how you will handle it and stand above it. But my personal fear is more like, what they do with these data --.

R: I think a lot of them do like, they know you like these things, you may like these things, that's just advertising, I don't have a problem --.

S: [Raising her voice] this is a simple computer program, you bought this, other person bought this, maybe you like this, it's a simple computer program, this is no -- it's nothing to do with me [R., agreeing when S. talks: It's no problem for me]

F.: It -- isn't that limited, that is limited information, because you can't get, you get only what fits with you

S: But, yeah --.

N: I agree with you, I think, it's-- um, it might be a problem.

S: But, yeah, I don't base my opinions on what Amazon says I like--.

N: But, even -- always coming back to this Facebook example -- even on Facebook, I think it turns out that, they modify your feed, so what you actually see [several "yeah"], by how often you click on a persons profile, or what you like, or what you type in on Google

Rafael:I think --.

N: So in the end, it's got like-- you only get a part of, your reality actually in your feed you know, so some people will disappear from you eventhough you might be interested in like what they have to say as well --.

R: If you're intereseted you click on that things

[S: Yeah, I think that -- it's, (...)]

N: Yeah, you might, you might not, you know (Sophie talking in the background]

S: But..

R: Yeah, but, so you can't see all of the feeds, so they have to separate, so I think it's better if you have the feeds of the top 100 instead of all the 800 so --.

N: Yeah! Fair enough, they have to do some separation [R: Yes], but this might be a problem --.

R: So how should they do that (...) they should do it because how much you click them --.

N: No, no! Um -- I agree that it is difficult to like -- where do you draw the line you know [J: Uhmm] but if all of a sudden an entire chunk [R: Yes of course --.] totally disappears --.

R: There can be some problems, but I think--.

J: Yeah, but actually, on almost everything you find on the Internet or you see on the internet is biased, umm, because it depends on what you Googled before.

F: Yeah, so it's always limited [J: Yeah!] and they, they -- like -- they judge what I'm going to see [J:yeah], what I'm going to find, what information [J: yeah], and that is like "what?", crazy..

H: So who are "they"?

F: [laughter] that is a good question --.

N: Big brother [laughter]

S: They are companies like Facebook and Google

J: Yeah, Silicon Valley [laughter]

H: Silicon Valley, yeah

S: But, I'm not looking for such hidden things in the Internet that they don't come up at Google, when I Google, [looking at F], so I don't know what you're looking for, but --.

F: No, no! But, that is already interesting for them, whatever you Google is interesting for them --.

S: It's not personal, it's interesting for them --. [F mumbling something] so, hmm

F: But isn't it scary for -- or not scary, wierd that they're creating, they use that for their marketing strategy [J saying something]

N: I think that's super alright! I mean, that's how they make their money [S & J: Yeah, it's the way --.]

F: But -- um -- is -- okay

N:I mean the alternative is not having any of this

R: I mean, it's like if you go to Spotify, and then you can um -- if you have Spotify, and know Spotify, and you hear some songs you like, and I think it's really great that they say "hey! do you know this artist, you make like him" so --.

S: Yeah, it's just a computer program! There's no one sitting and watching what you say and hear saying "oh maybe you like this" just based on what other people hear. And you don't have to listen to it. [Still raised voice].

R: So now I think it'ß limited, but I think it's good, because I couldn't see all the songs that are available on Spotify, so I like it that they are -- the computer program it's chose what maybe fitting me.

H: So did you hear about this case, the American company "Target" and the young girl, teenage girl, that was pregnant, they , um, started sending her pregnancy things, but she was very young [N:On the internet?] um, in the mail, and she was living at home with her parents [F: Oh] and her father didn't know that she was pregnant. And so he called to target and yelled at them because they sent pregnancy stuff back to her place. But then after a while, he had to call back and say "I'm sorry, it is true, my daughter is pregnant, she hadn't-- she didn't tell me. And that's kind of -- that's the extended version of Netflix and or -- sorry -- Spotify, but --.

[Group have not heard about this before]

N: Did she order these things though?

H: No, they anticipated -- that's what the computer programs do, they have these analytical tools, that says that you looked at this, this and this, that means that you must be here and here and here, [N: Exactly] so we'll send you this [J: and they send a suggestion] and this and this.

N: But they sent --.

S: But what's Target?

N: It's like Walmart

H: It's like this major, major store --.

S: Ah, so she did online shopping?

H: Yeah, I can't really remember, but they traced her pattern ["oh wow"] and realized that this girl is pregnant in the first trimester, the first three months --. ["Wow" and laughter]

N: And then they sent her actual goods without her ever ordering them?

H: Like goodie bags, pamphlets, you know, free stuff

N: Alright!

S: I mean, this is in the US, in Germany, I've never heard of --.

J: I don't think so!

F: Not yet! BEcause the people -- if that is the perception that it doesn't matter, then I think that will happen --.

N: But, that is, that is kind of extreme, that like, physical stuff coming to your place where you live, that's kind of the next step --.

S: Maybe if you, for example, Google mail scans your mai-- scans your e-mail for like, key words, and if you often write "I'm pregnant" you get like pregnancy test, ads on the side, but if you have an ad blocker you don't even see it, so it's okay, it doesn't bother me, but um, sending actual stuff is something different.

J: But, I think for me this is very scary, because, um --.

N: Are you pregnant? [Laughter]

J: No, but, um, if I was, and I was looking for books, on pregnancy, on Amazon or what ever, um, and they would send me mails with suggestions based on that, um, because my mom sometimes has access to my iPad, she uses it sometimes, and then she could see those mails, and that would be the same, I mean --.

S: But, if she use your account, she is in your privacy, it's not Amazon's fault ...

J: Yeah, yeah that's true

N: Yeah, but that they send stuff, that's um, that's a no-go, like

H: It's the only example I've heard of but --.

S: But, still you can say it's important to keep up traditional family values like talking to each other and um, have a stable trust relationship and um [laughter] [N: That's Target's argument] then say technology is, is, is worse -- or is like should, or the fault of technology

H: Yeah, so, um, there are different kinds of applications, and if you found this really really good application, that will help you in your everyday life, it will be very convenient, I don't know what would be convenient for you, but it would help you, like Ruter helps everybody in Oslo [smiles] um, would -- how much information would give up, where would you draw the line? Would you go as far as to adress and e-mail adress, and bank accounts and everything or would you say "my name and my e-mail, and that's it or". How much information are you willing to give out for a good app?

N:It totally depends. Like I have amazon, the app, on my phone, um, I don't why, it's super easy ordering online from your computer already, but I got it, and then you log in with that app, into your, account, and you can order via your app, so they have your address and everything, credit card information, bank information, everything, and then you can order book, while lying on the couch on your back, and I, I've given out my adress and everything there actually --.

J: Yeah, so given that, I would almost, um, yeah -- give them almost every information.

N: But, depending on the app [all agreeing], like -- if, with Amazon it's necessary that they have to have your adress, otherwise there's no need for Amazon. If for ex-- but if it would be a different app, let's say, Ruter, all of a sudden asked me for my bank account number -- well acutally they have that too, because I have the app you can buy tickets with, yeah Ruter was a bad example as well [laughter].

H: Facebook, or Skype or whatever, asked me for my bank account number, and my shoe size, and how often I go training, and where, and stuff like that, then I would not give that up, because --.

J: Sorry - did you hear about, um, is it "iClick", this new payment, um, program, Apple introduced last night?

N: AppbleBuy, yeah --.

S: ApplePay

J: ApplePay, whatever, you can just pay, with one move of your hand

S: Yeah, but it's just in the US so far, and there are some retailers already used it, so and they --.

H: That brings me to our next topic

[Taking up an android phone]

N: You bought an iPhone six! [Laughter]

H: Yeah, I got it sent directly from Apple. No, I have, this is actually another phone [F: Oh wow]. I'm going to show you something, it's an application, very similar to the one you were talking about right now. So, the media expert says that payment apps are the next big thing, and this app, called ValYou is kind of just an application you download, and it's, it's this small icon here, I can show you when you open it [showing the ValYou symbol on the screen]. And you open it -- and I've installed it now -- so let's say this -- it's a simulation, but let's say this is my bank, and I have a lot money in my bank account [N:Nice!]. And I want to pay something, so let's pretend this is a terminal [taking another phone and putting it on the table with the NFC sticker on top] where you draw your card, and it has a sticker on it, and I just walk up, and I do like this [putting the phone with the app on top of the sticker and it takes a while for it to react], [J: And it doesn't work] [N: That's why you don't use these apps.] I will complain, it worked earlier. Okey, [the phone making a beep] and it says that I can pay if I give a code right now, so I just .. [entering a code] and then the transaction is complete. ["Wow"]. So this was an amount of 456kr, if it would have been underneath 200kr I could have just tapped it, and went a way, and it would have paid for it, [N:with no code?]. With no code.

R: This was just a simulation, or what did you pay for?

H: It's a simulation.

N: The pizza, that's coming now. [Laughter].

J: But there's no difference, um, between that, and doing it with your credit card. Because in Norway, you sometimes don't even need your pin number or something, or your signature.

S: So this a big -- we discussed it earlier -- this is a big difference with Germany, because in Germany it's not that common to pay with credit card, especially when you're going out, for

example, were -- you need to have cash with you. Yeah, so I just read about it, in the news paper, that a woman tried to live with one week without credit card, and she wrote about all the situations were she had to borrow money for friends because she couldn't pay with her credit card.

H: Here, here in Norway?

S: No, German.

J: In Norway it would be even worse

S: To pay with credit card. If someone finds a credit card, you can go online shopping, and if you lose your phone, it's the same. So...

H: So, would you download this app, if it was -- if you thought it was --.

S: LIke, maybe I would wait one month, and see how people or experts reacted, and then if it get's more common it in my opinion, it could be safer, because more people are think about "how can we make it safer" when a lot of people are using it. I don't think I would have a big problem with it.

F: I think it's smart from the producers, or the inventors of this, because I think it makes you buy more eagerly, because then you don't even need to get your card out, you just take your phone out --.

R: You have to get your phone out, so

S: You don't have more money, so! --. [Laughter]

F: But you, I think, um, what I recognize now in Norway with my card is also that I spend, okay, everything is fucking expensive so [laughter], but still it's like, it feels like, if I pay with card I don't have overview with my money, so I prefer to pay with cash so I know, okay, this is what I have, and I think if you use your smart phone, it will just be a routine, just click here, click there --.

A: It's the same with the card

[Everybody speaking on top of each other.]

F: NO, I think -- yeah -- in my opinion there is a difference, because there is a difference, becuase it's not another thing, it's a smart phone, you use for all the one hundred things you already, um, doing with --.

R: Do you have an amount, or is it directly on your bank account? So, if you have money on the bank account, you can pay with this, or is it like you make a transaction on this app, and then you can use these money?

H: It depends, you can -- you download your cards into this app, so you download your visa, your Mastercard and whatever you have, so the credit cards works as they do, you get a bill, and, um, the other cards. So I think it depends on what cards you chose. And it also collects

like loyalty cards, where you would have Starbucks, were you get free coffee, every fifth, and key cards, I could have a card like to get into this building or --.

N: Is this a recent app?

H: It's coming next week actually.

N: Is it a Norwegian start up?

H: Yeah, that's my next question actually.

N: I think it's my friend that started this app actually.

H: Because, would it -- obviously you've all said that it's not a big difference between this and a credit card, but -- would it help you, or would it change your mind if you knew that the provider of this app was the -- a major Norwegian telecom company called Telenor, I don't know the similarity from Germany, but would it change anything?

N: I don't mind.

R: It depends on the company. SO if it would be a great telecommunications, um, comapny, it would be okay because, that's their world, it's like um --.

F: If they were to deal with your bank issues?

R: No, but if they had to work with my phone -- um, like phone stuff, so they invent -- yeah

J: For example Apple, yesterday, introduced ApplePay and they worked together with American Experss MasterCard and Visa, and there you can see they work with a company I already trusted, my money and my credit card [N: That's a good point], so you see, um, there's no big difference -- and -- yeah, maybe it's different if it's a company you don't know already but, --.

H: Yeah, if it was a startup, like a small company you haven't heard about before

J: But maybe it feels a little bit safer knowing that it's buy a Norwegian company ... than a Chinese, or an American,

S: Or even Chinese is really safe, because they open country, they're used to protect information so

J: But I wanted to add earlier is that, that's maybe just a matter of reducing devices and cards in your everyday life

F :And is that good?

J: I don't know [laughing]

H: So with this app, it will develop, but they will also start using this technology called "beacons" which is your bluethooth you have to have it on, and let's say you walk into a

shopping mall, and you will get offers into your app. So you will pass something, and they will collect information from your app and see that you shopped there, and there and there, and they will give you an offer that's directed to you. Like, to you, F, that you would get something from Ghana, or I don't know, but they would pick up on that, would you think that's okay?

N: It's okay, but I think it will be so annoying --.

S: I wouldn't used it, because you get ads and ads and ads and

N: There's already so much "ding, ding, ding" all the time--.

A: So much information --.

N: And all of a sudden your phone is vibrating even more, all the time, but I'm skeptical to this entire like, you get more and more dependant on your phone, so like just keep it as a telephone, as much as I can.

H: Why do you get sceptical? Or why is it a problem?

N: Because, um, have you've ever had like phantom vibrations, [touching is pant pocket], like when you think like, "oh my phone just rang", oh no it didn't. Omg, what is this thing doing to me, you know. Like this kind of more general sceptisim.

R: If you use this as your credit card, and it, um, break down or something, you can't use it. What do you do? You need cash, but don't have it.

S: But the same can happen to credit cards, the same can happen to credit cards

R: Yeah, but with credit cards, [N: passports, and everything is in your...], card for ebay and if it's everything, you just, if you lose your phone, you have, [J: You completely]

S: Yeah, but I think it's like a very slow process of replacing things, but not completely, maybe you stil have your credit card,

R: Yeah, then it's okay, but if I don't have a credit card, it's --.

S: Yeah, but this won't happen from one day, so maybe in ten years, but then other things will appear, so it's like slow process.

H: So you would be more worried that your phone would be stolen than somebody would get information through the internet from your phone

S: Yeah, because I think -- yeah -- yeah

J: Yeah

N: Umm

F: No [laughter]

H: No? What do you think?

F: Yeah, I think, as I pointed out already that this, like -- yeah, I don't have so much things -- I don't do so many things through my phone, that I -- if lose I can, um, deal with it somehow, and, um -- but the whole thing in the internet is much more crazy, it's more -- it's bigger than just losing my phone.

Julia: I think in general, if you think about that, um, ongoing process of creating a, um, superbrain you so much depend on, it's very scary, but people are getting used to it so sloly, no one will care, in I don't know, a couple of years --.

F: But -- sorry --

J: Yeah, I'm done

F: WHen we talked about GPS earlier, I never use that, and I it's wierd like, when I saw friends with it, you walk and you like se the arrow move, you turn at it turns, and I'm like "who's watching me?", and um, yeah -- it's so cool to have a real map out of paper, and because, I think we'e also losing knowledge, what you also meant, I think, by having everything digital in our phone, and so it's--.

S: But this happened all centuries, that people didn't lose knowledge, this is a key process--.

F: But does it mean because it has been like that, that it has to go on like that, or I think --.

S: Yeah, you can still use maps, no one will say don't use paper map

F: Yeah, but I --.

S: So they just exist, the roads are build, but, maybe someday people won't produce new maps, or books [laughter]

N: Like, it's this thing again, this app makes it easier, right, not necessarily, because it's just as easy paying with your credit card, probably takes the same amount of time, however, if this app manages to like, um, collapse all your reward points, you know, you don't have to have six coffee cards from six different companies anymore, you know, so it will make it easier, it will make it rewarding, so people will start using it, more and more, I guess, if it becomes rewarding enough. However, I think that's a bad thing!

H: Okay? Why is that?

N: Because you get incentivized, um, things that you normally wouldn't do, you get incentivized to do them, and more and more so. And I don't think that, that's a nice development.

H: Because, even if the process is that we get more and more used to it, so we do it, does that mean that we don't have any threats anymore? Because um, privacy is, about protecting information. You want to protect your information, say your address, you don't everybody about your address. Does the fact that we get more and more used to giving our information

to these things, does it mean that nothing can happen to us? Or nobody could get our information, or? Did you understand the question?

[Umm]

N: Yeah, to me again, like I said in the beginning, all this information, that I might give out, is, maybe I'm too careless with this, but it doesn't seem that important, like who -- so, so what if I give my bank account to Amazon, there's 150kr in my bank account, you know, but then again, that's how I think now. I can't say how I would think if I have to lose something, if I have to like -- family in the background or stuff like that I might think very differently. But right now, all the information that I could potentially give, in this sense, and that's like excluding, like pictures and stuff like that, where I'm like kind of careful, just doesn't seem that important. So I'm willing to to kind of just throw it out there, I guess.

J: I think as long as the convenience is caused by such apps or whatever are bigger than the fears of people getting your information, this system will work.

H: Yeah, so would you -- because we pay for these apps that are usually free, we pay with our information, obviously [S: Yeah], companies use our information to sell their products, and would you consider paying a small amount of money to use all your apps in stead of giving out your information [J: yeah], you would just give your first name or something, and then you would pay, I don't know how much you would pay a month or, would you be willing to do that, to make sure your information wasn't spread?

J: Yeah, I think so, if it was a small amount.

N: Yeah, exactly, it depends on the amount.

H: How small of an amount? Would you pay 50 NOK in a month?

J: 50? For one app?

S: I wouldn't pay anything to Facebook. Because, I don't -- for me it's fine, because I don't post much on Facebook, and they can use what they have, they can sell it, if they make any revenue it's fine [Julia: laughing, if it makes them happy]. But I wouldn't pay them any dollar, because they make --.

H: Because, they're Facebook, because they are --.

S: For example if there's like a newspaper, trying to make some money from the app, or their online e-paper. I would say because journalists and writes need to -- their support. But Facebook don't need my -- doesn't my support.

N: But it's the same thing that if you start paying the companies to not use your information, you're kind of accepting that, like the idea that before you were paying, they were doing bad things with your information, and if that's the case, then like, the entire system is going very very in a wrong way [S: Yeah, and also --.] And then it has to like be regulated on a law kind of level

S: Then there's a two-class society of the people who can afford to pay and those who can't

afford paying, and I don't think this is not the idea of the Internet.

N: Yeah, I think it should be regulated in like, with laws and stuff, [S : Yeah, like political --.] we don't have to pay in order to get your information secured. But then again, how would you, because you have to give the information anyways, right, otherwise the apps don't work [S: Yeah! You have to --.]

S: You have to have a bank account, otherwise you can't pay [laughing]

J:Yeah!

H: Yeah, it's a good point

R: Yeah but I mean if someone says, you still have to trust them, but if someone says "you have to pay me for this app", so we can provide it, and -- because if someone say -- um, takes it for free, then it's obvious that he has to make something with your information, because he'd still have to have a server, and he has to have staff that regulates -- um -- that provides the app and if someone takes money for it, "yes, we just take this money and don't use the information". It's still different I think.

N: Depending on the app, if they don't need information in order to get the app working, fair enough, but an app like Amazon [R:Yes, of course!], they need your information --.

R: Yeah, but, if they say "we need money for the app", [N:okay], maybe, so yes --.

N: Okay, so then you're not concerned about data security, but just about what they do with the data, [R: Yes], okay. Fair enough.

R: Because, yes, they need my data, so I have to give them to them, and if they say "yeah, we don't want to do something else, but we need money because we can't run the company without money.

N: But I don't see it as a data security leak, if some company analyzes my data and sell it to somebody else [R:No, me neither] --.

S: This is the concept --.

N: It's all anonymous, right? [Looking at H] You're the expert.

H: I'm not the expert. [Laughter].

N: But like, I mean these data, I think that all the data that's out there, that's maybe not a picture or something, is all randomized, so they'll have an idea about you as a person, but they don't know who you as a person are --.

S: And actually their not interested --.

N: That's how it should be -- that's how it should be at least

S: They're not interested in i you as a person, they're interested in you as a customer, and

there you're anonymous

F: But they will know, okay, I don't know Oslo too well to say that, but in Hamburg, were I'm from, they can follow, this is a rich living area and this is a poor area [demonstrating on the table] and they can -- these things they know -- like they know like your tracks if you pay with a Visa card, if you go with Deutche Bahn, --.

S: It's a different company, it's not Facebook

N: But what's the problem with that?

R: Yeah

N: Like, I don't see that as a security issue

R: Because they have you as customer, 5300, so -- it's just -- you are just a number for them and if they make an advertisement just working for you, and they know were you are, and they know you can afford this, and you can not afford this --.

F: Yeah, but it shouldn't be their, like --.

[Many speaking on top of each other]

N: If there's an actual leakage, if something bad happens becaues of that, that's bad!--.

S: They're responsible for the data, but, um there's not one company collecting all the data, because if Ihave a bank account at Deutche Bank, they don't care if I travel with Deutche Bahn!

J: Yeah, as you said, the companies are interested in just you as a consumer.

S: yeah

J: Right no, but what if that changes? And it could.

S: So, I think, one should also be concerned about what Apple introduced yesterday, the health thing [laughter], because if it started with people who are more fit than others, it get also like, people are fitter they have to pay less for health insurance, or --.

N: Already happens in the states [laughing]

S: Yeah, so, but not in Germany, but it's a starting process, but this maybe also one of the things which is more into your privacy than we have now.

H: Health information?

S:Yeah, because, I don't share any healthinformation yet, but I think it's like a big new thing, also with the thing around your arm [], and people gets, gets, um interested about their body, about random facts that you don't actually need to know because --.

J: It really reminds me of selection

N: On the other hand, Google for example, is able to predict the spreading of influence and all the stuff [J:Really] weeks ahead of any like medical institutions, thus being able to supply vaccines and stuff, way more timely then would be able without this - so, like, there's an upside as well, you know.

S: Yeah, of course

R: I think it's okay, as long as I'm anonymous

F: But that's what you think, but you know --.

R: No, I don't know, that's what I mean, as long as -- I think in the moment it is, I think if it's abused, and if there's some work guy in the company that says "I want to know what RK, how healthy he is" that would be a problem, but if it's just --.

S: But, if, for some point you still need to -- at some point you still need to give up all your privacy, for example at some point you still have to have an insurance, because that if something happens to you, you get money, so if you'e not anymore able to work, you have to give everything from the last five years when you went to the docotor, so, and this is like twenty years ago, so there are, um, some, areas, where you have to give up your privacy, in -- to get something back, so, yeah

H: What if they were able to identify your close relationships, your families, or your boyfriends or girlfriends or, kind of, they could identify you, or, and start, kind of targeting your inner circle, and they could find out that you were interested in this, and you live there, and your family is so and so, maybe this person is also interested in this.

S: Facebook, or who?

H: I don't know who, we are talking about "they" all the time, Big Brother, or

N: That's the thing, I had a girlfriend, and valentines day was around or her birthday, that would even be more messed up, and all of a sudden I'd get like an e-mail like "hey, give your girlfriend a shampoo". I think I would feel a little violated, but then again they're targeting me with like something very specific, directly, and that I think, is kind of the line.

H: Because they know something about your personal relationships?

N: Yeah, I guess. Like if I would get an e-mail then, "hey, send your girlfriend.." -- like wait, who are you?, who's talking to me, how do you know I have a girlfriend, how do you know it's her birthday tomorrow?

H: But that's kind of -- Facebook know's your social status, I don't know about you, but I often get -- um, ads, kind dating places or -- I lived in London for a while, dating places in London, it's kind of, they tracked me -- do you think that's wierd, or is it okay?

J: They do that already, don't they?

H: Yeah, they do that.

J: And Facebook knows it's your girlfriends birthday

N: Exactly, but if they would target me directly -- I guess, an ad on the side is one thing maybe, but if I would get a direct e-mail, that would again be one step --.

R: I always, if it's just a computer program that writes me, that makes an advertise, that's everything okay for me, because, it's just a computer --. [S: Yeah, this is not stalking] I know that the chance that a real person -- and that's a problem for me, so I don't want this, because it is also possible it's a person, but if I would know that it was just a computer program, it would be okay for me

N: But then again, if you respond to that computer program, and say "oh, yeah, actually.." then in the end you would at some point get in contact with a real company with a real person, you know, I guess. It's just little bit, removed as just that point

R. Yes, of course, but I mean, um -- a computer program has information about me and not the person, and if I go then to a company to buy shampoo for my girl friend, then I get in touch with them, but they don't know why, and just know that I'm buy the shampoo, because my girlfriend has a birthday

[S talking on top of R]

S: And if you don't give out information about your girlfriend, if you don't put any relationship, how does the computer program know that this boy your friends with on Facebook is your boyfriend, or is your girlfriend, so the computer program needs information and standardize information, so they don't, because you're writing a lot of people messages, but still they don't know he's your boyfriend, unless you tag them in your "I'm in a relationship", so, it depends. But maybe in someday, these information system computer will get so intelligent that they know everything, [laughter].

J: Concerning what you just said, I think it's just lacking of connection between FAcebook and for example Amazon, because of -- they would corporate, or Facebook would buy Amazon or whatever, um, facebook had the information and Amazon could send you direct e-mails, and I think we're not that far from --.

N: At that point I would say, I would like -- "okay, guys, this is not okay, you know"

J: Yeah, that would be the line

S: But then you just don't put your girlfriend as "I'm in a relationship with.. " on Facebook and it's done

H: So Facebook, or the Norwegian newspaper recently wrote about that Facebook knows what you're doing when you're not online, so there's was this guy at BI, he wrote about that when you shop at any physical shop, Facebook can actually get that information about you when you do a card transaction or anything. I don't know the details [N wispering: they probably can, yeah], but would think about that, would you draw the line there

S: That's maybe why Germans like to pay in cash, because if you pay in cash, no body knows.

N: But that, that, that doesn't feel like -- that's nothing, Visa also knows and probably through like very many networks, somehow FAcebook finds out, but [sigh] Facbook, that's nothing else really, than me Googling something, then FAcebook suggesting me "hey, buy this t-shirt". And if I pay something in the shop, and they'll find out, in the end it's the same thing "hey, why don't you go back to Carlings, one day" I don't feel like that's a big problem again. Me personally

A: Just knowing, knowing --.

S: But maybe it's interesting to know, if you know how it works, you can avoid maybe

F: But isn't also -- or what I fear, is that there are many people who are not sitting in a discussion like we do know, and who don't like have these forts, maybe if they would know they also would try to avoid that their security lacks or that the data is being sold or whatever, and yet, I think the majority of people in Germany and also in Norway is not aware of it, and that is I think the power of these companies, because, um, yeah, it's so easy for them to get access to the data and make their marketing strategy with and they -- yeah -- get richer and --.

S: So you can do a help organization, "How to behave yourself on Facebook". But people don't know a lot of things so..

H: Do you -- have you thought about that there's differences between Norway and Germany in theses things before?

S: Yes, so what I know so far is that in Scandinavia in general, heatlh data is more open to, like, for example unis or researcher, so like unis can do better research on some conditions, because they have all this data connected, and in Germany if I go to one hospital one day, an another next day, they wouldn't know about it. And here, I guess it's more open, and that is why a lot of medical studies came from Scandinavia

J: And there are not even doctors at Germany uni

R: I think, what I also heard is that you also can see the salary of every person, as long as know the ID number, or what is?--.

[F: "Wow"]

J: Yeah, for --.

H: As long as you know the name

[Laughter]

R: Yes, that wouldn't be able in Germany

H: Would that be uncomfortable?

[All: Yes]

S: But I think it's good to know, because, then you have something to talk about, "why is this person gaining more?" No, and you can start argue for your self "I'm doing the same work, why is he earning more?" And, um, I think, in some way, this open society is also useful in -- and even if it has, you have to give up your privacy

A: Yeah, we discussed about in, um, Norwegian [class], and um, “debattklubb”, and I think it's hard to imagine for Germans, but I know it from Norway, and I think it's, yeah, it's a bit, it's difficult, because you can't, um, compare Norway with Germany, it's, umm, -- in Norway, there are so, um, less, people who live here, and, um, it's more like a big family, and yeah it is, and we talked about the advantages and disadvantage, and yeah, maybe it's, you can be very jealous, but, um, I don't I think it's difficult, and, um, the Norwegian look to other countries, and see "oh, it's not the same in German, and hm, maybe we should change this, and" yeah, they start to think about, and, um, to know, it can be different, and yeah, and we look to Norway and to Scandinavia, and think "what? no it's impossible" and yeah..

H: Hmm. We are nearly finished --.

F: I just, one small thing, what I forgot to say earlier on that, I pay actually, for my e.mail account, because I have an alternative one and it's called -- now I'm doing advertising, now I'm the marketing expert -- [laughter] It's called posteo.de and, um, it is safe. They don't sell your data, they block all spams,

J: Do you, do you save your mails?

F: No, I don't remember quite, but they, it's, the safest thing what you can actually get, and they use their energy for they're, servers. They use green energy for that, and, they, um, from the over -- like left money they get -- they support some, um, social project. And you pay every month, one euro, so that's 12 euro for year. And if you're interested in it, I

[laughter]

Frieda: Yeah, it's an alternative to, um, Gmail

H: That is interesting, I will definitely look it up for my assignment.

S: Yeah, maybe you can post the link...

Frieda: Yeah, I can, post the link

H: Pizza is coming in ten minutes. Um, have you ever decided, I you know you have, Frieda, not download an app or visit a website because you were afraid of your -- what they would do with your information?

N: Just visit a website, or like sign up for something?

H: Visiting, sign up, or let's say, have you ever not done anything online because you were afraid of what they would do with your information?

[All saying yes]

J: Streaming [laughing]

N: Yeah, mostly illegal stuff [laughing] Oh no! [looking at the audio recording]

H: I will report this right away [laughing]

N: Just kidding! [Saying into the audiorecorder]

F: Facebook is also listening to us right now [laughter]

N: Through the iPad

H: Telenor is listening through this [tapping at the android]

H: But have you -- other than streaming? Have you for example avoided signing up for, I don't know the english word, for a campaign, you know were they have signature campaign

J: Ah, petitions

H: Petitions, yeah, have you avoided signing up because you don't know what they would do with your information?

[No]

F: This for example I do regularly, to sign up like that

J: Yeah, me too

F: Because then, I also think I stay behind that message, and I trust these people from [..] that are big NGOs

R: What I don't do a lot of times i, ym, some websites, you ahve to get in, or not alot, but sometimes you have to get in with your Facebook account

J: Because everyone can see what you do on those websites

H: Do you press "like", when you know, if you go, up to another site on Facebook, and you have to "like" to get into the site

N: No! I hate that!

R: I think Ilike the --. Five times in my life

N: Sneaky people

S: And also, I don't use the like button if there's a news article -- you can like it -- I never use it, because, this is a way Facebook can track you to other websites, and if you don't use it, you're probably safer then

R: So, what's the problem for me for example, is that a lot of websites have this like button, and if it would be a website, I don't want others to know, and I just misclick and then, yeah, everybody knows I'm on this website, and I don't want them to know this

S: But so many people are not aware of the fact that everyone can see that.

N: Hm.

H: Any closing remarks?

F: For you, maybe interesting, you know about that theory, actor network theory, yeah, yeah I know, because that is quite what we talked about

H: I will check that out.

Appendix 3: Interview 2, Norwegian group

Research interview 2/2
Conducted September 22, 2014, at the University of Oslo, Institute for Media and Communication.

Interviewer: Hanna Kaupang
Respondents: Six Norwegian students
Time: One hour, fifteen minutes
Place: Group room at the Insitute for Media and Communication

Codes in use

--	As if they change their minds about what they are to say
--.	Interrupted by somebody else
…	Pause, thinking
(…)	Something missed on the recording
umm hmm	Agreeing
hmm	Not agreeing/uncertain

This transcript has gone through minor editing to ensure that it is understandable to readers that were not present in the interview. I have let as much of the originial statements, pauses and hesitations, to convey the actual interview as well as possible. Words that were not uttered by the respondents in the interview, but was added to the transcript clarify are put in [brackets].

H: Det er mange forskjellige meniger om personvern, hva det er og hvordan vi skal behandle det. Derfor er mitt første spørsmål; "hva slags informasjon om deg selv anser du som privat, eller personlig? Hvor går grensa for hva du er villig til å gi ut av informasjon?"

T: Det spørs hva jeg gir det til da, det vil jeg si er det første, hva jeg gir det til

[Gruppen er enige]

H: Så for eksempel til et nettsted, eller en applikasjon, eller..

T: Hmm, jeg er litt sånn -- altså en ting er jo navnet mitt, og ofte er det jo med [i] en e-mailkonto, og mitt navn er ikke i e-mailkontoen min, så det går greit da, men sånn som kjønn, alder og adresse anser jeg som veldig privat. Men sånn som kjønn, det er okay -- ikke så, det går greit å oppgi, men så fort dem skal ha alder og adresse, så vil ikke jeg

F: Adresse -- jeg støtter den, adresse er litt privat, jeg er med den

T: Og da trenger jeg ikke applikasjonen

[Latter]

I: Jeg tenker litt sånn at med en gang, hvis du må skrive ned hele navnet ditt, så får du jo tilgang på alt med en gang på en måte, så jeg synes å gi hele navnet til noe er også litt privat synes jeg, og etternavn. Da synes jeg det er bedre å bare gi e-postadressen, som jeg kun har fornavn i og eventuelt bare et sånt brukernavn eller noe, hvis det er en applikasjon da.

M: Jeg tenker det er litt for lett å søke meg opp uansett, så der er nærmest grensa ved personnummer. Hvis du virkelig vil finne navnet mitt, så klarer du det jo -- hvis du virkelig vil finne adressa mi, [kremt], det tar deg kanskje et minutt med søking å finne fult navn og adresse og alt det der, det finner du hvis du vil, så det plager meg ikke så mye å måtte oppgi fullt navn fordi at -- ja, um, kanskje den mailen jeg faktisk bruker er litt privat, fordi jeg ikke vil ha spam.

T: Ja, det var interessant, etter at jeg ble 20 fikk jeg spammail. Du fikk det når du var 18 da! [Ser på A ved siden av seg].

A: Ja

T: Neimen, jeg synes det er interessant, jeg har ikke fått det før da, altså det var liksom når jeg blei 20, altså i dette året her da, så fikk jeg spammail. Så det betyr at informasjonen min har blitt gitt videre til et sted. Sålenge det er mailen, så går det greit, for jeg kan alltid sjekke mailen min, men det er litt sånn skummelt da, fordi dem selger jo -- altså store firmaer -- selger jo opplysningene dine videre, og du vet jo egentlig ikke hvem som faktisk har opplysningene dine. [M: Hvis dem vil.]

A: Det var litt morsomt at Facebook drev med ulovlig forskning på Facebook, sånn de ikke hadde fått godkjent, men [latter]. Men bortsett fra det så synes jeg det er enklere for meg -- så er det nesten greit å oppgi informasjonen min hvor som helst. Altså jeg skjønner veldig godt hvorfor folk ikke synes-- har lyst til det, men, um, informasjonen din blir jo brukt til videre forskning på et eller annet--.

M: Men du må jo ha en eller annen grense, jeg tror ikke du ville oppgi personnummeret ditt, håper jeg ihvertfall

A: Nei, altså, bankkonto og alt sånt, det er jeg litt sånn skeptisk til--.

T: Men tenk på hvor mange som skal ha bankkontonummer og sånn da..

A: Ja..

M: Bankkontonummer er jo greit

T: Sånn som på applikasjoner og sånn, sånn som på Google Play, der vil dem jo gjerne at du oppgir et eller annet kontonummer, jeg har ikke gjort det, så jeg er ikke sikker. Sånn at hvis du skal betale i fremtiden, så har de nummeret ditt. Og alle de tingene de lagrer inn, sånn at det skal være enklere å gjøre ting.

H: Det er ubehagelig?

T: Ja! Altså, jeg vil ikke oppgi noen, før jeg faktisk må oppgi det

F: De fem siste i personnummeret er sånn -- det! -- da er jeg skeptisk, da stiller jeg meg kritisk

T: Men altså, hvor mye skade kan du gjøre uten personnummeret? Du kan jo gjøre like mye skade uten personnummeret ditt

F: Men det er sant det, jeg føler det er sånn gammeldags tankegang, foreldrene (...) bare, nei det skal du ikke si bort, men jeg vet ikke jeg...

T: Nei, men du skal fortsatt ikke si det bort --.

M: Så lenge man har to-trinns [passord] på det aller meste man faktisk bryr seg om, så er det -- jeg tenker at det får være mitt sikkerhetsnett, og så får jeg oppgi alt det andre nesten, og satse på at det holder, for du kan finne det hvis du vil, det tar deg et halvt minutt --.

I: Det er akkurat det jeg mener, jeg også, at, um, folk finn-- hvis folk vil finne ut av ting, så finner de det. Det er ikke værre enn det. Hvis du skal være redd for å oppgi noe som helst, så må du ikke si noe som helst --.

[M er enig]

T: Ja, men tilogmed da! Folk kan si ting om deg!

I: Ja, det er sant. Det kommer fram på et vis uansett.

M: Men hvis man har noen som helst verv blir man alltid nødt til å oppgi mail og -- ikkesant --

I: Du kan jo mail, så må du jo si det

M: Ja ikkesant, så er det lett søkbart for alle, så...

T: Ja, var det ikke noe med Google, at du ikke trengte å oppgi fullt navn, for å lage Google-kontoer [M mumler: du kunne skrevet hva du vil der]

H: Men, betyr det da at det ikke er noen ting som er privat lenger? Er alt ute i det åpne --.

T: Hvis det er på noe elektronisk, så er det ikke privat lenger--.

M: Hypotetisk sett, hvis det er noe som er privat, og jeg sier det her, så er det ikke privat lenger, så jeg vet ikke helt hva slags svar du forventer å få på dette spørsmålet, sorry! [latter]

H: Det er sant

T: Men hvis det går som privat, som at hele verden kan gå inn på, så vil jeg si at alt som er elektronisk er i prinsippet ikke privat lenger

H: Er det sånn det skal være da, er det greit?

F: Det er vel litt med tiden vi lever i nå, tenker jeg at, at det er en del av informasjonsverden

og en del av samfunnsendringene, at det har blitt sånn rett og slett. Alt er tilgjengelig, 24/7.

A: Men vi er jo også mye mer opptatt av privatliv her i vesten enn i for eksempel i Asia da. Og de klarer seg jo helt fint uten et så sterkt privatliv, hvis vi skal si det sånn. For eksempel i Sør-Korea, så er det veldig vanlig å oppgi all sånn der, um, sånn informasjon fra legen og sånn til nære venner [latter], så de vet liksom hva som feiler deg.

M: Nå får vi endelig digitalisert vår egen journal ganske snart, skikkelig, og det må ærlig innrømme å si at det ser jeg frem til.

I: For det var noe av det jeg også skulle si, at det eneste som på en måte, som er ordentlig privat i dag, er jo legejournalen vår, det er jo privat og det vil jeg holde privat --.

T: Hvilken som helst lege kan jo gå å se på den--.

I: Ja, men leger kan se det, men det er jo ikke noe som kommer ut--.

M: Men, det som en, og uansett nå så vil det bli logga hvis dem ser på den, du vil også kunne se, og hvis du begynner å se masse leger som ikke har noe med deg å gjøre, så vil du kunne se det når vi får digitalisert ting. Det kunne du ikke før, før så kunne faktisk hvem som helst lege finne papirene, jaja, så leste man dem bare, men nå vil det bli loggført.

I: [Snakker delvis i munnen på M] da leste man dem jo bare. Og det er jo liksom det første jeg tenker på når du stilte det spørsmålet om "hva er det jeg vil holde privat" og da er det den legejournalen. Det er ikke nødvendigvis alt som jeg ikke vil dele, men det er liksom, det er mitt, det skal ingen se. [T prøver å si noe].

F: Det er jeg ganske enig i--.

T: Du har ikke noe med det!

I: Du har ingenting med det!

T: Det er sånn som når folk spør deg om ting, altså, du har egentlig ikke noe med det du spør om. Jeg er ikke pålagt å fortelle deg det.

A: Og det er akkurat den tankegangen som er forskjellig rundt omkring i verden [latter]

M: Hmm, men gitt at en vei, det er fortsatt en veldig hjelpsomt, det gjør ikke noe forskjell

T: Det går jo på å respektere hverandre, å respektere enkeltinvidet--.

I: Hvis du går å leser den journalen er det kun for nysgjerrigheten, du får ingenting ut av det, det er bare fordi du er nysgjerrig. Men sånn, ja.. så det er vel det jeg synes er privat, så langt

[Latter]

H: Hva med sånne ting som hvor du står politisk, eller om du er religiøs, eller om du -- er det informasjon som er greit for alle å vite

T: Ja .. men først --.

A: Sånn kan jo bli brukt mot deg, på en eller annen måte

T: Alt kan brukes mot deg--.

A: Alt kan brukes mot deg, men særlig det å -- særlig hvis du har makt, er det veldig viktig hvor du står politisk og sånt

M: Men jeg har jo politiske verv, så det er ganske tydelig hvor jeg står, et Google søk, så kommer det opp som nummer to eller noe sånt. Så jeg har ikke dem helt store problemene, men så lenge det er noe sånt man oppgir selv, altså, jeg er ikke veldig keen på at folk skal kunne grave og finne fram til mitt politiske ståsted, gjennom at vi for eksempel hadde åpne, hva man stemte på, det er jeg skeptisk til --.

I: Ja, det er jeg enig i.

M: Men jeg har gitt ut ganske tydlig hvor jeg står politisk, så lenge det er opp til meg, så ser jeg det ikke som et stort problem

H: Men det hadde ikke vært greit at de dere stemte på ved valg, ville være offentlig

[Alle er enige om at det ikke er greit]

F: Det synes jeg skal være privat

M: Tilogmed med medlemslisten til partiene helt lukka, så det betyr at du kan være medlem i alle partier, samtidig, hvis du vil [latter]. Det verste er at du kan ikke kaste noen ut, jeg vet det fordi vi har vært i en sånn situasjon, fordi at, ja, neimen, fordi at hvis du prøver å gå å få dem kasta ut, pågrunn av det, så kan dem si at, "det her vet dere ikke noe om, dere har brutt personvernet, hvis dere vet noe om dette" [I: de kan bruke det mot deg.] [Latter]. Poenget er at alle kan -- på møter til andre partier, så kan dem si "neimen jeg står ikke på den lista".

I: Er det ikke lov å være medlem av flere partier?

T: Det er kanskje ikke --.

M: Miljøpartiet har lov, men --.

T: Det kanskje ikke -- kan hende at dem ikke liker det --.

I: Nei, selvfølgelig ikke--.

M: Mange partier har faktisk regler mot det, men vi innså at det går ikke an, fordi at du vil aldri kunne bruke de reglene --.

T: Men sånn politikk og religion, jeg har sånn prinsippsak da --nå mener jeg politikk, ikke politi, jeg har en sånn prinsippsak da, at hvis du har noe å si, så skal du si det med ansiktet ditt fremme, og derfor irriterer det meg når folk skjuler ansiktet sitt og er så påståelig og sier ting, hvis du har noe å si om et politisk parti, så skal du si det, men du skal også signere

navnet ditt [M mumler: jeg er uenig, men okay]. Hvis jeg da stemmer på et parti, jeg stemmer rødt for eksempel, eller jeg stemmer Høyre og jeg skal ut å si det, så mener jeg at jeg som en prinsippsak skal stå for det med mitt eget navn, for det er noe jeg tror på og det er samme med religion. Hvis du tror på noe, så skal du stå, bak det. Og jeg er religiøs, jeg er katolikk, og jeg har ikke noen problemer med det, men det er mange som har problemer med det.

I: Det er et sårt punkt for mange

T: Ja, for altså, hva er det vi er i Norge, "personlige kristne"? Jeg skjønte ikke hva det var først jeg. Men altså, jeg er sånn at hvis du skal snakke om det, og du skal si hva du skal stå for, så får du stå for det altså.

H: Så det er greit å ha sånn informasjon på nett--.

M: Sålenge det er frivillig--.

T: Hvis du velger det -- altså hvis du først sier det, så må du også stå for det altså

F: Ja,

M: Jeg er skeptisk til det altså, jeg liker ikke anonyme drittsekker jeg heller, men det er jo en sikkerhetsventil, altså, hvis alternativet er at de ikke sier noe som helst, så kan dem jo få være anonyme.

I: Jeg tenker jo litt at hvis du står for noe, så står du for noe på en måte, hvorfor skal ikke folk få vite hva du står for? [M protesterer]. Men igjen så synes jeg at det er ditt eget valg om du vil dele det eller ikke [T: Yes!] --.

M: Men hvis du har sterke meninger, som er for eksempel i en familie som er sterkt skeptisk til-- eller du har en vennegjeng som er virkelig skeptisk, la oss si at du stemmer rødt, men du henger bare med FpU-folk, vil du da sagt det-- tror du det da at du ville uttalt det like fritt, hvis du måtte stå frem med fullt navn?

I: .. Ja, hvis jeg står for noe, ja...

M: Altså, det er lett å si det, av prinsipp, men hvis du risikerer å miste ditt sosiale liv, hvis du risikerer å bli utstøtt fra familien og sånne ting--.

I: Men det ser vi jo i hele verden

M: Så--.

T: Men hva om det er det som skal til, for jeg har mange ganger stått ut om det jeg mener, og jeg vet at de som da står igjen til slutt er mine venner, men ja, fordi jeg har aldri hatt et problem, for jeg har aldri brydd meg

M: Men ja, det er fint for deg at du har det sånn, men alle har ikke den--altså, det vil i praksis bety at folk det blir å holde mer kjeft--.

I: Men jeg vet at det er ikke sånn det er, det er noen som står fram og noen som ikke står

fram, og det er fordi de ikke tør, fordi de er redd for å bli utstøtt--.

T: Ikkesant, å hva er galt med den tankegangen der, ikkesant, sånn som samfunnet å si da, vi lærer--.

M: Jeg synes dem fortsatt skal ha mulighet til å uttale seg selv om dem ikke tør å stå for-- altså, hvis du har noe imot anonyme drittsekker så gjør man jo det, men la folk uttale seg selv om man er i en situasjon der det ikke er helt enkelt.

[I er enig]

T: Men det er jo det som er så fint at når vi stemmer, så blir det jo ikke oppgitt hva vi stemmer på, for da får vi jo tilslutt mulighet til å uttrykke oss uavhengig, hvis du er for eksempel i Høyre også stemmer du på rødt, ingen i Høyre finner ut at du stemte rødt, men da gjorde du det.

M: Det er jo en veldig begrensa påvirkningsmulighet, egentlig.

H: Det vil jo si at vi må ha noen form for privatliv, hvis vi skal kunne oppholde det at vi, at det skla være mulig å snakke anonymt, at man skal få lov til å si menigngene sine selv, selvom man ikke tør å vise hvem man er.

A: Det er -- jeg tror det ikke handler bare om det, fordi ny forskning hviser veldig tydelig at å lyve er veldig bra for samfunnet sin helthet, det styrker følelsen du har med andre personer, selvom de lyver om deg, til deg, selvom de baksnakker deg, tilogmed baksnakking hjelper å fremme en, et godt samfunn hvor alle sammen fungerer og det er egentlig veldig morsomt.

[Latter]

M: Jeg er litt nysgjerrig på hvordan dem satt opp den undersøkelsen, men det får vi ta etter at det her er over, for det ser ikke helt hvordan det forskningsprosjektet kan settes opp--.

H: Men vi kan snakke om det etterpå. Vi har snakket om informasjon som går veldig på det generelle. Er det noen informasjon som du bare finner på nett om deg selv, som du ikke er komfortabel med at hvem som helst vet om. Det er jo for eksempel en-- når vi er på nett er det for eksempel en IP-adresse som folk kan spore tilbake til oss, når vi bruker stedstjenester på telefonene våres og, så kan vi finnes et eller annet sted, folk kan se hvor vi har vært. Er det greit, at alle kan se og benytte seg av?

A: Nei, det synes jeg ikke. [Smiler]

M: Hadde jeg (...) så sikkert, men--.

F: Nei, vet du hva, det jeg gjør på internett føler jeg at andre kan se, så jeg føler ikke at det er noe problem i seg selv.

A: Det er jo også litt irriterende når jeg vil lese en side på engelsk, også kommer det alltid på norsk.

M: Det er ganske lett å unngå det, men okey..

A: Det er ganske lett, men det er fortsatt sånn irriterende. Så det ville vært bedre, ihvertfall for meg, hvis alt sammen var nøytralt.

M: Nå snakker du om sånne tekniniske ting, altså sånn type (...) og den slags, eller?

H: Ja, det er jo mye-- vi legger jo fra oss mye informasjon på nett, mye ting som -- som kan spores tilbake til oss, som kan identifisere oss, for eksempel at Netflix kan--hvis du har sett på en del serier, så kan Netflix etterhvert finne ut mønsteret ditt, også anbefaler deg og det er jo en del av at de finner ut hva du liker og--.

T: Men da sporer dem deg ikke, da ser dem på hva du har sett på--.

I: Men det er jo samme på Facebook, reklamen på Facebook er jo reklamen av ting jeg har vært å søkt på--.

M: Nei, virkelig ikke--. [Sukker].

I: Det er jo ofte det jo--.

T: Nei, ikke alltid.

I: Masse reklame som kommer opp der--.

T: Det er sånn som når jeg får "date single jenter" på profilen min står det faktisk det (...) jeg liksom "okay, hvor får du dette her fra" [latter] Ellers på voksne menn altså, "det er det dere tror nordmenn driver med, jaja"

M: Nei, altså jeg føler meg aldri så--jeg føler aldri at personvernet mitt er så god ivaretatt som når jeg er på Facebook og får så mange reklamer som ikke har noe med det jeg er interessert i å gjøre --. [Latter]

T: Kanskje det er sånn skalkeskjul, de har masse informasjon om deg, men så sender de deg feil reklame for da tror du at ikke (...)

A: Mens de egentlig forsker på deg og sjekker hvordan du reagerer--.

T: Ja det var hvordan de gjorde--.

M: Jeg bannes mye, men okay

H: Hva tenker du om det, A?

A: Um, jeg tenker det at det er unødvendig å logge hva man--hvilke sider man er inne på, hva man på en måte skriver ned og sånt, for det at man vet liksom ikke hvem som får tilgang til det og hvordan det benyttes, hadde man visst det så hadde det vært noe helt annet. Jeg er ikke generelt sett redd for å gi fra meg personopplysninger egentlig, men det er bare hvordan det brukes og hvordan det kan evt. misbrukes senere, når slettes det for eksempel? Slettes det noen gang?--.

T: Men skal det ikke slettes etter et år?

A: Nja, sånn forskjellige nettsider og nettlesere har forskjellig lengde på hvor lenge de bevarer informasjon--.

A: Det burde kanskje standardisereres, eller--være noen lover mot, maks antall tid og innsyn i hva de har spart på, for eksempel

A: Noen har sånn makser på bare noen uker, men jeg tror det var-- Internet Explorere hadde på sånn opp til to år hvor de lagrer informasjonen din. Det er litt sånn veldig stor kontrast på forskjellige nett--nettlesere--.

T: Ja, men da har du jo ikke så mye med hva jeg søker på, da er det mer det at det private--privatlivet er veldig sånn, du har ikke noe med det hva jeg søker på. Altså, hvorfor skal du vite det?

I: Jeg tenker og, i hvilken sammenheng er det nyttig, at noen vet hva jeg har søkt på. Altså hvorfor? Jeg vet for lite om det til å vite hvem er det som bruker den informasjonen, hva blir det brukt til?

T: Vil du at sånn veldig klar da, at politiet kan jo gå inn--.

I: Ja, det er det eneste jeg tenker på, at hvis det har skjedd noe da, så er det kanskje greit for politiet å kunne gå inn å se, men det er den eneste grunnen til at jeg tenker at--.

T: Nei! For jeg-- ja ikkesant--.

I: Eller så skjønner jeg ikke hvem--.

A: En ren sånn reklame for Facebook er jo for at du skal kunne bruke mere penger da, ikkesant, så det er en måte, men det er også for å sjekke hvordan verdenssamfunnet oppfører seg, hvordan det vil gå i fremtiden, se for eksempel aksjer, eller hvordan aksjer vil forandre seg, det kan du se på Facebook. Det er jo den informasjonen, så alt er nesten pengespørsmål.

T: Du mener å spare på det og? Nå skjønte jeg ikke hva du mente.

A: Hvordan? Nei, altså, de tar informasjonen din, også finner de ut hva du bruker penger på også viser de deg flere ting, sånn at du bruker enda mer penger.

T: Åja, ja, ja, yes, da, ja. Sånn som på eBay og sånt, "hva har du kjøpt? Da skal vi gi deg mere tips til hva du antageligvis kjøper"

M: [Mumler] Det plager egentlig ikke meg allverdens.

H: Men, når dere--kan man si-- ferdes på internett da, når dere bruker nettsider og applikasjoner, tenker dere noe på hvordan dere beskytter informasjonen deres, eller har dere--er dere bevisste på det, når dere er på nett, at dere skal beskytte informasjonen, eller?

M: Ja, men det er noe, det er veldig lite, men det er noe jeg beskytter helt, men igjen, det er privat, så det sier jeg ikke her [latter].

H: Hva gjør du for å beskytte informasjonen din?

M: Hva jeg gjør? For det første så bruker jeg en PC som jeg ikke bruker til torrents for å unngå alt [latter] neida, eh, utover det, jeg gjør ikke noe mer enn å bruke proxy server [en maskin som fungerer som et mellomledd mellom webleser og internett. Fungerer som en sikkerhet.] det gjør jeg ikke, men, det er det jeg gjør. Det kan være mulig å finne ut av det, men det skal ikke være lett--altså, det gjør meg ingenting om politiet kan finne ut av det, men hvis du vil finne ut av det så må du gidde å gjøre en innsats, men det gidder du ikke hvis du er ute etter å tjene penger, for dem aller fleste gjør det ikke, så da går de etter dem i stedenfor, så det er rett og slett, ja, sikker nok, ikke så sikkert som jeg kan gjøre det, men sikkert nok.

I: Jeg gjør ikke så veldig mye [smiler]. Jeg vet for lite om det. Det eneste jeg ikke gjør er å registrere meg på ting--.

T: Ikkesant, det er så vanskelig, ja for du vet egentlig ikke hvordan det virker--.

I: Nei, jeg vet ikke hvordan jeg skal beskytte meg, så jeg bare gjør ingenting

T: Nei, ikkesant, i starten, så det jeg gjør er at jeg får hjelp av noen som kan [peker på A] og så får jeg en veldig enkel forklaring, også skjønner jeg det litt, også vet jeg at jeg ihvertfall er forsvart mot det, og ikke mot det.

F: Jeg skrur av og på Java, når jeg har vært på nettbanken og ikke, men det er fordi jeg har fått beskjed av en venninne. Men ellers så gjør ikke jeg noe spesielt heller.

T: Ja, hva da med nettbanken, hvor trygt er det?

A: Ja, ikkesant, det er litt det som er poenget at de må oppdatere Java hele tiden for hvis ikke du gjør det så er de gamle versjonene alt for sårbare, altfor lett å komme seg igjennom.

T: Ja, du snakket om hvor mye du lar folk se, ikkesant? [Ser på H]. Gammel versjon av Java? (...) på nettbanken

A: Jamen bortsett fra det, så gjør ikke jeg noe særlig egentlig, selv. Jeg vet om forskjellige ting jeg kan gjøre, men det er ikke hvertfall for meg, stor vits, informasjonen kan de sikkert bruke til et eller annet, men, hvem har lyst til.

M: Altså, i den grad det kan brukes, så blir det stor aggregerte data, og da er det i verste fall, hvis vi går på personnivå, så går det på typ reklame og det lever jeg helt fint-- [noen prøver å avbryte] jamen altså det lever jeg helt fint med, eller hvis det skal brukes i noe mer hissig, så må det være at dem aggregerer og bruker på større populasjoner og da er det jo ikke direkte retta mot meg lenger, og da bryr jeg meg ikke så [latter] så det er greit.

F: Ja, det er akkurat det jeg tenker også, ikkesant. Det jeg søker på internett, når jeg søker på ulike skoletermer, hvem er det som er interessert av det? Det er liksom.. nei. Jeg har ikke noe imot at alle ser det.

H: Det er et-- det er kanskje ikke et ordtak, men det er noen som sier at hvis du ikke har noe å skjule, så trenger du ikke privatliv heller, at det er mange som mener at hvis du har noe å

skjule, det er da du er en forkjemper for privatliv og personvern, men hvis ikke, så bryr du deg ikke noe om det. Er dere enig i det, eller?

I: På en måte

M: Halvveis

F: Ja, jeg kan si meg enig i det

I: Ja, det er litt det jeg tenker at det er samma det, for jeg har ikke noe å skjule, men igjen så vil jeg jo ikke gi folk nettbankkoden min så de kan gå inn å sjekke det, jeg vil ikke gi de journalen min hos legen, jeg har noe privat, men det er ikke det at jeg nødvendigvis har noe å skjule allikevel. Men med en gang du har mer å skjule, så blir du veldig redd for at folk skal finne ut av det, og da er du mer forsiktig med en gang, tenker jeg.

T: Men sånn som å skjule, det er jo sånn enkelt, "ja, jeg hørte du fikk 2-er i matte i åttende klasse på ungdomsskolen, hva føler du om det?" [latter] "hvordan vet du det?" Det er jo en ting å skjule, fordi du selv føler deg bedre av at ingen vet det.

M: Jeg tenker-- mitt problem med det her er jo at det man har å skjule her, det skjuler jeg også i den her samtalen, så får ikke ta det opp uansett, men ja, jeg har noe å skjule og ja derfor vil jeg ha personvern. Det er ikke noe ulovlig, men jeg har noe å skjule, så --.

T: Jeg synes det er sunt jeg, å ha noe du ikke deler med andre, det er ikke nødvendigvis å skjule det, at ingen skal finne ut av det--.

M: Jo! Det er at ingen skal finne ut av det [latter]

T: Altså, du har noe som er eget, sånn at du vet at dette har ingen andre noe med. Ikkesant, så det er jo det tankene dine er. [M mumler: nei, det er ikke det tankene mine er, men okay].

I: Jeg tenker jo bare sånn i forhold til alle bloggerne og alle de også deler livet sitt, og det er ikke nødvendigvis at jeg skjuler at jeg-- det er ikke det at jeg vil skjule at jeg går å trener, å skjule at jeg spiser sunt av og til, men jeg har lyst til å ha noe av det livet mitt privat da. Jeg har ikke lyst til å dele det med hele verden liksom og det igjen er ikke fordi jeg vil skjule noe, men det er at jeg ikke vil dele noe av det.

M: Men vil du da at noen ikke skulle kunne aktivt søke opp.

I: Jeg tror ikke at noen-- ingen trenger å søke opp hva jeg gjør.

M: Neimen, altså, ingen trenger, men vil du at det skal være mulig eller umulig--for en ting er hva du ikke velger å legge ut selv, men en annen ting er hva som skla være mulig å finne for dem aktivt som leter.

I: Hvis du aktivt har lyst til å finne ut noe om meg og mitt hverdagsliv, så har ikke jeg noe imot det--.

M: Nei, for da blir det litt sånn at personvern ikke betyr så mye på en måte, for jeg sier ikke at det skal være sånn--personvern handler ofte om regler for å forhindre--.

I: Men det er jo en grunn til at jeg ikke legger det ut--.

M: Jojo, det er greit, men

T: Men når folk begynner å spørre deg ut, så begynner du å lure hvorfor spør du meg ut?

I: Ja, det er sant.

H: Men handler det du sier der, om privatlivets fred, eller--skjønner du hva jeg mener da?

I: Ja ja

H: At du vil ha noe i fred, noe for deg selv, eller--.

I: Noe som er mitt og mine nærmeste sitt liksom, det er jo det. Åikke måtte hele tiden være på passelig med hva jeg--hva folk tenker og hva folk mener om det du gjør. Åfå kommentarer og liksom tilbakemeldinger og-- folk trenger jo ikke å liksom ha noe å si på alt det du gjør.

T: Det er akkurat det, det er bare noen ganger når du er -- interact, altså at du har med andre folk å gjøre, da er du liksom, da er du pålagt å forklare deg, men til vanlig så er du jo ikke det.

I: Og som du sier, M, at hvis noen spør meg om noe, så kan jeg fint svare på det

M: Men spørsmålet om personvern er ofte lovgivning og sånt, fordi at det vil ikke nødvendigvis være et problem at det er mulig for folk å finne ut ting om deg og sånt, for det bryr du deg egentlig ikke om. Men for meg, så vil det faktisk være et problem, jeg vil ikke at folk skal kunne søke det opp, jeg ville ikke at folk skal kunne finne ut av det punktum. Så da er jeg litt mer avhengig av at det er noe lovgivning, at det er noe beskyttelse av det.

I: Absolutt

T: Hvordan gjør man det? Hvis du sånn i prinsippet vil at de ikke skal kunne finne noe som helst, hvordan gjør man det i praksis?

M: Altså, jeg vil ikke at noen ikke skal kunne finne hvis de virkelig, det er grenser for hvor mye jeg gidder å gjøre for å forhindre det, men jeg gjør det såpass mye at du skal kunne mer, du skal kunne ganske mye mer over middels over data for å kunne finne ut av det.

T: Jaja, men det er det jeg mener.

M: Du skal aktivt bruke masse tid og ressurser på å finne ut noe spesifikt om meg, og det satser jeg på at folk ikke gidder. Men jeg vil fortsatt ikke at de skal klare å finne ut av det.

T: Ja, og da blir det jo sånn at det legges opp til at hvis du skal finne ut noe om meg, så må du aktivt prøve å gøre det og det kommer til å ta masse tid og da er det liten sannsynlighet for at du gjør det--.

M: Det er ikke alltid, bare noen få ting om meg--.

T: Men poenget er at det er den eneste måten du kan sikre--nå snakker vi om all informasjon på nettet-- det er den måten du kan sikre at ingen finne rut noe, at du må satse på at du gidder ikke.

M: Og det ser ut til å funke ganske bra [latter]. Hvis du må være aktiv hacker for å få det til og du må bruke masse tid og ressurser da gidder du ikke gjøre det på meg.

A: Njao, sånn sett, så er kanskje det--.

M: Den informasjone jeg skal holde skjult, kan du ikke tjene noe på økonomisk heller, så det er litt det.

H: Hvem holder vi informasjonen vår skjult fra da? Hvem--hvorfor beskytter vi informasjonen vår. Nå tenker jeg på nett mest, men --.

T: Jeg vet det glir over i det personlige--.

H: Det er fint, helt greit, jeg er veldig interessert

M: Alle. Fordi at hvis jeg legger det ut på nett, så går jeg utifra at det er tilgjengelig for alle, så enten så skjuler jeg det, eller så skjuler jeg det ikke. Og det er ikke så veldig mye imellom, fordi at så snart jeg har lagt det ut på nett, så -- altså, en hemlighet er en hemlighet så lenge en vet om det. Hvis tre personer-- og det er sånn semioffentligt på nett, da finner alle som gidder det.

H: Mhm. Men hvem, um, er det et, en organisasjon, en enkeltperson, er det myndigheter, hvem er det? Hvis jeg kan bruke ordet -- hvem er det du er redd for skal se informasjonen din, hvem er dette, eller de eller den eller--.

T: Jeg ville sagt--jeg vil ikke at alle skal se min informasjon, helt til noen har løyve til å komme inn å se på det. Igjen, du har ikke noe med det, så det er mer at du ikke har noe med det enn at jeg er redd for det-- "okay da, da har du sett det da, we move on". Men jeg ville sagt at jeg forsvarer det for alle, som ingen kan se, også er det bare noen enkeltpersoner som da kan gå inn å se. Og igjen, da er det det, da vil jeg at de skal ha lov, i følge norsk lov eller noe sånt.

I: Altså jeg skjuler det jo fordi jeg er redd for at de vil misbruke det, og det er vanskelig å si hvem det er, det er jo sannsynligvis enkeltperson, på en måte, men, jeg vil jo ikke tro--det er jo-- men jeg vet hvem jeg skjuler det for--.

M: Altså, sålenge det er sånn privat og ikke noe som man tjene på økonomisk, som er det jeg gidder å holde skjult så er det ironisk praktisk -- i praksis, mine egne, dem jeg faktisk kjenner jeg skjuler det for, for det er dem som vil kunne bruke det, eller dem som vil bli påvirka av det og dem som vil påvirke meg. Så jeg skjuler for dem jeg faktisk kjenner. Merkelig nok, fordi at andre ville ikke ha noe særlig nytte av det. [Latter]. Altså, folk som ikke har noe forhold til meg vil ikke få noe ut av det--.

I: Mm, og for meg er det mer omvendt da. At alle de jeg kjenner kan fint vite det, men de jeg ikke kjenner har ikke noe behov for å vite det fordi jeg vet ikke om de vil misbruke det [Atle:

Helt enig]. Eller evt. hvis du har noen uvenner eller noe, som vil... [Latter].

T: Ja, det var jo den mattekarakteren ikkesant

I: Ja [latter]

H: Har dere opplevd det, at informasjon har blitt misbrukt, på noen som helst måte? Misbrukt er jo, det kommer jo an på deg selv, hva du opplever som misbruk av din informajson. Det kan jo være alt fra at de sender reklame direkte til deg, til at noen stjeler identiteten din på en måte. Det--.

I: Det er vel det det verste jeg har opplevd at jeg får masse spam [latter]. Og det ser jeg jo på som misbruk på en måte, det er jo ingen som--noen ganger så spør de jo om det er greit at de sender informasjon, men hvis de ikke spør om det, altså sagt noe om at de kommer til å gjøre det, så synes jeg at det er misbruk på en måte.

T: Det er jo det.

I: Det er ikke veldig alvorlig.

T: Jamen, dem har jo tatt din informasjon og brukt det for sin egen del uten å spørre deg. Jeg er helt sikker på at det er en eller annen regel på det altså, du må spørre personen først.

M: Jeg har ikke opplevd det selv, men jeg har opplevd at folk som la ut sånn personlig informasjon i seg selv fikk det misbrukt av egne bekjente, folk dem omgås med. Jeg har ikke opplevd det selv, men det er også derfor jeg er litt påpasselig med akkurat--men det var ikke noe alvorlig eller noe sånn super--men det var ubehagelig for den det gjaldt. Altså, det er liksom hvis noen legger ut.. Ja.

A: Jeg leste en artikkel for sånn kanskje et par år siden, om-- det var om sånn forsikringsselskap og sånt, og de, for så mange var liksom redd for at, ja, å legge ut at de skal på ferie før påske eller sommern eller noe sånt, men så sa de det at det er ikke farlig å Facebook, så lenge du på en måte gå heller gjennom lista med venner på Facebook, enn å la være å legge det, så du vet på en måte hvem som får den informasjonen liksom--det var litt sånn, så-- ja, så jeg tenker litt sånn at det kommer veldig an på hvem du gir den til og, for at hvis du på en måte gir informasjon til venner som misbruker det da, så tenker jeg at da er det egentlig ikke venner, eller noen du burde liksom beholde relasjonen til.

M: Men altså, misbruk eller sånn, det høres kjipere ut i mitt--okay, det jeg mente var mer sånn type ting da du skikkelig dret deg ut og får høre det i all evighet, eller noen som kødda med Facebook-kontoen din og noen som trodde på det, også ingen som aksepterer at det her var en veldig utspekulert Facerape.

T: Dette foregår jo muntlig og, at jeg sier noe, også vrir du ordene mine og plutselig er foreleseren sur på meg for en eller annen grunn. Og det er jo også å misbruke det jeg har sagt, ikkesant, det er jo personlig det også.

A: Men det er jo bare sånn ting funker egentlig, for min del ihvertfall har jeg vent meg til at det er sånn, så man bare tenker på hva man sier. Så går det an å formulere seg på mange måter og man kan få fram det samme med mange formuleringer, der en formulering vil være

mye lettere å tilbakevise eller sånn, på et senere tidspunkt, så bare tenke litt gjennom når man sier ting.

H: Vi skal snakke litt om bruk av smarttelefoner. Har alle smarttelefon her?

A: Nei!

H: Alle untatt en? Har du-- er bevisst, eller er det ubevisst holdt jeg på å si--.

A: Um, det spørs litt, en ting det koster penger [latter], en annen ting er at jeg er rett og slett ikke har bruk for å kjøpe ny telefon, min telefon fungerer fortsatt kjempefint, det var sånn at den forrige jeg hadde, da plutselig ble det noe med skjermen, så da fikk jeg fikk jeg den gamle telefonen til moren hennes [peker på T], men den funker jo fint fortsatt den [T:Så hva har du behov for?] Det jeg har behov for er å sende meldinger og å ringe, ikkesant. Og jeg sender melding mye raskere med den her og en smarttelefon og den er også mindre, okay den er stortsett større enn den forrige jeg hadde, men den er fortsatt mindre enn en smarttelefon. Så da har absolutt ikke behov for en smarttelefon.

M: Jeg hadde heller ikke før etter jul, men da innså jeg at politikk og mangel på smarttelefon er en forferdelig kombinasjon [A: Okay, det skjønner jeg]. Det har jeg faktisk behov for. Jeg må faktisk kunne sjekke mail og sånt under en samtale, jeg risikerer at det skjer, det er dritlite hyggelig å gjøre, men noen ganger så må jeg gjøre.

H: Så du bruker den mange ganger daglig?

M: Jeg bruker den mest hvis jeg må være på kjedelig fellow [?] møter eller sånt, der jeg vet hva som blir sagt allerede, fordi jeg har forberedt innleg eller noe sånt, så da bruker jeg det for å jobbe, når jeg ellers ikke vil kunne jobbe, egentlig, mest. Og for å kunne kjapt svare, gjøre avstemninger via mail, for å av--bestemme hva Grønn Ungdom skal mene.

H: Hva med dere andre? Bruker dere den mange ganger daglig, eller?

A: Ja, alt for mye

I: Jeg bruker ganske mye, for bare unødvendige ting

F: Nei, ikke så mye. Jeg synes det er en sånn tidstyv jeg. Jeg prøver liksom å la være, for det tar så mye tid, så jeg bare sånn "okay, nei, nei".

I: Jeg prøver, men, jeg klarer ikke helt å.. Nei, men det er veldig greit til sånn mail og sånt selvfølgelig, men ellers så er det jo bare VG og Facebook og sånt superunødvendig ting

A: Snapchat

F: Ja, du har alt på en og samme plass, det er så genialt, du slipper å liksom ta på PC og det tar jo tid ikkesant, det er jo liksom effektivitet her.

T: Ja, det tar jo sååå lang tid, så må du sette deg ned og så må du skru den på [sarkastisk tone]

F: Ja, så er den der liksom, så har du--.

M: Et eksempel er jo at jeg skrudde på nett, og nå ser mobilen min sånn ut [viser mange ikoner på skjermen og ler], sånn ihvertfall femten ting jeg må svare på her, det er veldig greit å kunne gjøre, bare mens jeg venter på at forelesningina skal begynne

I: Ja, ikkesant, det er jo sånn-- det er jo da jeg bruker den. Jeg bruker den jo når jeg venter på ting, på toget på vei til skolen, det er da jeg bruker det

T: Veldig bra tidsfordriv

M: Da slipper jeg gjøre det når jeg egentlig har bedre ting å gjøre.

I: Så det er jo det jeg egentlig bruker den mest til. Jeg har vurdert noen ganger å bare droppe det og kjøpe en ny mobil, når det ikke funker lenger, men så er det sånn av og til hvis du skal et sted og du ikke vet adressen så er denne kart, så er det hvis du skal ha telefonnummeret til noe, altså sånne småting som er utrolig greit. For jeg hadde jo klart meg uten å måtte sjekke Instagram og Facebook og Snapchat hele tida. Det hadde jeg jo klart, men det er jo liksom det når du "åh, jeg skulle ha telefonnummeret til et eller annet"

M: Det er så praktisk hvis man treffer nye og skal bare få noe perfiere--vent litt, vi må snakkes seinere, også legger man dem til på Facebook med en gang i stedet for å skrive ned navn også kan vi...

I: Da glemmes det--.

T: Men altså jeg har jo Instagram og Snapchat, men jeg bruker det aldri

In: Ikke begynn! [Latter]

T: Nei for det så lite å bli avhengig, det er det samme med Facebook før jeg var 18, og det var ikke fordi mamma og pappa sa nei, det var liksom prinsippsak, for det trenger jeg ikke. Men hovedgrunnen til at jeg fikk det er fordi jeg er halvt kanadisk, så halve familien min er jo på andre siden av kloden og det jeg fant er jo at det er veldig mye enklere å kommunisere med dem og se bildene og ja-- for mange har barnebarn også har vi, altså fetter og kusiner her og der, mener vi, så vi-- i Australia og vi har i India, så det gjør ting enklere på den måten å ha alle samla på et sted, men sånn som de av dem jeg snakker med mest, da går det på e-mail.

H: Hva med applikasjoner da? Bruker dere det? Så alt fra spill og sosiale medier til e-post og bank.

I: Ja, jeg bruker bare sosiale medier og bank

A: Jeg laster ned andre ting, men jeg bare bruker det ikke

I: Ja, ikkesant

M: Ja, jeg bruker også bare sosiale og mail, og jeg bruker det til noe som er sånn her til verv og sånn, fordi det er veldig greit å kunne gjøre det kontinuerlig og ikke bli tvunget til å "nå er jeg foran PC-en nå må jeg gjøre alt det her, nå har det samlet seg opp i løpet av hele dagen" og da er det sånn nei,nei,nei, gruer meg til å komme hjem.

I: Da legger du deg aldri den kvelden

M: Nei, ikkesant det er ganske praktisk å ha den sosiale medier greia, og men apps ellers, nei, jeg tar heller å jobber enn å spille.

I: Det eneste jeg spiller er sånn Quiz

M: Du er en av dem

T: "Epic Battle"

I: Å, nei det har jeg ikke hørt om.

T: Åja, nei, det er det er ikkesant

I: Åja ja ja, alt med Quiz er gøy, det er det eneste spillet jeg spiller

T: Også Wordfeud er gøy

I: Å det er jeg så lei av! [Latter] Jeg er så lei av det spillet, det er lenge siden jeg har spilt det da.

H: Men når dere laster ned applikasjoner, tenker dere på hva informasjonern-- for man gir jo ofte litt informasjon. Noen litt noen mye, når man laster ned applikasjonen for at de skla fungere sånn de skal da. Tenker dere på hvor informasjonen går, hvem som får det, eller?

M: Ja

T: Ja, jeg leser gjennom hver gang, hver gang jeg må godta noe

M: Okay, du er den ene

I: Nei, det gjør ikke jeg [ler]

A: Ikke jeg heller, jeg ser--.

M: Det er noe informasjon jeg ikke vil gi til sånn som, min ordentlige e-mail og sånt, men utover det så--.

H: Så du har flere enn en e-post?

M: Ja, jeg har den gamle, som jeg fikk når, som jeg hadde når jeg gikk på barneskolen og sånt, som er nå min spammail også har jeg den ordentlige også har jeg en jobb--verv-mail, som er kobla sammen, så det er den jeg har. Men utover det, så bryr jeg meg ikke så veldig, jeg prøver å heller ikke å si ja til at den skal bruke tjeneste som krever--siden jeg har trådløstne--siden jeg ikke har mobilt bredbånd, så unngår jeg å hake av på ting som bruker masse data ellers--.

I: Jeg ser på også på med en gang jeg må, for når man må skrive inn informasjon, det

kommer litt an på hvilken type informasjon jeg må skrive inn og hvis jeg ser at det er veldig mye jeg ikke har behov for å dele, så dropper jeg det heller, på en måte

M: Dem aller fleste apps, så kan du også gå via browseren din og få samme tjensten, så da gjør jeg heller det

I: Ikkesant

H: Fordi du ikke vil gi den informasjonen?

M: Ja, eller for at jeg ikke vil at appen skal få mulighet til å gjøre ting for mye på mobilen min--.

T: Ja, automatisk--.

M: Ja, og noe av det er rett og slett fordi jeg har ikke-- jeg har en arbeids-veldig enkel telefon, så det betyr at jeg vil helst ikke at den skal kjøre masse prosesser som gjør at den blir mye treigere rett og slett, jeg har en dårlig telefon og vil helst ikke drepe den med apps [latter]

I: Ja, men det er litt min grunn og til at jeg ikke vil ha så mye apps, jeg vil ikke at mobilen skal bli treig

M: Jeg må gjerne ha hva som helst, så lenge det ikke kjører i bakgrunn, med en gang det kjører i bakgrunn så nei, da vil jeg ikke ha det.

T: Jeg skrudd av 3G-nettverket, jeg pleier å skru det av, for jeg vet når jeg har behov for det ikkesant, så da skrur jeg det på og da vet jeg at ikkenoe skjer i mellomtiden, hvis jeg trykker på noe, eller appen gjør, så bruker jeg penger på det for det er en forferdelig utgift. Det er sånn unødvendig.

A: Det er en ting, på PC er det mye lettere å skru av bakgrunnsprosesser, men det har jeg ikke sett på smarttelefonen

M: Det går an, men det er litt styr. Det er ikke mye styr, men det er mye enklere å ikke si ja til at bakgrunnsprosessen skal komme på i utgangspunket

I: Eller så må du gå inn å gjøre det på hver app etterpå

M: Men det finnes innstilling som--det er faktisk ganske lett, du må bare gidde å søke på nett for å finne det--men ja

T: Jeg gjør jo det, og det er derfor den virker. Men tingen er at, det er derfor dem sier at du skal skru av mobilen din minst en gang i uka for at bakgrunnsprosesser skal lukke seg ordentlig. Og derfor sier dem at alle smarttelefoner skal skru seg av en gang i uka.

H: Så, det var en som leste personvernserklæringer, er det flere som ser på det når dere godtar applikasjoner, eller bar trykker dere OK--.

F: Jeg stoler blindt jeg jeg, bare OK

A: Ja

M: Jeg tror kanskje jeg gjør det samme som ho, fordi at jeg leser--jeg skimmer ned, er det noe jeg burde reagere på, er det her de vanlige avsnittene, og hvis jeg bare "okay, som vanlig, og greit" så er det ok, hvis jeg "vent litt, den her så litt rar ut" da leser jeg det ordentlig. Men det er litt fordi at det er del som spør om informasjon til mail og hvis jeg da er tvunget til å oppgi den ordentlige mailen min, så har jeg faktisk en del personsensitiv informasjon der, ikke om meg selv, som jeg må, altså som jeg skal beskytte, som det er liksom jeg har taushetsplikt i noen sammenhenger, så jeg vil--jeg kan ikke gi appen tilgang til den informasjonen. Men hadde det ikke vært for det, så ville jeg selvfølgelig bare "bryr meg ikke", men, ja.

I: Men ja, men det er jo fornuftig

T: Nei for jeg laster jo ned fra Google Play, så jeg vet jo hvilken informasjon som er der allerede, for den er jo kobla til Gmail kontoen min, og da vet jeg jo egentlig informasjonen som driver å spiller.

H: Okay, så når du skal laste ned en applikasjon da, hvor går grensen for hvor mye informasjon du gir? For, som sagt, hvis for eksempel, jeg vet ikke om noen av dere bruker løpe-apps eller, Nike har jo en sånn app hvor den måler-- eller distansen og farten og ofte kan den fortelle deg hvor mye du har forbrent osv., men jo mer av de detaljene du skal ha, jo mer informasjon må du gi den appen om deg selv, da må du jo, den må jo få vite hvor du er, og vekt og alder og høyde og alt sånn der. Hvor går grensa for dere i hva slags informasjon dere gir en app? Har dere en sånn her "hit men ikke lenger"

A: Kommer litt an på hvor mye jeg stoler på appen og hvor mye jeg føler selv at jeg kan få utbytte av å bruke den, hvis jeg føler jeg kan få veldig mye utbytte av den og hvis jeg føler det er en seriøs aktør kan jeg ofte gi mer informasjon enn hvis det er liksom sånn, det er ikke noe poeng for meg å gi den informasjoinen, for den gir meg ikke tilbake, da gjør jeg det ikke.

M: Jeg bryr meg vel-- altså, utover det med mail, at det jeg er veldig var på det, så bryr jeg meg vel ikke så veldig. Om noen vet hvor høy og tung jeg er, så fint for dem, du har kasta bort et minutt av livet ditt, kos deg, med det er ikke helt--.

I: Men, sånn som jeg bryr meg ikke om sånne ting jeg heller, men noen gjør jo det sikkert, men det er sikkert veldig variert. Men akkurat, igjen, det er ikke så veldig sånn type informasjon som jeg har noe behov for å skjule, for folk finner ut av det hvis de vil uansett.

T: De tvangsveier deg [latter]

I: Ja, ikkesant. Det er litt det der

M: Jeg vet ikke selv hvor mye jeg veier, så det er litt håpløst å snoke i den informasjonen, hvor mye veier du? Hm, ja, godt spørsmål

H: Ok. Du sa noe om seriøse aktører, det spørs litt hvem som gir dem [ser på A], er det forskjell, på apps, på - i forbindelsen med hvem som har dem, hvem som har dem, hvem som tilbyr dem, er det noen du laster ned og noen du ikke laster ned?

F: Ja, jeg ser det er sånn der at man kan gi stjerner på hvor mye andre liker de, også tenker jeg "å full score, bra!, kjør på", også noen bare sånn en stjerne, her er jeg skeptisk [ler]

M: Det har vel ikke helt med personvern å gjøre akkurat

F: Neida

T: Påvirket av massene da

M: Utover bank så tenker jeg at det ikke betyr noe. Det jeg har som er personsensitivt er personsensitivt, så det kan jeg ikke dele, så det, jeg veit ikke. Jeg skiller ikke mellom seriøse og useriøse fordi at--.

T: Jeg ville si det ligger igjen fra videregående når vi lære å bli kildekritisk [latter]. Så jeg sitter noen ganger når jeg kjenner igjen, pleier jeg å sitte å se hva det faktisk er, også "nei, liker ikke deg" da finner vi en annen og det er liksom på hva du liker og ikke liker. For veldig få forstår egentlig hva som står der, ikkesant. Så det går på hva jeg kjenner igjen, hva som blir brukt mest, ikkesant, og fram og tilbake.

H: Brukt mest av folk generelt, eller?

T: Ja, altså brukt mest i samfunnet, allment akseptert da.

T: Ikkesant, sånn som Skype er utgitt av Skype, okay da laster vi ned Skype utgitt av Skype. Hvis vi har Skype utgitt av et eller annet annet, da laster vi ikke ned Skype.

H: Har dere noen gang bestemt dere for å ikke laste ned en app fordi dere var usikre på hvem som stod bak den, eller hva den gjorde eller--.

T: Ja

I: Njae [ler]

F: Nei

T: Ja, men jeg skjønte ikke hva som stod der, så jeg lasta den ikke ned, derfor trenger jeg den ikke. Jeg leste jo, også skjønte jeg ikke helt hva dem skulle ha tilgang til, så tenkte jeg "da legger vi deg vekk" også tar vi en annen.

I: Jeg har ikke lasta ned en app før, ja, men ikke fordi de skulle noe informasjon jeg ikke ville dele, det var mer for "nei, det så ikke noe gøy ut allikevel liksom"

[De andre sier seg enige]

A: Min er liksom en blanding av det

M: Jeg laster jo nesten ikke ned noen apps, men jeg føler at det er nesten--hvem kan jeg stole på av apps fordi at jeg vet jo--altså hvis dem prøver å få tilgang--det er en ting på mobilen som jeg ikke vil de-- som jeg ikke kan, skal dele, så ja, jeg har latt være å laste ned apps på

telefonen, og hvis det har vært noe veldig krise som jeg kan gjøre på PC så har jeg heller gjort det der.

T: Jeg synes det er irriterende at du ikke kan avinstallere noen av appene jeg

M: Kan du ikke?

T: Nei, det er noen av appene--.

I: Ja, de som ligger der fra før--.

H: Ja, det er de som kommer med telefonen

T: Så kan det hende du må oppdatere og sån hæ? det tar så mye--unødvendig plass, også får jeg dem ikke vekk

M: Eh, jo, men... [mumler]

H: Vet dere om noen farer ved å laste ned og bruke applikasjoner? Farer er jo et ganske sterkt ord, men..

I: At de sluker batteri, det er vel det eneste [latter]

H: Tenker litt mer personverns--.

M: At them raider innboksen din og som-- fordi at dem kommer jo direkte inn på telefonen min, jeg har ikke noen to-trinns når jeg er på mobilen min, det er det eneste stedet jeg ikke har to-trinns for e-post. Så det kan dem jo i teorien gjøre, lese--alstå raide e-posten min og få masse kjipe personlige data om andre personer og legge det ut og det hadde vært litt kjipt, så derfor er jeg veldig restriktiv med hva jeg laster ned av apps, men ja

A: Men altså burde det ikke være fullt mulig å lage en app som egentlig bare--som egentlig--som bare tar å stjeler din informasjon som et virus da--.

M: Men det fins--det fins, det er det som er problemet, det er derfor jeg ikke tør å laste ned noen særlig apps på den utover type ting utgitt av Microsoft, lasted ned fra Microsofts egen side som jeg kan saksøke til helvete og forbi hvis dem gjøre noe med det. Okay da kunne gått.

I: Men har det ikke vært noe greier om det iMessage--nei ikke iMessage, men Messenger på Facebook? Vet dere hva mener da?

M: Ja

I: Har det ikke vært noe greier med det, at med den så kan Facebook lese hva som står i mailen?

M: Hvis du har kobla mailen opp mot Messenger

H: Jo, det har jeg hørt om

I: Ja, det er vis du har en Messenger da, ikke gjennom Facebook, men hvis du laster ned den appen, så kan Facebook lese alt som står

M: I Messenger-meldingen? Ja, men den kan lese det bare i Messenger, eller kan det lese det i annen e-post også?

I: Bare i Messenger, så Facebook kan liksom lese alt det du har skrevet hvis du har lastet ned den.

T: Men vet dere at Facebook har tatt oss å -- har mange forsøkskaniner og brukt oss, så ja, så tror jeg det er en veldig sjangse for at de gjør det, men det er jo problemet at nå tror vi faktisk at de kommer til å gjøre det

I: Men igjen, jeg bruker jo ikke Facebook Messenger hvis jeg skal dele noe veldig sånn privat da. På en måte, det håper jeg ikke så veldig mange gjør. Men allikevel så er det jo ikke alt man trenger å dele.

A: Hvis vi skal gå litt, altså-- var det-- det skjedde--på macer da så-- de passer jo på alt inni, bortsett fra batteriet som også er mulig å hacke, så da var det folk som hacket batteriene til macer rundt omkring i verden og fikk dem til å overkjøre og eksplodere. Så da fikk folk plutselig en mac som eksploderte i fanget sitt.

H: OI

M: Det har skjedd

T: Det er så greit med mac!

A: Neineinei, det er fult mulig med pc også

M: Det var det som er poenget mitt

T: Konspirasjonsteorier, kanskje det var Apple som gjorde det.

A: Ja, ikkesant

H: Men når jeg laster ned apps så popper det jo opp ofte-- så spør den, "kan jeg få lov til å ta i bruk mikrofonen, kan den få tilgang til bildene dine, til kontaktene dine, pleiere dere å si ja til det?

A: Nei nei nei

M: Nei, den får ikke-- altså--den--altså virkelig ikke

I: Du må jo det noen ganger

M: Men jo, men da bruker jeg ikke den, men det er ganske--for jeg bruker PC-en mye, så jeg bruker PCtil det som-- der dem skal ha tilgang til altmulig rart, greit. Da bruker jeg det heller på PC-en min, den bærbare PC-en min, så bruker jeg heller mobilen min til, altså, mobilen

min er det som er sikkert 100% der jeg ikke gir tilgang til noe.

T: Kan noe elektronisk være 100% sikkert?

M: Nei men så lenge jeg kan saksøke dem som tar det som er usikkert, så holder det

T: Ja, men ikkesant, det er samme poeng da så hvis du er syklist-- eller hvis du er fotgjenger og går over gata på grønt lys, men du blir påkjørt av en bil. Du kan jo saksøke helvete ut av den bilen, men du ligger jo fortsatt lamma på sykehuset.

M: Jojo, men altså-- alt er risiko-- du gjør jo risikovurdering hele tida, så

I: Men jeg tenker jo noe, sånn som Instagram, da må du jo godkjenne at de tar bildene dine.

T: Det liker jeg! For da ser du det at da kan du velge enten eller

I: Jaja, men da sier jeg ja, eller så er det ikke noe vits, men, ikke at jeg egentlig legger ut så mye bilder på instagram, men altså, men sånn mikrofon er jeg litt skeptisk til. Hvis de spør om mikrofon. Men bilder har jeg ikke så mye i mot, forde jeg har ikke så mye interessant, men akkurat mikrofon da, der sier jeg nei, og da sletter jeg den appen

H: Fordi du er redd for at noen skal kunne hacke mikrofonen, eller?

I: Ja, eller for at de kan ta opp, uten at jeg selv ønsker det. Jeg vet jo som sagt ikke så mye om, men det går jo sikkert an på et vis.

A: Det er også mulig for andre folk uten å--.

I: Uten at jeg har godtatt det, det er helt sikkert mulig, men akkurat mikrofon det--.

M: Kjøper man en billig nok telefon så har du en såpass ræva mikrofon at du faktisk må snakke inn i den for at den--.

I: Skrike inn [latter]

M: Jeg har problemer nok, okay den her fungerer greit nok, men jeg er ganske sikker på at hvis jeg nå, bare noen hadde hørt i mikrofonen nå når mobilen ligger denne her veien så ville dem slite med å få med seg hva vi snakker om

I: Men nå tenker jeg hvis jeg snakker i telefonen da, da snakker du inn mikrofonen og da kan jo det tas opp--.

T: Det er det samme med båndopptakeren som ligger på bordet, hvis ikke du hadde sagt at du tok opp samtalen så hadde vi aldri visst det, for der ligger jo bare mobilen din. Hvis vi ser bort i fra den andre. Og det er jo også personvern.

H: Det er jo litt -- det er jo den store debatten med Google Glasses, jeg vet ikke om dere har lest mye om det. Men debatten på de her-- sånne teknologi som blir på klærne dine, du kan få små kameraer som sitter fast i jakka di, som tar bilder, automatisk, Google Glasses tar jo bilder med at blunker, mer og mer sånn teknologi da, som kamera på hjelmer,

sikkerhetsvakter for eksempel går jo med kamera på brystet nå, sånne ting blir jo mer og mer populært og mer og mer brukt. Og da--.

T: Det går jo imot personvernet, for hvis jeg da blir tatt bilde av, og jeg ikke har sagt ja til det, og de da--så er jo det ulovlig, men det som er mest ulovlig er hvis dem legger det ut. Derfor synes jeg det alltid er veldig interessant med NRK og sånn når dem filmer på gata og mennesker som går forbi også ser vi ansiktet på alle sammen.

M: Jeg tenker jo det, det med sikk-- altså gitt at den dataen som samles på den måten-- altså den blir lagra men du får ikke-- altså ikkesant, du får en live feed på det, også går man inn i det hvis det skjer noe--.

I: Det er jo det samme med overvåkningskameraer. Det er jo ikke lov å sjekke de overvåkningskameraene hvis ikke det har skjedd noe.

M: Nei, ikkesant. Og det er jo ikke-- jeg er ikke så veldig for sikkerhetsvakter som har kamera på seg, fordi at --.

T: Det høres jo positivt ut da--.

M: Dem brukes så mange--. du får ikke en person -- du klarer--du gidder ikke å betale en person norske lønninger for å se over alt det i tilfelle det kanskje har skjedd noe--.

I: Det er jo bare hvis det skulle--.

H: Hva med Google Glasses da, som er for privatpersoner?

T: Og der kommer jo spørsmålet, for privatpersoner er jo noe helt annet. For dette her vi snakket om er jo på en måte offentlig da, hvis vi sier sikkerhetsvakter offentlig med at det er lagra og beskytta, men plutselig er offentlig, og dem kan legge det ut og--.

M: Men samtidig så er det litt vanskelig å forhindre deg i å bli observert, at noen tar bilde av deg i det offentlige rom, det skjer jo hele tiden, det har jo skjedd nesten siden kameraet ble oppfunnet og ble i praktisk nok til å holde i hånda -- så har jo det vært -- altså alt som er offentlig er i teorien mulig-- kan

I: Jeg synes ikke det er noe verre enn mobil--.

T: Ja, men du ser det ikke, tingen er at hvis jeg tar oppp mobilen nå og tar bilde av deg

I: Men jeg kan jo late som jeg tekster -- men jeg kan jo late som jeg tekster

M: Altså, hvis du går i en folkemengde, du klarer ikke å holde øye med 100 og x antall personer uansett. Og pluss at jeg vet ikke helt om jeg bryr meg så veldig mye altså hvis 100 personer ser at jeg driter meg ut, så blir det ikke så mye verre om en tilfeldigvis har tatt bilde av det. Altså 100 personer husker fortsatt at jeg dreit meg og-- offentlige er jo offentlig nesten uansett om du blir tatt bilde av eller ikke.

A: Men jeg tenker det at hvis man har sånne type ting da, så hvis man er på--ja, i på, private arrangementer, men det fortsatt er noen som går med sånne type ting, så kan jo de da liksom

dokumentere hva du gjør, i en privat setting, utenfor det offentlige rom, selvom du på en måte er- ja, så da tenker jeg liksom litt sånn--ja, de burde jo ha lov til å gjøre som de vil, men samtidig må man jo ta hensyn til

M: Det er jo litt sånn hva kan man tillate på sine egne-- altså er de hjemme hos meg, så kan jeg for eksempel kreve at, nei sånn skal ikke være i bruk og, og nå er jeg litt på den dere "saksøk folk til helvete og forbi beskyttelsen" men, det er en-- det er ikke -- da må det være-- altså, det er en grense for hvor mye folk gidder å snike med kamera og sånn, hvis-- altså så lenge det er lov å gjøre det

T: Det var en sak da jeg var i syvende, på det der, med altså hvor mye folk gidder, hvor en gutt hadde tatt et bilde av en jente i en jentegarderobe når hun var naken. Of course it went viral og sånn stor sak og masseerstatning og blablabla. Skaden er jo allerede gjort. Og det er jo mye mer det som er (...) med kamera som i garderoben. Altså, jeg bryr meg ikke noe særlig, for jeg er ikke noe særlig sky, men tenk å, det er jo mange. Altså, hvem vil ha et nakenbilde av seg lagt på nettet og spesielt når man ikke vet om det, og kanskje ikke i den beste siden, ikkesant [latter]. Så vi fikk jo inn regler mot det da. Altså, alle ble forklart at vi vil heller-- vi ser helst at dere ikke gjør det på grunn av det, og så fort alle skjønte det, så ble det--så tok ingen opp mobilen lenger.

M: Men--jeg vet ikke--jeg tenker at akkurat sånne her ting må nesten bare reguleres med lovgivning og potensiale for straff, for det er ganske håpløst å forhindre folk å gå med kamera, spesielt når dem er så små og sånn. Sant, da må beskyttelsen heller være at--.

I: Hvis det kommer ut, det er jo da man--.

T: Det er jo problemet!

M: Jaja, ikkesant!

I: Det er da man blir tatt--.

M: Jaja, hvis du legger det ut og det kan spores, det kan det ikke nødvendigvis men, jeg vet ikke. Jeg er selvfølgelig ikke noe veldig glad for det, men det er litt--jeg ser ikke helt hvordan man skal hindre det, spesielt på offentlig sted. På private sted så kan du bare ha at "her er det ikke lov å ha-glasses på og ta bilda, uten" og hvis du ikke gjør det, så hjelper vanlig regler, du vil bli anmeldt for det, så det--.

F: Kan man ikke bare sette seg i de andre sitt sted og bruke litt sunn fornuft da, bare sånn der, tenke gjennom det her med hvordan vi lever--.

M: Men det meste av det her-- men altså det meste av det her er det jo lovning på allerede, sånn at hvis du--altså, i utgangspunktet satser vi på at folk bruker sunn fornuft, hvis dem ikke gjør det, og du synes det er ille nok, så kan du faktisk gå til politiet og si "hei" eller bare til tvist eller rettsdomstoler og forsåvidt.

T: Nei, for dette er jo problemet, eller når jeg sier problemet, med dette samfunnet er at det er så mye teknologi og vet ikke helt-- ikke alle vet hva alt gjør og kameraer over alt, dem tar opp hva vi sier, dem ser hva vi gjør, og det kommer jo ned til at det er såpass nytt så vi har ikke regler for det.

M: Jo, vi har faktisk regler for en god del av det, for man har valgt å anvende gamle lover på en ny måte, som jeg kommer på--.

T: Men hvem vet det?

M: Ja ikke sant, det var det jeg skulle fram--.

T: Jeg kan ikke reglene. Det eneste jeg kan si er at okay jeg har sunn fornuft, så jeg tar ikke bilde av deg og legger ut på nettet.

M: Men det er kanskje noe som-- man bør--folk bør være mer bevisst på sine egne rettigheter i disse situasjonene, fordi det er ofte dårlig lovning som blir anvendt på litt kreative måter for å forhindre det her. Men dem finnes jo ihvertfall

F: Men siden det er så nytt så må de kanskje forandre--.

M: Jeg synes kanskje det er viktigere at folk er klar over hva som er--hva du kan reagerer på-- som du faktisk har lov til å reagerer på, enn at-- ja, det er vel et større problem det enn lovene. Ja, jeg snakker mye med folk i JussBuss [gratis rettshjelp i Oslo] og det er faktisk et problem, at de ikke er klar over hva de har rett til og mulighet til å gjøre--.

A: I statene så blir det jo mer og mer ulovlig å fly sånne fjernstyrte helikoptere eller fly fordi det er mulig å feste kamera til der og da blir det overvåkning--jeg tror det var sånn den logikken gikk--.

M: Det var også noe med å kræsje i fly, men okay, hvis man er litt uheldig--.

T: (...)

H: Jeg er lei for å avbryte en veldig interessant debatt, det er jo mange veier man kan gå med personvern. Vi er snart ferdige, men jeg har en ting til jeg har lyst til å vise dere før vi avslutter, som jeg vil gjerne ha deres mening på. [Viser fra en telefon og applikasjonen ValYou] Det her er en ny applikasjon som-- jeg skal bare vise dere hvordan den fungerer-- som--det kan hende dere har lest litt avisene om det nå den siste uka, men den ligger her på skjermen som heter ValYou. Det er en applikasjon som gjør at du kan bruke telefonen din som et bankkort. Det her er ikke mitt bankkort, det er en simulasjon [latter]. Jeg har ikke 12345kr på bankkontoen min, jeg skulle ønske [latter], men her laster du altså inn bankkortene dine og så når du kommer til en butikk, som har en sånn--et sånt merke på den-- skal ha et sånt merke [viser fra NFC-klistremerker]. Så legger du telefonen inntil merket [telefonen piper], lager den sånn lyd, også må du -- nå er -- ser du beløpet det er på 456kr, så da må jeg taste inn en eller annen kode. Også står det at transaksjonen er utført. Hvis det er under kr 200 så kan jeg bare "bipe" og så har jeg betalt for det.

M: Er det mulig å endre settinger så du ikke kan bare "bipe" hvis det er under 200 kr?

H: Ja

M: Ja, da har ikke jeg noen store problemer med det.

H: Ville du lasta det ned?

M: Ja, det er ganske greit utprøvd allerede og--altså jeg er jo ikke-- altså i det i mange land så er det mer vanlig med mobil enn med bankkort fordi at folk har mobil og ikke bankkonto. Det er jo ikke noe værre enn-- jeg har jo bankkortet mitt over alt, og mobilen min med over alt. Hvis du fortsatt på taste koden, så er det jo ikke noe-- altså, det er ikke noe større sjanse for at jeg mister mobilen min enn bankkortet mitt allerde--.

I: Men problemet er vel hvis noen kan ta den informasjonen. Er det ikke det?--.

H: Det blir jo, informasjonen ligger jo på nett--.

I: Ja, det er det jeg mener for jeg har ikke noe-- jeg hadde ikke hatt noe problemer med det, jeg hadde lett lastet det ned, sålenge det er kode som du sier [ser på M]. Men for bankkortet, ja, mister jeg bankkortet så kan noen misbruke det. Men her er vel ikke poenget at, hvis du mister mobilen, men her er vel poenget at det ligger ute på nett

A: Det blir vel sikkert samme type greia som nettbank egentlig, du har jo på en måte mye informasjon på nettet (...) [M overdøver hva A sier videre]

M: Men forskjellen er vel-- kan du koble den til en type kodebrikke, som du ville gjort med nettbank?

H: Det kan du ihvertfall ikke gjøre nå

M: Når jeg tenker meg om så ville jeg ihvertfall ikke brukt den før det skjer, fordi at, da vi-- jeg ville heller-- eller-- altså det kan jo hende at krypteringa er god nok til at jeg kunne brukt den nå også. Er det ikke så god kryptering da vil jeg helst ha tilsendt en kodebrikke, fordi den er ganske mye vanskeligere å hacke. Eller dem er fysisk umulig å hacke. Du må klare å simulere dem, men, det klarer du vanvligvis ikke.

[De andre snakker om applikasjonen i bakgrunnen]

T: Jeg ville--.

A: Jeg bare tenker på en annen ting, og det er det at, står ikke banken egentlig ansvarlig for penger som blir tatt--misbrukt, for jeg tenker at hvis--når de gjør det, og velger å stå ansvarlig for det, da føler jeg i grunn det at det er ganske stor sannsynlighet for at de passer på informasjonen din ganske godt. Fordi at de får store erstatningskrav hvis ikke--.

M: Stortsett har dem, men ikke alltid.

H: Det stemmer for denne applikasjonen også.

A: Det var den jeg tenkte på.

T: (...) De har jo også et tall på hvor mye de er villige til å miste på dette her, altså hvor mye dem er villige (...) Eh, altså, jeg ville ikke lasta ned den, for jeg har ikke bankID på mobilen heller, for jeg føler at PC-en er sikrere enn mobilen og det er den, så derfor er nettbanken, det gjør jeg alltid på PC-en--.

F: Det gjør jeg også, pågrunn av det her skru av og på Java, så jeg er veldig skeptisk til det her med--. [Latter]

T: Og det jeg også ser er at jeg kan miste telefonen min like enkelt som et bankkort, problemet er at hvis jeg mister mobilen, så er det mye--så får du mye mer informasjon ut av min mobil enn at jeg-- enn dem får hvis jeg bare mister bankkortet. Og hvis jeg har det at jeg bare sånn-- under 200kr beløp-- så kan de jo bare fly rundt-- det er veldig mye som koster under 200kr i Oslo altså.

A: Ja, men du kan maks bruke 600 på et døgn, så da er du jo i sikkerhet, da må du--.

I: Du kan jo bare endre det, kan du ikke det?

M: Men det kunne du ta på settingene-- det kunne du-- men du har innstillinger-- jo ho sa at du kunne endre instillingene-- så du kan jo faktisk gjøre sånn at du må ha kode uansett.

T: Men jeg er jo sånn at jeg lar andre være forsøkskaniner, så to år fra nå, hvis det er fortsatt bra alle bugs er ute av systemet, da laster jeg ned.

M: Så lenge man har en bank som har penger nok til at man kan saksøke dem, så tenker jeg det kan funke. Jojo, men ikke gjør det Cultura for eksempel. [Latter].

H: Men hva om jeg sier at det er Telenor som står bak den applikasjonen her? Ville det endre på om du ville lasta ned eller ikke lasta ned? Har det noe å si, at det er telenor som har laget den.

A: I forhold til andre store, eller i forhold til?

M: I forhold til hvem er alternativ, hvem var det første?

H: Til-- ja i forhold til -- nå var ikke dere veldig skeptiske til denne applikasjonen generelt, men si du hadde vært skeptisk da til en applikasjon også får du vite at det er Telenor som står bak den applikasjonen, har det noe å si? Ville du da valgt å laste den ned?

M: Så lenge Telenor gjør det sånn høvelig greit økonomisk, så ja, det hjelper jo selvfølgelig, men når man kan--.

A: Det handler jo om hvem som er ansvarlig

A: Ja, det gjør jo det

M: Ja, det handler jo til syvende og sist om hvem og hvordan lovninga fungerer men, jeg kjenner at jeg måtte vite mer om hva reglene er før jeg kunne brukt det. Hvem som til syvende sist er ansvarlig, hva som regnes som-- jeg vet som sikkert hvordan de gjør med mitt eget bankkort, hva som må til for at jeg--for at banken ikke lenger er ansvarlig for misbruk, da skulle jeg gjort sånn og sånn, det er greit. Men det vet jeg ikke med den der, så det må jeg nesten vite.

A: Å, ja, og sånn sett er det mye-- jeg føler det ville vært mye bedre å da nedlaste apper fra

statlig eide organisasjoner, fordi da er det staten basically som står ansvarlig, så hvis-- det skla mye mer til for at staten går bankrupt enn banken

M: Men beløpene dine er til en viss grad sikra gjennom staten allerede, dem som er fra banken, på kontoen din faktisk. Så jeg vet ikke om det har så mye å si i praksis

H: Men så du har mer tillit til statlige organer eller organisasjoner--.

A: Nei! Det har ikke jeg

T: Nei, ikke tillit, de har mer penger, altså det er større sjanse for at banken goes bankrupt-- hva er det på norsk a?--

A: Konkurs?

T: Takk! Det er større sjanse for at banken går konkurs enn at staten går konkurs.

M: Akkurat hvis banken går konkurs så er beløpet ditt sikra gjennom staten uansett--.

A: Men det er bare opp til 2 millioner som skal bli nedjustert--.

M: Er det noen her som har stor fare for å ha mer enn to millioner--.

[Latter]

A: Nei, nei, men altså, kanskje en gang

I: Det hadde vært veldig greit

A: Men det finnes liksom en øvre grense

M: JAja, jeg vet det

A: Men gjelder det også for privatbanker? Og banker i utlandet?

M: Eeh, faktisk

A: Det gjelder uansett.

A: Nei, det gjør det ikke. I EU er det 100 000 EUR og det er det det skal bli i Norge også.

T: Men vi er ikke i EU?

A: Nei, men EØS, men vi får alle reglene allikevel. Nei vi er ikke EU, men vi må følge alle reglene allikevel

T: Nei, vi er ikke i EU, det er ikke noe som har skjedd [ler]. Nei, men jeg håper ihvertfall folk leser, altså, en sånn app, så håper jeg folk leser mer på da, fordi det har mer med pengen dine å gjøre enn vanlig.

M: En ting som jeg merka meg, du sa at du var redd, du ville ikke bruke for du var redd for å miste-- mobilen var det mer informasjon på, men du går jo rund med mobilen og bankkortet ditt stort sett uansett, så den informasjonen fra mobilen din vil dem kunne finne hvis du mister mobilen din allerede, du legger bare til en ting. Og hvis man går ofte med dem sammen, som man fort gjør, fordi at man har dem i den sikre lomma, så er det--.

T: Nei, ikkesant, å det er--tingen er at jeg har kortene mine fra hverandre, så hvis jeg mister ett så mister jeg ikke de andre--.

M: Nei, altså, jeg har også, for jeg bruker bare et kort [latter]

A: Det gjør jeg i utlandet, da deler jeg det opp. Men jeg gjør det ikke i Norge.

T: Ja, ikkesant, jeg har jo veska mi, men altså tilog med i veska mi så er det-- altså delt opp, det er sånn at jeg har mobilen også har jeg bankkortet. Og det skal mye-- og tingen er at når du går-- du går jo ikke med mobilen-- eller det beste eksempel da, menn i gamle dager gikk med penger i skjortelomma også bøyde seg også falt alle pengene ut også gikk de videre. Ikke gjør sånne ting, ikkesant, ha litt mer sikre med tingene.

A: Men det går veldig mye kjappere fra jeg merker at jeg har mistet mobilen, enn, lommeboka, lommebake kan gå, jeg bruker kanskje en eller to ganger om dagen, og den ligger enten i jakkelomma eller en plass i sekken, mens mobilen har jeg hvert femte minutt liksom--.

M: Det er faktisk et veldig godt poeng--.

A: Du finner ut av det med en gang hvis den er borte

M: Jojoj, jaja, det er faktisk et jævlig godt poeng, for nå kjenner jeg at jeg kanskje ville vært litt mindre skeptisk til for akkurat-- for ja, jeg ville kanskje ikke merket at jeg hadde mista kortet før et par dager etterpå--.

A: Ja, det kan gå et par dager for du tenker bare "det er sikkert bare glemt hjemme på en eller annen plass"

M: Eller, jeg sjekker ikke!

T: [Ser på I] Du har mista mobilen.

I: Alt!

T: Var det smarttelefon, eller?

I: Ja det var en iPhone, og bankkortet og lappen og togkortet

T: Åh. Men altså, hvor mye jobb var det å stenge av alt.

I: Det var en telefon. Det var en telefon.

T: For mamma mista sekken hennes i (..)så da er jo, mamma er jo mye eldre enn meg,så da er

det mange andre kort, så da var det jo å ringe, altså først, jeg stengte e-mailen, jeg ringte banken, og det var så mye jeg måtte ringe og stenge og ordne og greier, for at hun fikk jo tilbake alt på forsikringen, men jeg var jo--.

I: Men man skal aldri ha med seg alle kortene sine til utlandet, det er sånn [latter].

T: Men hun hadde ikke alle kortene, men det er liksom bankkortet. Men tingen er at jeg stengte e-mailen også (...)

A: Jeg bruker bare kredittkort i utlandet

[Samtalen fortsetter litt om private ting mellom respondentene]

A: Det som jeg tenker mest på egentlig med sånn NFCteknologi og sånn type ting, er at det går kanskje ann å kopiere mobilen og da om det går an at de kan på en måte få lagt det over på sin mobil, din betaling, hva med liksom å-- jeg vet ikke hvor mye som skal til. Hvis du har mobilen liggende liksom og noen på en måte kan sitte to meter fra også bare hacke mobilen din.

M: Samtidig så er jo, så lenge bankene står ansvarlig for det så vil, ikkesant det er litt det. Det er dem som--så lenge det er dem som tar risikoen så er jeg ikke så bekymra for det.

I: Akkurat, det er det. Det har litt å si hvem det er som står bak.

M: Så lenge det er noen andre enn meg som står ansvarlig for sånne avanserte måter å ta den på, så plager det meg ikke så mye.

H: Så det har ikke med tillit til tilbyderen å gjøre altså, det her med--.

A: Jo

T: Jo det har med, jeg liker ikke Telenor, jeg har bare problem med Telenor.

H: Så du ville kanskje valgt å ikke laste ned pågrunn av Telenor

T: Ja, av prinsippsak, ja, ikkesant. Det ikkesant, at jeg har hatt veldig mye problem med telenor, som internett og mobilmessig, så jeg bytta jo vekk fra det. Og det er så deilig å ikke ha dem lenger.

H: Vi har kommet til en slutt. Vi har ikke mer tid. Nå ringer snart pizzabudet.

Appendix 4: Codebook

Unbelief

- Apathy
- "A computer – not people"
- Not believing anyone would use information

Implications (actual implications of loss or fear of loss of privacy)

- Chilling effect
- Fake information
- Deleting information
- Rejecting application due to fear
- PC instead of phone
- Pictures
- Protecting information
- Protecting money

Hypothetical fear (fear of something that could happen now or in the future, but not taking precautions)

- Example of Facebook
- Example of health information
- Fear of future consequences
- Surveillance

Threats of loss of information

- Pictures
- Power
- Protecting money
- Who to protect from

Mainstream (making decision based on either upbringing, close relationships or the masses)

- Culture
- Upbringing

- Following the crowd
- Good faith

Trust

- Adaption
- Apathy

The right to privacy (privacy for yourself and your “inner circle”)

- Basic assumptions of privacy
- Control over personal information
- Privacy for the sake of privacy
- “Privatlivets fred”
- Protecting family

Adaption (adapting to a new reality)

- Adaption
- Allowing apps to access information
- Application types
- Convenience
- Good faith
- Owning smartphone
- Positive effects of less privacy
- Smartphone usage

Use

- Application types
- Owning smart phone
- PC instead of phone
- Smartphone usage
- Not using apps for practical reasons

Feelings (from not protecting information)

- Fear
- Shame

MISC

- Respondents' definition of private information
- Democratic benefits of privacy
- Media
- Economy of information
- Experience with privacy invasion
- Heard of examples
- Illegal activities
- Lack of knowledge
- Law regulations
- Personalisation of technology
- Privacy policies

Appendix 5: Follow-up questions

Norwegian group

Questions

1. Ville du vært villig til å betale en sum i måneden for å bruke applikasjoner, uten at de fikk noe informasjon om deg? F.eks. 50kr?

2. Bruker du ditt ekte navn på Facebook?

3. Av de som har et innebygget webkamera på laptopen sin, er det mange som dekker det med et klistremerke for å unngå at noen hacker seg inn på kameraet. Gjør du det, eller kjenner du noen som gjør det?

I: 1. Det kommer helt an på app'en. Men tror ikke jeg ville betalt en pris i mnd, heller et engangsbeløp.

2. Ja, det gjør jeg.

3. Jeg gjør ikke, og kjenner ingen som gjør det..men har hørt at folk gjør det.

A: 1. Jeg ville i det minste vurdert å betale for å slippe unna all registreringen av informasjon av meg selv! 50,- er ikke spesielt mye, så tror jeg ville endt opp med å betale, men kommer litt an på hvilke aktør det var snakk om og hvorvidt jeg følte det kunne være sensitive eller om det bare var overfladig. Altså informasjonen de ville fått. Lagret og brukt om meg!

2. Jeg bruker mitt ekte navn på Facebook!
3. Jeg både har gjort det aktivt selv og kjenner andre som har gjort det aktivt. For tiden gjør jeg det ikke (kanskje litt over 1 år siden jeg sluttet) og vet ikke om hun andre fortsatt gjør det eller ikke...

T: 1. Jeg er ikke villig til å betale for applikasjoner. Men jeg er mere åpen får det hvis de ikke får noe informasjon om meg.

2. Ja jeg bruker mitt ekte navn på facebook, men jeg har mellomnavnet mitt med noe som hvistnok har gjort det vanskligere å finne meg.

3. Jeg gjorde det da jeg var yngre, og det var fordi jeg ikke helt forsto hvordan ting virket. Nå som jeg er eldre har jeg sluttet med det. Hmm. . . Dette har jeg ikke tenkt over før. Men ja jeg kjenner flere som gjør det spessielvoksene/eldre

F:
1. Jeg ville vært villig til å betale en sum uansett om de fikk noe informasjon eller ei. Om noen ønsker å finne informasjon om oss, så kan de finne det på internett uansett.
2. Ja, det gjør jeg.
3. Ja, kjenner flere som gjør det. Gjør det ikke selv, men vet at de gjør det fordi de ikke ønsker at noen skal ta bilde av de og opprette en falsk profil i deres navn eller stjele identiteten.

German group

Questions

Q: If you one day found out that the police had looked at the information available about you online (e-mails, Facebook account etc.), stating that it was necessary to solve a case, how would you react to that? Would it be okay?

S: I think it depends on the possible crime I've committed. Suppose, I am a terrorist and threaten people lifes I would fully understand that the polices looks into my facebook and every possible data thats avaible. But If I am curious why the police needs my personal data from the internet to solve the case: there should be a guideline when it is really necessary to look into ones life and when its not allowed to use the data.

A: Det er et godt spørsmål fordi faren men er en politibetjent. Jeg skulle ha vært veldig sur når politiet leter etter noe i private meldinger. Først og fremst bør jeg spørres. Jeg vet at politiet har mange rettigheter, men de har også plikter. Det er definitivt ikke ok!

N: First reaction: not ok! However, if there was probable cause that I commited a murder or sth like that, I guess - though I would still be pissed, it could be understandable.

R: I would be confused because I would have expected them to ask me before they look at it.

J: This would not be ok for me because I have not agreed that the police or any official or public institution may use my data.