Understanding digital privacy

Vejleder: Birger Larsen
Semester: 10
Studieretning: Informationsvidenskab
Gruppe nr.: 71
Antal tegn: 171603 / 71,50 sider

COPENHAGEN INSTITUTE OF TECHNOLOGY
AALBORG UNIVERSITET

Synopsisskema /projektbeskrivelse
Humanistisk Informatik
Forår 2015

Vejleder:Birger Larsen	
Gruppenr.: 71	Semester:10
Retning: Informationsvidenskab	
Fuld for –og efternavn for alle gruppens medlemmer samt underskrift:	
Kasper Risgaard	
Mads Maarup	
Projekttitel: Understanding digital privacy	
Anslag og sideantal (projekt modtages ikke ved overskridelse): 171603/71,50	
Dato for aflevering: 1/6	2015

Abstract

Projektets fokus er at identificere hvordan brugere opfatter privat data og indsamlingen af dette samt hvorvidt vi kan forsøge at ændre adfærd og holdninger ved at øge opmærksomheden omkring hvilke data der bliver indsamlet fra dem.

Vores videnskabsteoretiske tilgang til projektet bygger på socialkonstruktivisme og fænomenologi. Socialkonstruktivismen bruges til at opnå en større forståelse for det sociokulturelle, og de sociale konstruktion der binder danskernes forståelse sammen. Det fænomenologiske bruges på ontologisk basis, til at forsøge og forstå begrebet 'digital sikkerhed' som et fænomen snarere end en betegnelse.

En indledende undersøgelse af hvordan det nuværende tilladelses system i Googles Play Store fungerer som platform for vores prototype design. Designet af prototypen bygger på en undren over hvorfor forskellige apps skal have adgang til data der ikke umiddelbart tjener noget formål i forhold til deres funktionalitet

Vi indsamler vores data ved hjælp af tre forskellige metoder. En spørgeskema undersøgelse, tre ekspert interviews med henholdsvis en advokat, en app udvikler og en person der arbejder med forbrugerrettigheder og en fokusgruppe. Spørgeskema undersøgelsen giver os noget kvantificerbar data vi kan bruge til at generalisere over vores demografi. De tre interviews giver os en praktisk viden omkring fænomenet digital sikkerhed. Med den viden vil vi forsøge at forstå hvorfor brugernes handlinger i forbindelse med installation af software som vi har forsøgt afdækket i spørgeskema undersøgelsen.

Prototypen bliver herefter taget i brug i fokus gruppen hvor deltagerne får mulighed for fravælge tilladelser de ikke føler appen skal have tilgang til mod at funktionaliteten også ændrer sig.

.

Vi konkluderer på baggrund af vores data at det er muligt at er muligt at ændre brugernes adfærd ved at øge opmærksomheden på hvilke data der bliver indsamlet om dem.

Vi foreslår som yderligere forskning at der udarbejdes en digital prototype af designet der vil sørge for at forbedre den data der kan indsamles vedrørende brugernes interaktion med designet. Ydermere vil det være fordelagtigt at forske i hvorvidt faktorer som alder, køn og uddannelses niveau med mere påvirker brugerens forståelse af privatdata og deres opførsel i forbindelse med deling af privat data.

Indhold

Introduction

During the past few years privacy and private data has become a popular topic in the media. All of this was fueled by the Edward Snowden case of 2013. The revelation of widespread government surveillance surprised the American public, starting an ongoing debate on the boundaries of using the average person in data mining.

Alongside the discontent displayed by the media and the public debate, also raised the more questions about privacy in general. In a modern digital age where the majority have access to computers, internet and a smartphone, the concept of privacy also becomes more transparent. The case of Edward Snowden caused a reaction of such a great magnitude due to the fact, which something the public had acknowledged as privacy, suddenly turned out to be the opposite. As such, the acts of the American government was seen as a violation of one's privacy. In response to this, a series of data analysts have argued what the definition of privacy when seen in coherence with the modern digital age. Data analysts Karen Levy states, *"Privacy is not something that one has, but something that one seeks to achieve*" (Levy, Marwick, & Boyd, 2014). During the past years, this statement has moved closer and closer to being an evident truth. Meanwhile the media debate created by the Snowden leak was spun around the governments' access to digital private data; it also raised questions about the data collected by private companies. Meanwhile the government might access data users would deem as private, this might also apply to third party companies depending on social media companies choices. This possibility is quite possibly often taken for granted by the user despite it raises the risks of their private data being exposed. As an example one of the most popular smartphone apps Snapchat is tailored to give the user the impression that the data they create and/or share with others is contemporary, thus creating the illusion of using the app ensures confidentiality. Though looking at the terms of service and privacy for Snapchat it becomes evident that the app is collection information, storing the images that might seem contemporary, and accessing a wide range of other data provided whilst using the app.

Somewhere along the way, it seems that the user have lost control over their own privacy, in the era where big data is the new gold for companies. And the fascinating and at the same time horrifying thing about big data is, that there is no limit to how much data a company could wish for. At this moment in time all companies only, seek to obtain more data about their users. The more you use your smartphone, computer or electronic devices in general, you are constantly creating data. Data that can be collected, that signifies who you are, what interests you have, your whereabouts, your job, your amount of friends. The Danish newspaper Politiken published a feature article about big data last year, with the headline "Big data vil vende op og ned på din verden". (Jalner, 2014) the article takes us back to 2009 where the term "big data" was yet to coined, and gives an example of how powerful big data truly can be. During that, time there was an outbreak of the flu in America. The American healthcare department CDC were trying to keep track of the spread,

meanwhile instructing the people infected, with the prober ways to get well. Meanwhile Google experienced an increase in searches involving the flu. 50 million different search words and search combinations in correlation to the flu. From all of this data, they made an algorithm, which enabled them to tell where the flu was spreading. Meanwhile experts used to handling flu epidemics tried to predict the spread of the flu, however Google were always several steps ahead. Suddenly a private data company, with employees with no expert medical knowledge, where able to outdo the American government's healthcare department. Since then big data has become a common term, used in far more advanced scenarios than back in 2009. Companies like Google and Facebook, now gather the data created by their users, to tailor everything to the individual user, from commercial to additional services. From a utilitarian point of view, this is a good thing. The user gets a better experience, and does not have to put up with irrelevant commercials or content, when using the internet. However, since the collection of user data have become almost like a symbiotic relation between the company and the user, one could argue that the user along the way have lost his right to choose which data might be collected, and which data is private.

One of the most important terms used in this thesis, is digital privacy. When we talk about digital privacy in this thesis, we do not perceive it as something that has a definite meaning. However, given the nature of this thesis concerns itself with users using digital devices such as smartphones, what we try to hope to understand at the end of this thesis, is a better understanding of what digital privacy is to the user. In addition, how the user can come closer to obtaining it. We join Levy's notion about the clear definition of digital privacy is nonexistent in an era where digital technology is constantly changing. Instead, we perceive it as a phenomenon that changes along with the user. As such when henceforth mentioning the term digital privacy, it is from the user perspective, unless stated otherwise.

The user is the person located in Denmark, which uses a smartphone and other digital devices on a regular basis, as well as engaging in online activity across the internet.

Now one the questions of how it is possible to increase the user insight into what data might be collected during his or her use of a digital device, we have to look at the way companies are allowed to collect the data in the first place. Whenever a user chooses to use a digital service, for an example and app, they need to accept that specific app's terms of service. However, if the user ever tries to understand these terms of service, they meet chunks of text written in their non-native language. In this thesis, we seek to research the users' behavior when interacting with these terms of service, and figure out an easier way to let the user know if they might be downloading an app that gathers data, which they might see as private.

Additionally we will seek to understand the user's current rights, and to what extent companies are able to gather data from their users, in both a law-related perspective, as well as developers'.

All of these considerations leads to the following research questions and problem area.

- What rights do the users currently have over their digitally stored data?
- What are the users' current standpoint when being confronted with apps' terms of service?
- Do the users have interest in gaining more knowledge about what data they are sharing while using digital devices?

"How does users understand privacy and data in smartphone applications and is it possible to change their behavior by increasing awareness."

Theory

Qualitative Interview

The qualitative interview, also known as semi-structured or unstructured, is one of the most widely used methods for collecting qualitative research data. The reason for this is that the method, compared to the structured interview, is very flexible (Bryman, 2008). In quantitative research, the interview serves as a way to measure key concepts. As such, it very clearly structured because the data needs to quantify whereas the qualitative interview tends to revolve around the interviewees perspective. This means that in the qualitative interview the interviewer will have a more loosely defined set of questions and will instead try to ask follow up questions to further clarify the interviewees' point of view (Bryman, 2008). As the data are not meant to be quantifiable, there is less emphasis on the reliability and validity of the interview in the sense that several different interviews in the same research may not have the same wording or order of the questions (Bryman, 2008).

The qualitative interview can be further divided, as mentioned earlier, into the semi-structured and the unstructured interview. In the unstructured interview, the researcher works from a set of prompts or hypothesis inside a topic. The researcher may have a few questions and from there decides if the answer the interviewee gave is worthy of a follow up question (Bryman, 2008).

The semi-structured interview on the other hand is based on an interview guide. The interview guide holds a set of topics that is to be discussed with questions under each topic. As it is still a loosely structured interview the interview guide is not a manuscript that has to be followed precisely, but in most cases, the interview guide will hold the most necessary questions for the research (Bryman, 2008).

What type of interview the researcher chooses can depend on several different factors such as whether the researcher feels that a semi-structured interview will constrain the interviewees and not allow them to give their genuine perspectives, whether the focus of the research is general or specific and the setup of research team? For example would it probably be necessary to use a semi-structured interview in case the interviews are conducted by different people to have comparable methods (Bryman, 2008).

The qualitative interviews whether semi- or unstructured should always, when possible, be recorded and transcribed. When the researcher is conducting the qualitative interview, it can quickly result in the interviewees giving long complicated answers and as the researcher needs to be prepared to ask follow up questions it is best that he or she is not distracted by note taking (Bryman, 2008).

The qualitative interview can also be done by telephone. This method has some clear advantages over the face-to-face interview. Firstly, the amount of time and resources is greatly cut down as the researcher do not have to account for travel and setup time. Furthermore, in some cases it may be easier for the interviewee to take time out of their schedule to conduct a telephone interview than a face-to-face interview. There have been very few studies of the effect a telephone interview has

opposed to the traditional face-to-face interview, but the evidence seem to suggest that there is not a noticeable difference in the responses given (Bryman, 2008).

In the qualitative research field, there is often issues in relation to the sampling of interviewees. These issues are often in regards to the methods where the interviewees are selected and the quantity of the interviewees (Bryman, 2008). In many cases, the researchers' samples are out of convenience, using friends or family or opportunity. These issues often occurs because of certain constraints put upon the researcher and results in the researcher resulting to the safe choice.

The constraints regarding the qualitative interview, especially in regards to the telephone interview will be examined in the section regarding method constraints.

Constraints

Even though it is not as much a constraint as a consideration the researcher must have a clear idea of what type of data is needed for the research project before deciding what type of interview is being carried out. If the researcher is looking for specific knowledge in a field the interview will likely be semi-structured whereas the method used for collecting a more general knowledge will probably be an unstructured interview (Bryman, 2008).

When conducting a qualitative interview via telephone the researcher must have an in mind a set of issues that can occur.

The first constraint is obviously that certain groups are not reachable on telephone. This is becoming increasingly irrelevant with the spread of mobile phones, but must be considered before the researcher lays plans for the research. Secondly this method is not well suited for long interviews (Bryman, 2008). Then there is the problem of not being able to see the interviewee. This only matters if the researcher has a presumption that the interviewees body language is of concern to the research. Then there is the purely technical limitations including but not limited to: The loss of phone signal, sound problems and the fact that some form of special equipment is needed to record the conversation through the telephone. The last part has somewhat been mitigated by the rise of the Apple app store and Googles play store as there are applications directly downloadable to the researchers mobile phone that can record the calls. However, this raises another problem. In case the researcher conducts a face-to-face interview and records the interview on a recording device the interviewee can, with relative certainty, presume that the recording will not be shared. When the phone call is recorded with a third, party application the interviewee cannot be certain that the researcher has made sure the app do not share the files. As such, the researcher has an ethical obligation to take precautions to protect the people who has agreed in participating in the interview.

Lastly, there is the human factor. It plays a part no matter if it is a face to face or telephone interview, but it need to be considered as well. It may be easier for the interviewee to back out of a telephone interview because they only need to not answer their phone. It can also be difficult to set up an interview in the first place if the potential interviewee is not answering the phone for various reasons.

Focus group

As an academic interview form, focus group interviews has increased in popularity compared to the one on one interview (Kvale & Brinkmann, 2009). At first focus, groups were primarily used for market research but since the 1980's they have gained strong traction in academic research (Kvale & Brinkmann, 2009). As the name suggests the focus group is a form of group interview with several participants. Focus groups are a non-controlling interview form, which, as the name suggest is not controlled by an interviewer in the classic fashion. Instead, the interview is led by a moderator who presents the topic and help guide the conversation if it stops or the conversation is derailed from the topic (Kvale & Brinkmann, 2009). The main purpose of a focus group is to get different opinions from the participant and create an environment where the participants feel safe enough to express their personal opinions. The purpose with focus groups, traditionally, is not to get the participants to solve a certain problem or come up with solutions (Kvale & Brinkmann, 2009) but rather to get a discussion flowing over the chosen topic. The group dynamic can also be helpful in getting opinions from the participants that they may not have shared in a more cognitive interview form (Kvale & Brinkmann, 2009). When conducting academic interviews, no matter the format, several moral questions arise because the interviewer researches the private opinions and life of the interviewees and intends to put the results out in public (Kvale & Brinkmann, 2009). Steps such as keeping the interviewees anonymous in the paper or making the paper confidential can help mitigate these concerns, as the opinions will not be valid for anyone who does not know who the interviewees are.

When conducting focus groups some practical aspects have to be considered. The best results are achieved by recording and transcribing the session (Bryman, 2008). A reason for this is that: *"the simple difficulty of writing down not only exactly what people say, but also who says it"* (Bryman, 2008, s. 476). While the interviewer in a one on one interview might be able to write down what the interviewee says, it is almost impossible in a focus group because the nature of the interview invokes discussion between the group members and interrupting the discussion would disrupt the flow of the interview. Another point is that it is important to the researcher to know who says what. If this element is lost the focus groups loses the advantages of doing the focus group is also lost (Bryman, 2008).

When conducting focus groups the researcher must decide on how many groups is needed to achieve the results needed. There are no defining limits on the matter, but it is unlikely that one group would be enough (Bryman, 2008). Depending on the research project, several constraints that must be taken into account. How much time does the researcher have to conduct the focus groups, how much money is available, to pay the participants directly or in other way compensate the people involved and what resources does the researcher have access to. These are all arguments for keeping the number of focus groups from getting out of hand. When the researchers reaches a point where they can somewhat anticipate what the group is going to say there is probably enough data (Bryman, 2008).

As with the number of groups, there are no defining size of the groups. There a some recommendations based on how the group dynamic affects the discussion: *"Morgan (1998a) recommends smaller groups when participants are likely to have a lot to say on the research topic [...]He also smaller groups when [...] gleaning participants' personal accounts is a major goal"*. (Bryman, 2008, s. 479).

The researchers role once the focus group is started, is as a moderator and facilitator of the discussion. This does not suggest that the researcher should try to control the discussion as the main goal of the focus group is: *"... to get at the perspectives of those being studied"* (Bryman, 2008, s. 480). The researcher should merely try to guide the discussion along the line of the topic and let it unfold. If the discussion is being derailed, the researcher can intervene and steer the discussion back on the right track. This has to be done carefully as the researcher does not have a total picture of what the participants are getting at and may interrupt the process that could have revealed information of interest.

In the following section, we will examine some of the limitations that focus groups has as a method.

Constraints

As mentioned earlier the focus group method gives some advantage from the single interview. Its loose structure and the group discussion aspect may reveal things that would not have come forward in a single interview. It also forces the participants to reveal the reason behind their answers which can be difficult to achieve in a single interview without leading the interviewee on the course the researcher wants. However, the method has its limitations as well.

The first and probably most demanding constraint is the loose structure of the focus group. The researcher, presumably, has less control over the group than in an individual interview. As earlier mentioned this can bring out interesting results that otherwise would not have been uncovered. However, it is a double-edged sword, as the researcher has to try to limit how far the discussion is taken. If it gets too much outside the topic, the researcher has to cut in which interrupts the process. If the researcher does not cut in and allows the group to take, control the data gathered from the focus group can end up not being useful for the researcher and that means that time and resources are wasted (Bryman, 2008). There are no clear definitions of how much control can be given to the group and therefore it takes an experienced researcher to fully utilize the potential of the focus group.

The data gathered from focus groups are typically difficult to analyze. This is in part because of the sheer amount of data that can be gathered and the fact that there are multiple people talking, sometimes at the same time. This means that the recordings probably will take longer to transcribe as the transcriber will have to be clear on who says what at all times (Bryman, 2008).

There are also possible problems with the so-called group effect. Often there will be people who are more inclined to: *[...]hog the stage!"* (Bryman, 2008, s. 489), and those who are more inclined to stay in the background. If the interviewer has given

up to much of the control to the group, it can lead to people not getting to express their perspective.

Lastly, there is a logistic limitation to the focus group. Firstly the date and time needs to be coordinated so all the participants can make it. Secondly, it needs to be at a location where the participants do not feel constrained. It could for example work against the purpose to hold the focus group at one of the participants house as that person could feel relaxed and at home, while the others might feel uncomfortable. Thus a neutral location would be better suited for the purpose.

Routinisation

Before a user can engage in the usage of many ICT-services the user is required to give consent that, they understand the terms and conditions for using the service. This consent is only valid if the user has a sufficient knowledge of the content of the agreement (Ploug & Holm, 2013). There is some evidence that few people actually reads the entire terms and conditions before agreeing to them (Ploug & Holm, 2013). This practice is known as routinisation.

Informed consent is an important concept in the protection of one self. The term implies that the party who consents *"[...] should be given as much information as might be needed to make an informed decision [...]* (Bryman, 2008, s. 694). The consenting party can then freely decide whether they will give consent. In the case of ICT-services, the consent given is legally binding and as such may have large implications as it *"implies that the right to remain anonymous is replaced by a requirement of providing personal information and accepting to some extent the registering and tracking of one's digital footstep."* (Ploug & Holm, 2013, s. 1098).

The can be varying reasons for a user's apparent routinisation in dealing with consent in ICT services. If the user for example declines to read the terms because terms are long then the user has not shown a reflection on how this specific consent will affect the them (Ploug & Holm, 2013). Another reason can be that the user has had the software or application recommended by someone they trust. In this case there may or may not be a degree of reflection, but as the user is affected by something other than their own reflection there may not be an instance of routinisation, or at least not to the degree as described in the first example (Ploug & Holm, 2013). Lastly, there is a chance that users may be affected by the brand name of the software company. If it is a brand, they trust the routinisation may lie in the brand recognition.

Methodology

Scientific Research Methods

In the following chapter, we will discuss the chosen scientific research methods for this thesis. The chapter will be segmented into three sub categories, each describing the trail of thought that lead to the chosen theories. The first segment will describe our initial thoughts and consideration that caused the selection and deselection of the possible theories, which could be deemed usable to answer research, questions of the research questions. In the second segment, we introduce phenomenology and social constructivism as the chosen theories, and discuss our approach and understanding of how these two theories separately may help answer our research questions. Phenomenology and social constructivism are two theories, which normally does not have any correlation. That is why, the last segment will be used to discuss how these two theories may be used together and create a more proficient way to answer the research question, than if one were to be used individually.

Chosing a scientific research method

This thesis uses phenomenology and social constructivism as the primary research methods. These theories were chosen based on a series of considerations, which we will explain in the following.

In this thesis, we seek to understand gain an understanding of the term privacy in correlation to digital data. As previously discussed, we do not believe that there is a definitive definition of digital privacy amongst users. This causes us to approach the concept of privacy as a term emphasizing a subjective individual understanding of what truly is private when creating digital data. To be able to ascertain a temporary definition of privacy we seek to perceive privacy as a contemporary term, which at the same time may also be perceived as a phenomena.

Social constructivism

One of the theories used as the ontological standpoint in this thesis is the theory of social constructivism. Social constructivism is theory originally based in sociology and as the name applies, concerns itself with the construction of social understanding from a philosophical perspective. (Berger & Luckmann, 1966) The results we seek to obtain are heavily based on what we believe to be a joint cultural understanding. With social constructivism, we are able to gain a better understanding of how the average Danish consumer perceive privacy when using a smartphone. When interacting and obtaining empirical data from a predetermined cultural setting, it is also necessary to be able to what part of the empirical data might be due

to a similar cultural background. Accessing the empirical data from a social constructivist approach will enable us to separate the behavior that is caused by interacting with a cultural setting, compared to the behavior, which are unrelated to a cultural setting. In addition, as such be able to find unique factors about Danes view on defining the term privacy.

Social constructivism is based on a long series of different philosophical thoughts on the social construct of reality ranging back to before the nineteen hundreds. However the first clear publication defining the term social constructivism originates back to the release of "*the social construct of reality*" in 1966 **(**Berger **&** Luckmann**)**. The book approaches the understanding of reality, rules, right and wrong as something created over a course of time in a group of people. As such, it dictates that the rules of society is based upon the fact that people gather and create a joint understanding of reality based on their setting. This is seen as argument as to why countries share the same beliefs and understandings of certain aspects, and at the same time why some countries disagree. Berger and Luckmann also argues that "compared to the reality of everyday life, other realities appear as finite provinces of meaning, enclaves within the paramount reality marked by circumscribed meanings and modes of experience" **(1966, s. 25)** which entails that there is no definite correct and wrong, as everything is determined by the circumstances created from the cultural setting. This also creates an interesting notion that there is no such thing as an objective understanding of something, since everything is subject to an individual subjective perception of the world. From an epistemological point of view this also means, that knowledge itself is a social construction created from the interaction of individuals, which afterwards have defined what knowledge itself is. However, fractions of social constructivism can be traced even further back in time to the philosophy of Vygotsky. However, during Vygotsky own work he merely addressed the thoughts as constructivism, which only concerned itself with meaning making though oneself. **(Derry, 2013, s. 45)** As such, we have chosen not to rely on Vygotskys more straightforward take on constructivism, but instead focus on Berger and Luckmanns approach, which emphasizes more heavily on the social construct of culture.

Phenomenology

The second scientific theory used in this thesis is phenomenology. The basic understanding of the phenomenology is seeing the world as a world filled with phenomenon, which we as human beings seek to understand. To be able understand these phenomenon's, one needs to experience them, however there is several opinions about how this may be done. A variety could for example be Merleau Pontys, which heavily emphasizes that to understand the world, one needs to experience it in physical form, as a sort of learning-by-doing approach. It could arguably also be seen as a more pragmatic approach, despite being a theory based from an ontological viewpoint. (Merleau, 2005, s. 405) However because we seek to understand a phenomenon, which we assume originate from a longer period of cultural changes,

we need to use a theory, which is based on physical experiences. As such, we look at one of the founding fathers of Phenomenology, Martin Heidegger and his thoughts on Phenomenology's approach to technology. He argues that the technological universe, as well as the physical universe, both co-constitute each other, one cannot exist without the other, and as such, one must explore the technological world and its phenomenon in coherence with the physical world, to understand it. (Heidegger M. , 1977, s. 7) As such, we perceive the concept of digital privacy, as a phenomenon and in order to understand it, we must research its circumstances, which will enable us as researchers to gain a greater understanding of the things related to digital privacy, including the user, which might be affected by it.

The phenomenological theory originate from Edmund Husserl in the beginning of the nineteen hundreds, when he released the text "Logische Untersuchungen" the basic concept was to experience the world, instead of pondering behind a desk. (Husserl, 1999) Another one of the greatest contributors to the phenomenological trail of thought is Martin Heidegger, which develops Husserl's original philosophical theory, into a more existentialistic-based theory. In which he puts the human being, and the physical world as two units in constant relation to each other, and argues while the world influences humans, so does the humans influence the world. (Heidegger M. , 2008)

Phenomenology and social constructivism

The reason we have chosen to include two different scientific theories in this thesis, is our problem area, which create two different problematics. The first problem we wish to solve, understands digital privacy, which we already described as an ever-changing constant. In order to understand this we approach digital privacy as a phenomenon as described by Heidegger. This is not something we can seek to understand by using social constructivism, since our preliminary research indicated that it was a concept that users belonging to the same social setting, were not able to define.

On the other hand, we seek to understand the users of a specific demographic, in this case, social constructivism enables us with the tools and methodological approach to obtain the possibility of understanding how users in a specific setting might become more aware of the data they share without their knowledge, when using digital devices.

As such, we do not seek to combine the two scientific research methods, but instead use each of them as a way of gaining a greater ontological understanding of the problem area.

Data collecting methods

Interview

. We have conducted interviews with people from different positions inside the case spectrum. A senior lawyer from the consumer coucil "TÆNK" specializing in private data protection and an expert in the field of private data, an app developer situated in Danish App Lab and the press chief from TÆNK. On top of these two interviews, we have carried out a focus group to get the end user perspective. The focus group method will be examined in a later section. We have chosen to conduct unstructured interviews as our interview method. We were aware of the limitations of this method and we tried to mitigate them by knowing the theory behind the method. Firstly we chose on person to act as interviewer to make the otherwise unstructured interviews somewhat comparable.

We have interviewed the experts via telephone as it turned out that setting up the interviews in person showed to be too time consuming for the people involved. As mentioned in the interview theory there are certain constraints when using telephone interviews. Firstly, we tried to keep the interviews somewhat short, as the format is unsuited for long interviews. We also deemed that the interviewees' body language was not an important part of the data and therefore we saw no reason to set up face-to-face interviews instead. Regarding the technical issues that may occur we decided, based on anecdotal evidence from the both of us, that the likelihood of a phone signal breakdown or cutout was small enough to not cause concern. The extra equipment we needed to be able to record the interview through the telephone was downloaded through the Google Play Store. We ran a couple of tests to see if the application would work as intended and after satisfying results, we chose an application.

When choosing the application for recording the interviews, we tried to find an application with a minimum of data retention. The application we chose is the "Automatic Call Recorder" from Appliqato. Although the application requires several permits to install, there is none of them that indicates that the application keeps the recorded calls. We therefore felt that we tried secure that the recordings will not end up somewhere out of the consenting parties control.

The first interview was conducted with the press chief of TÆNK. The unstructured interview was meant to give us an overview of the demographic regarding the TÆNK user base. The interviewer had only a general notion of what we wanted from the interviewee. The interviewer set up the interview by asking the interviewee how he would describe the TÆNK user base. From there on the interviewer asked follow up questions to the parts, he deemed interesting in regards to our case.

The second interview which was set up was with the senior lawyer from TÆNK will be used to clarify what the current legal stand is on private data and how the users stand in this situation. We chose the unstructured interview because we do not

have a specific focus inside the field and as do not have an adequate enough understanding of the legal field to ask the person very specific questions. Therefore, we decided that we had more to gain by letting the expert talk about what the person deemed to be important. As such, we were not going to constrain the persons view of the matter and forcing them in a direction which may be unimportant.

The last interview we conducted was with an app developer. This interview as also an unstructured interview. Again, the reasoning behind this was that we would try to get the developers unconstraint view of data collection and to do that we would have to use this interview format.

The interviews was only partially transcribed, meaning that only the parts we used in the analysis was transcribed.

What could have been done differently?

We could have used a different interview type for the interviews, either a semi-structured or a quantitative interview. This would have had implications for not only the data gathered but also for the process, we would have been through. Had we gone with a semi-structured interview, which is still a qualitative method of interviewing, we would have had to first gather rather specific knowledge in each of the interviewees' field. This would have allowed us to ask more specific questions and the knowledge gained through this would be equally specific. However, as the focal point of the paper is not on the experts' knowledge of the field, but rather the user understanding of private data we decided that the experts would be used to shine light on private data from their perspective.

The other option would have been to conduct quantitative interviews. This method would have required us to conduct enough interviews with comparable persons to be able to generalize their answers. Again, this was not favorable, as we was not looking, for example, on how the app developers as a general entity looks upon private data.

Survey

In the beginning of the project, we investigated the opportunities of collaborating with TÆNK and using their user base to distribute a survey. The reason for this was that we would have access to a number of potential respondents that we otherwise could not hope to reach through our own network. After some initial talks with TÆNK, they told us that they could not help us with distributing a survey that they did not have control. After a while, we were able to reach an agreement where we collaborated on a small survey where we would not get access to the data set, but only the results. Although we were reluctant to do the survey this way, we decided that the data we could get by going through TÆNK, despite the constraints, was better than what we could produce ourselves with the limited time that was left now. This method also meant that we could ignore some of the constraints independent researchers usually face when trying to do a large-scale survey covering a large demographic such as the Danish population. The first was the distribution, as TÆNK would handle that aspect by sending the survey out to their user panel. The

panel consists of 2700 people between the age of 18 and 69. This is a significantly more representative panel than we could have covered, as the main way of sending out a survey of our own would have been through our network. This would have meant that a large part of the survey answers would have consisted of people in our demographic, 20-30 year old university students.

Although the lack of the data set means we cannot look into specific aspects of the survey such as how the age, gender or education may have a influence on how the participants answered we decided that the data would be useful to us anyway.

The survey was partially inspired by a paper that is mentioned in the theory section written by Thomas Ploug and Søren Holm, partially through our own reflections on the subject and partially by informal talks with a researcher at TÆNK who suggested some ideas for questions that they had had good responses to before. The survey consists of nine questions relating to terms and conditions. The first five relates directly to whether the user reads the terms and conditions when using different services. Even though the main focal point of the project is mobile applications, we decided that we needed to include other ICT services as well to uncover if there is a general pattern across platforms regarding the reading of terms and conditions. As the target demographic is Danish, the survey is also in Danish. The five questions was asked as follows:

- 1) Hvor ofte læser du vilkår og betingelser på nettet når du handler på nettet (online supermarkeder, online butikker osv)?
- 2) Hvor ofte læser du vilkår og betingelser på nettet når du er på facebook eller andre sociale medier?
- 3) Hvor ofte læser du vilkår og betingelser på nettet når du bruger apps på telefonen?
- 4) Hvor ofte læser du vilkår og betingelser på nettet når du bruger streamingtjenester (f.eks. Netflix ViaPlay, HBO)?
- 5) Hvor ofte læser du vilkår og betingelser på nettet når du bruger gratis onlinetjenester (f.eks. antivirus, e-mail, dropbox)? (Appendix 1)

With these five categories we felt that we had included the most commonly used ICT services and that this knowledge would give us a more complete picture than a survey focused solely on the terms and conditions regarding mobile apps. B

The other four questions was focused on the participants experience with the online terms and conditions. The four questions are asked as follows:

- 6) I hvilken grad oplever du at vilkår og betingelser på nettet er svære at forstå?
- 7) Vilkår og betingelser kan gøres nemmere at forstå ved at bruge symboler i form af f.eks. smileys, grønne og røde pile. I hvilken grad vil visuel hjælp have indflydelse på, om du læser vilkår og betingelser?
- 8) Hver gang man opretter en profil på nettet, køber en vare online eller henter en applikation ned på sin telefon, skal man acceptere en række

betingelser eller vilkår, som firmaet bag opstiller. I hvilken grad føler du dig tryg ved, at det er disse betingelser og vilkår på nettet der fastsætter dine rettigheder i forhold til din færden på nettet?

- 9) Facebooks nyeste applikationopdatering til mobiltelefoner beder om adgang til at læse dine smsér som en betingelse for brug af appen. I hvilken grad finder du det acceptabelt? (Appendix 1)

The sixth question was included because we found it relevant to examine whether the language of the terms and conditions make it hard to understand and that this could uncover a reason to why the participants may not read the terms and conditions. The reason that *"[...]svære at forstå?"* (Appendix 1) Was the specific parameter chosen and not for example, that the terms and conditions are too long, is that we had both had trouble understanding certain terms and conditions in the past. The following question was supposed to give us an idea of what could be done to make it easier for the user to understand the terms and conditions. The question was developed with the help from a TÆNK employee. The original question consisted only of the last part *"I hvilken grad vil visuel hjælp have indflydelse på, om du læser vilkår og betingelser?"* (Appendix 1). It was then suggested that we gave examples on what we meant with visual aid and the question was expanded. Question eight is partly related to the earlier described concept of routinisation. We were interested in seeing whether the participants had a sense of trust in the companies behind the terms and conditions. We thought about making a question regarding a specific set of companies but decided against it because certain companies create animosity based on their former actions. In the last question, we decided to give a specific example of an app that needs a certain permit for the user to use the app in order to see what response would come of it.

The results of the survey will be examined later on in the paper.

What could have been done differently

With regards to the method as a whole the only thing we could have done that would compare in terms of data would have been to conduct a large number of quantitative interviews and constructed the data from this. However, as far as efficiency goes the quantitative interview method cannot compare to the online survey. The amount of work required to conduct and decipher the interview data and generalize the data would not have been possible with the constraints we as researchers face. Another problem with doing quantitative interviews as independent researchers is finding enough willing people to actually have a valid and reliable data set.

In regards to the specific scenario we faced here with TÆNK, the other option would have been to conduct the entire survey from designing to distribution and data analyzing ourselves. However, as mentioned we valued to have a greater sample size and a more diverse demographic over control of the data.

Focus group

The first thing we had to do was recruit the members of the focus group. As we were looking for a somewhat specific set of people, students in the mid 20's, we

chose to go through our own network as the persona roughly matches our own. The reasoning behind this is that we were looking for a target demographic that roughly matches the demographic in the SensibleDTU as it would seem that the projects participants seems more likely to hand over their data. We would like to see if this is a general thing for a similar, albeit in much smaller scale, group of non-DTU students. Therefore, we recruited three people three degrees of separation from ourselves. As mentioned in the interview theory we made one of the regarding sampling the participants when we chose people we know, no matter the closeness of the relationship. However, as our other possibilities dwindled we chose to invite the participants. We were aware that the data would have been more valid if the participants were strangers but we decided that, as long as we remained aware of potential problems such as the participants trying to please us, we could secure the validity of the data.

We have only conducted one focus group. As the theory states, a single focus group will almost never be enough to obtain the data needed. However, we have chosen to only do with basis in our scientific method social constructivism. We used the knowledge of the method to put together a group that exists within the social setting and as such, we deemed that the results would be very similar across several focus groups, which according to the theory is a waste of resources.

What we planned

We had designed the focus group to consist of two parts. In the first part had chosen four different app categories: QR code scanners, camera apps, note apps and a PDF reader. In each category, there were four apps that varying levels of permits from very few to almost everyone. We would then ask the focus group participants to look at each of the apps and install the one they found most appealing. This would be repeated for each of the categories. After each installation, we would ask what had influenced the participants' decision and instigate a discussion in the group as to why they had chosen the way they did. The participants would not get any information as to what we were looking for. This way we could observe if any of them considered the app permits, terms, and conditions of use.

In the second part, the participants would be handed a piece of paper that would symbolize the install screen of an app from the Google Play Store. We created three apps on paper that most people at least had an attitude the three apps were Snapchat, Facebook Messenger and Mobile pay from Danske Bank. Before the exercise started, we would tell the participants that in this scenario the focus was on their opinions regarding what they would permit a specific app access. They would then be handed a paper app where a set of actual permits would be listed and then told to either let the app keep the permit or deselect the permit. When they had considered all the permits, they could then turn the paper around and look at how their choices would affect the functionality of the app. The paper representation of the app permits would be given to the group and we would ask them to think aloud and discuss why they chose as they did. This would be repeated for each of the three apps. One of the paper representation is seen in the picture below.

Figur 1 The left collum is first introduced to the participants, the afterwards the right collumn is introduced

What happened when conducting the focus group

When we carried out the first part of the focus group, we stumbled upon a major problem within the first few minutes. Two of the three members of the focus group had Apple iPhones. When deciding which apps should be included in the selection we had chosen the suitable apps from the Google Play Store as we are both Android users and overlooked the fact that they might not be available in the iTunes App Store. We had also not made sure that there was a replacement phone for the group members with iPhones. Because of this mistake, we had to change the format of the first part of the focus group. Instead of each member using a separate phone to choose the app, they wanted we handed the group one phone and asked them to inspect the app and agree on which app they wanted as a group. This change in format gave way to some interesting discussions that we would not have achieved otherwise. Of course, the data collected is significantly altered, as the choice of app is a result of group discussion opposed to personal reflection. Because of this we chose to only do the experiment in two app categories, the QR scanner and the PDF reader, for the experiment as the group discussions took significantly more time

than we had allocated and had we done all four we would only have made it through the first part of the focus group. We had promised the participants that the focus group would not take more than one hour and we decided that it would be better to have a shorter first part in order to get through part two as well. When the first part was done, we asked the participants some questions regarding their choice of apps and what had influenced their choice.

The second part of the focus group was not influenced by the mistake in the first part as it was meant to be a group discussion. We started by presenting the experiment to the participants and explained what we wanted them to do. First off we presented them for the Facebook Messenger, secondly the Snapchat and lastly the Mobilepay. For each app, we asked the group to discuss why they would permit the app access to certain data or why they would not give it permission.

What could have been done differently?

Firstly we should have been aware that not all apps are available across the different app stores or at least made sure that we had the right equipment to make up for it i.e. have extra phones so all participants is on the same platform or make sure the apps we had chosen was available in both app stores. The resulting restructuring of the focus group meant we also had to alter our expectation of the results. We had expected to have the individual reflections over the app choice in the first part and although the participants revealed some personal reflections in the group discussion. It would be very difficult to discern what stems from the personal reflections and what opinions is the result of the discussion. Similarly, the second part of the focus group could have been conducted as an individual exercise where each member of the group would have been required to take a personal stance regarding what they would permit the app access to.

If we had chosen to conduct more, even within the constraints we had put in place regarding the age and profession it is possible that we would have had a different data set, but we believe that the results would not differ much from getting more perspectives.

Related works

The following section we will introduce a series of work, which have inspired and influenced this thesis. Prior to the writing of this thesis, we looked into the field of the understanding of privacy. The previously conducted research along with its similarity or different from our original notion inspired our research questions and drive to concern ourselves with this topic. Some of these inspirations were academically based research, whilst other parts based on the media coverage of certain events, and the public reaction along with experts' reaction to these events.

An American nonpartisan fact tank and research center searched to uncover the Americans actual understanding of the term privacy. To do so they made a series of surveys and case studies concerning involving over 600 participants chosen in a diverse setting to represent the general American public. The result was the research paper "*Public Perceptions of Privacy and Security in the Post-Snowden Era*" with the combined effort of 6 senior researchers. The general summary of the survey was that the general American public had different conceptual understandings of what privacy exactly entails, especially in a digital setting. As such they describe that "*when Americans are asked what comes to mind when they hear the word 'privacy', there are patterns to their answers (…) their 'stuff', their solitude, and, importantly, their 'rights'."* (Pew Research Center, 2014, s. 2) Despite this differentiation of whether it is quite clear that the average American feel his or her privacy is at risk, no matter if it existed in the first place. Parts of the survey conducted shows that a whole 91 percent of the survey participants 'agree' that consumers have lost control over how personal information is collected and used by companies. (Pew Research Center, 2014, s. 3) This was particular interesting to us. The survey participants were not agreeing on a definite understanding of digital privacy, yet the participants still agree that they have lost control of it, which could indicate that the American participants share a mutual understanding of digital privacy, even though they might describe it differently. This inspired us to try to see if these results were replicable in a different Danish cultural setting. Both to see if Danish people feel their privacy exposed to the same extent as the American participants in the survey. Secondly if it is possible to trace a similar mutual understanding of a term such as digital privacy, despite describing it differently. There were parts of the research paper, which we assorted such as a strong focus on the public thoughts of being monitored by the government. Instead, we chose to include the most valid parts of the research paper, concerning the mutual public understanding of digital privacy. Combined with the general uncertainty about which private data they may share with companies without their knowledge. Is this concern also present in Denmark and is it possible to help it in any way, with our competences.

For a long period of time the debate about privacy and what digital privacy truly entails in a world, where big data is the new way for companies to earn money, were mostly taking place on American soil. However, last year one of the most popular

social media apps Snapchat was victim to a major attack by hackers. Around 200.000 pictures and videos where obtained by the hackers. These pictures and videos where both normal silly pictures taken by people during everyday things. However, a small portion of the data obtained by hackers also contained pornographic material created by the users of Snapchat. The hackers decided that they wanted to publish all the pictures and videos, which they had obtained, making it publicly available on the internet for everyone to download. This caused a momentary situation of chock between Snapchat users that feared their private intimate pictures exposure to everyone. The panic reached all the way to Denmark, since Danish Snapchat users took some of the pictures that were exposed. Over a hundred Danish news articles were published that concerned the Snapchat leak, and how to find out if you were on the people exposed. (Infomedia, 2015)

Following the Snapchat leak you could track a number of articles concerning, securing data and privacy from a wide range of Danish media and newspapers. One of the most recent actions in the media is the Danish public service company DR, which have lead a weeklong theme with the main topic being 'digital surveillance'. In this particular theme, they try to create increased awareness of which companies as might put you under surveillance as a user, without you even being aware of it. Even the municipal government has admitted that using their site, may put you at risk of sharing some of your data with international companies. Expert in cookies Karsten Rendemann also confirms this in a statement saying: "*Hvis du nu har besøgt et kommunalt website, og cookie registrere, at du nok har uro I privaten, så kan det betide noget for, om du kan få lov til at få et kreditkort, og hvad dine forsikringer skal koste*". (Valsgaard, 2015) While this by itself might come as a surprise to users, an interesting notion would be, to research whether there is any behavior change in users depending on what sort of data they might possible risk exposing. Out of the different takes, DR chose to have regarding digital surveillance the ones that were most popular all included topics regarding digital privacy and behavior, which might put you at risk of losing money. This caused the notion to test if the possibility of profitable gain is an approach that can somehow be a key factor of increasing the average user drive to gain more awareness considering digital privacy. Looking at the Danish user and judging from DR theme on digital surveillance we obtain validation that signifies the average user might indeed be unaware or have a lack of interest, in defending their own digital privacy. The Danish council of digital safety confirms this, the head councilwoman Birgitte Kofod Olsen has previously stated that "*Problemet er, at vi har vænnet os til at bruge cpr-nummeret som en indgangsnøgle til alle mulige ting – ikke bare I det offentlige, men flere og flere private virksomheder burger det til at identificere kunder med, fordi det er en let metode til at holde styr på kunderne"*. (Norre, 2014) In contrast to the worries of the participants in Pew Internets' research, the articles which causes greatest interest at DR might indicate, that the Danish users does not share the same insecurity about their digital privacy, as the Americans.

To summarize some of the main inspirational sources during our research with related works. The research center Pew Internet, have helped us obtain insight in

how the average American relate to the term digital privacy, and at the same time find that it is at risk. The majority agree on this despite division in defining privacy. We want to research whether the same sort of a unsaid mutual understanding is replicable in a Danish set demography.

The first design iteration

The idea to do the design we have come from the initial research we conducted regarding apps and permits. By looking through the Google Play Store, we discovered that many of the apps needed permits that we could not figure out why it needed access to. For example a QR code scanner that needed access to the entire contacts

and phonebook of the user. This got us thinking that either the developer is trying to get all the data possible by requesting access to everything or there were some of the functionalities that crossed over to access permits that you would not normally associate with a QR code scanner.

On this thought, we started developing the first iteration of the prototype we would use in the focus group. We got the idea that there should be a possibility to not give the app certain permits and to make it realistic the consequence would be that if you denied the app a permit you would lose some functionality. For example could you as a user choose to not give the app access to your pictures but in turn, you would not be able to upload pictures through the app or save screenshots. The idea was that during the focus group the users would be handed a piece of paper with the beforehand chosen app on it. Under the apps is a list of the permits the app requires. The user should then select which permits they would have and which they would not. An example of the concept can be seen below:

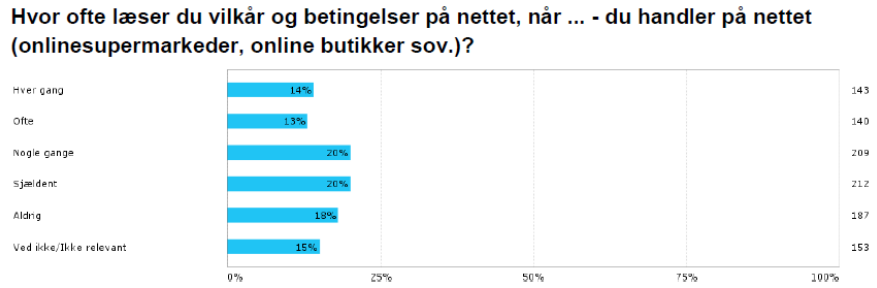
On the left is an example of the page the user would get to see. The apps name and which permits it requires. On the right is the page that the user would see when they were done with contemplating which permits they allow.

Analysis

Analysis of survey data

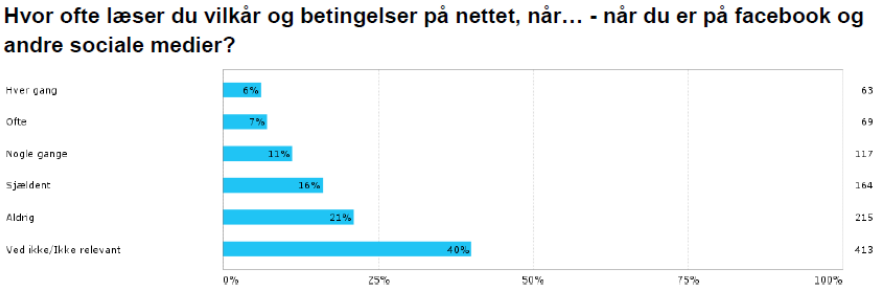
During our cooperation with the user organization TÆNK we developed a small scale survey. The survey was presented to a TÆNKs own user panel consisting of 1.088 respondents altogether which were selected based on the most accurate presentation of the average smartphone user in Denmark. The surveys was separated into smaller individual subjects, the survey were developed with this thesis in mind to gain additional knowledge about the average Danish user's behavior concerning 'terms of service' online. We will now present and analyze the results gathered from the survey.

The first question was asked with the intention of indicating if there are any generalized tendencies when it comes to reading the "terms of service" when using a digital platform. Looking at the answers it's quite diverse when it comes to actually reading the "terms of service" when looking at figure 1 we see an difference with no less than 10 percent in each category. To gain a more detailed perspective of how many actually read the terms of service most of the time, we chose to pair participants answers together which stated that they "often" or "always" read the terms of service. This leads to around 27 percent who often takes the time to read user agreements and terms of service. Excluding the group who chose the "I do not know" choice, we are left with 68 percent who most likely use a digital platform without reading any user agreements. To summarize, about 1/3rd of users actively take their time to read the terms of service judging from the surveys answers.



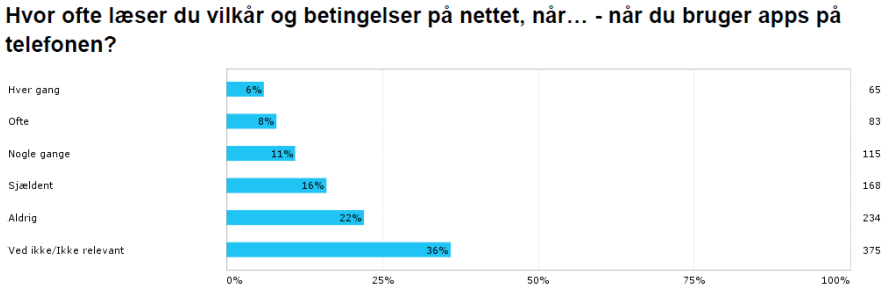
Figur 2

In the next questions we try segmenting the different situations in which the user will be confronted with a user agreement, to see if there is any particular situations where the user is more or less aware of reading the terms of service. Starting with figure 2, using the same form of categorization as the last question we are left with around 13 percent of the participants, which often takes the time to read the user agreements when using social media such as Facebook and similar services. Meanwhile 38 percent rarely or never take the time to read it. In other words 1/4th does not concerns themselves with whether or not social media might do something the user disagree with. The difference when comparing the two questions may be due to the fact, that when people use a digital platform where they use real money they become more worried compared to worrying about whether or not a social media is able to exploit them in any way, as long as it does not involve the risk of losing money.



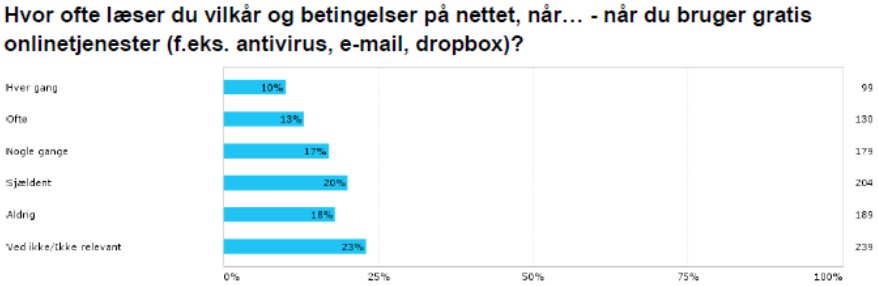
Figur 3

When moving on to the next question and the answers seen in figure 3 it becomes apparent that this might indeed be the case. When asking a similar question as the previous one, but with apps instead of social media we are met with a similar reaction as previously. 14 percent says that they often or always read the user agreements when using apps, meanwhile 49 percent is left in the category of rarely or never reading the terms of service when using apps on their smartphone. Out of the previous cases app usage is so far the case where the smallest amount of people take the time to read what they are agreeing to when using different apps.



Figur 4

The reasoning behind apps being the most common for users to use without reading into terms of service could be due to the fact, that a large number of apps are free and easy to access. Meanwhile you only use an app for a limited period of time before deleting it, you use social media like Facebook over longer periods of time, hence making it more appealing to find out the agreement behind using the social media in the first place. This is also supported when looking at figure 4 that asks the participants about whether they read the terms of service when using free software and apps, such as antivirus, e-mail or file storing services. Like apps, these are free but are more commonly stored and used by the user over a greater time period. In this case, 23 percent often or always reads the terms of service, meanwhile 45 percent rarely or never reads them. Compared to the other examples ½ of the users read the terms of service, when using online services that are most commonly used over a greater period.

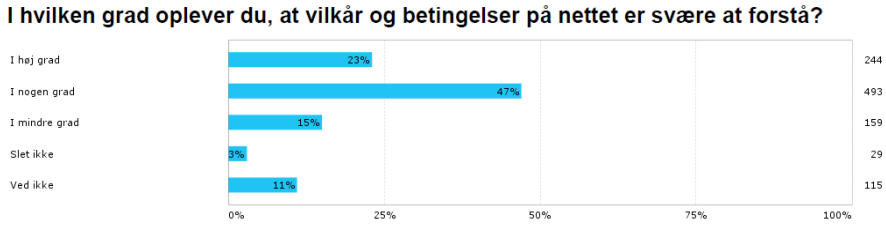


Figur 5

As to why the online services concerns the users the most might be due to the fact that many of the exemplified services functionality concerns certain types of data, which could possibly be deemed as either private or at least non practical for the user to lose control of. Take e-mail for an example, which many people send and receive personal information, may it be work related, personal or something entirely different, you do not want to risk losing control of your e-mail. The same applies for a file sharing service like Dropbox, where the user do not want to risk

suddenly losing all of his or hers stored data. Meanwhile a social media like Facebook typical does not contain the same amount of private data as ones e-mail for an example.

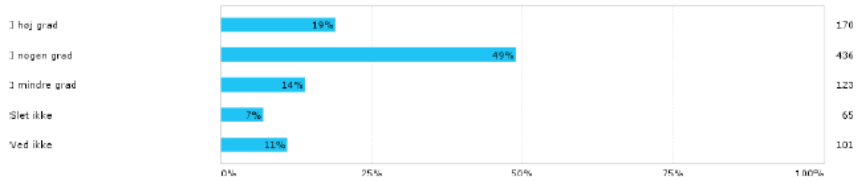
Moving on to the second part of the survey, which focuses on the reason as to why some users might not read the terms of use. One of the first things that might seem like a sensible answer is that the terms of service are too complicated or circumstantial to read for the user to take their time and do it. In figure 5 the participants are asked to what extent, they are experiencing difficulty of understanding the terms of service when using a digital platform. In this case, up to 70 percent experience difficulty understanding the terms of service, meanwhile only 15 percent are experiencing small amounts of trouble and only 3 percent do not have any problems at all. Out of the questions asked during the survey, this is also the one where the smallest amount of participants have chosen the "I do not know" option, which could indicate that of all the questions asked this is the one that is most relatable amongst the participants.



Figur 6

We now have a clear indication that such a large scale of users do not show any interest of reading the terms of service, is due to difficulty of reading the terms of service. In an attempt to gain, an understanding of how it may be possible to make terms of service more accessible to the user we look to the next question displayed in figure 6. The current tendency when looking at the average user agreement and terms of service is that the user is met with several pages of text. Looking at the average Apple user agreement at this moment is 12 pages with worth of text, without counting the additional policies such as privacy policies, which are accessed in a separate document. (Apple, 2015) A working theory of solving the users lacking engagement in taking the time to understand the terms of service might be changeable if summarized in a more accessible format. Out of all the participants, 68 percent were positive about the suggestion of making terms of service more accessible by using visual aid. While only 7 percent declined the idea of visual aid helping with understanding terms of service, deducting the 3 percent that did not experience any problems with terms of service that leaves 4 percent from the amount of participants that said they experienced problems. This could be seen a strong indication that in order to make the average user more aware, a way to summarize the terms of service could be by using visual aid.

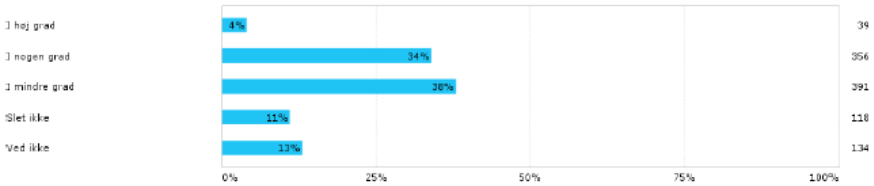
Vilkår og betingelser kan gøres nemmere at forstå ved at bruge symboler i form af f.eks. smileys, grønne og røde pile.
I hvilken grad vil visuel hjælp have indflydelse på, om du læser vilkår og betingelser?



Figur 7

In the next question, we tried to test if the participants found safe agreeing to the terms of service, and whether they found the companies, which terms of agreement they accepted, trustworthy or not. In this question, in particular we experienced a division of the participants. 38 percent found themselves very or somewhat safe when agreeing to different companies' terms of service, meanwhile 46 percent felt somewhat or very unsafe accepting different companies' terms of service. Considering the previous results this question differentiated in the sense that all the other questions would indicate a larger majority feeling unsafe about companies being able to set their terms of service when using a digital platform. One of the reasons for the diversity in the answers might also be because the question does not concern a specific part of using a digital platform as previously mentioned. As such some of the participants might be associating agreeing a companies' terms of service when purchasing a product online, whilst others link it to downloading an app and accepting its user agreement.

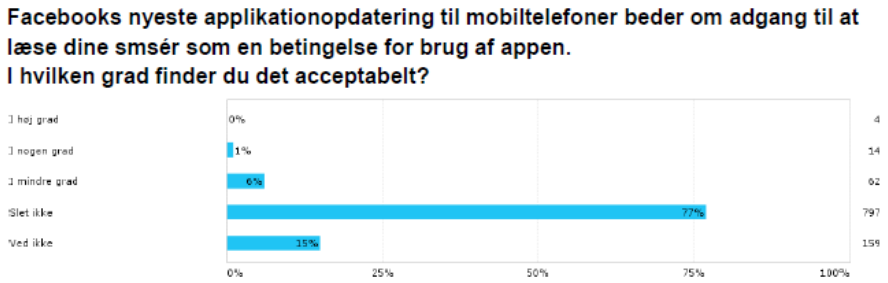
Hver gang man opretter en profil på nettet, køber en vare online eller henter en applikation ned på sin telefon, skal man acceptere en række betingelser eller vilkår, som firmaet bag opstiller.
I hvilken grad føler du dig tryg ved, at det er disse betingelser og vilkår på nettet der fastsætter dine rettigheder i forhold til din færden på nettet?



Figur 8

This point can exemplified in the question followed in figure 8, in which the participant is confronted with an actual example of Facebook using its terms of service to access sms data from the users mobile phone if the user want to download and use their app. When confronted with a clear example the participants an-

swers turns out to be quite one sided, with only 1 percent finding it somewhat acceptable for a company like Facebook to accessing their mobile phones, 6 percent finds it less acceptable the clear majority of 77 percent finds it unacceptable. The one sided answers show a clear indication that the participants might have interpreted the previous question differently. Also indicating that when it comes to private data things like the users text messages are deemed as private when they are not sent via the company's own app.



Figur 9

To summarize the findings of the survey, it differentiate greatly how often the user tend to read the terms of service when they use online services, where they are required to spend money. About 1/4th of the participants read the terms of service each time they shop online. Meanwhile only 1/8th does the same when they use social media. As mentioned this might be due to the user most likely are spending money when shopping online, meanwhile the participant is most commonly not spending any money when using social media. The participants turned out to be less interested in understanding the terms of service required from different apps, which most likely will not be used as much as social media apps, such as Facebook. If the user is instead using apps where they are confronted the risk with losing or giving something up urges them to understand the terms of service. The same is evident when they are at risk of using online stored data stored on either file storing or e-mail services. However even when the user purposely want to look at the terms of service the majority experience problems in understanding them. At the same time the participants find it useful if the terms of service were somehow made more accessible, easier and quicker to understand. A possible approach to this problem would be to visualize the requirements for each individual apps term of service. The group of participants that participated were supposed to represent the Danish public, and while deducting from the answers we find that there is a wide difference in how the participants depict the trust of companies being able to access different information from their users once they accept the terms of service. However when faced with an example of companies accessing personal information such as sms the participants mutually agree that is unacceptable.

With the data gathered from the survey we have gained a great understanding of the average Danish users' thoughts when it comes to understanding terms of service,

as well as their usage of apps. At the same time, they do seem to agree on certain aspects when it comes to privacy, which could signify that the average Danish users may indeed, how a common understanding of what data they deem as private. Looking at these results from a social constructivist viewpoint this could seem connected with the mutual understanding created from being part of the same cultural setting.

In the next section, we will look at a series of interviews to gain a better understanding of the different stakeholders involved when it comes to increase the users understanding of digital privacy.

In the following section, the three different data sets we work with, the survey data, the interviews and the focus group, will presented and analyzed. The reason for that there will be a presentation and walkthrough of the data is that we will make a comparative analysis of the data. This analysis will be used as the base for our changes to the current application permit system.

Interview presentation and analysis

In the following section, we will present the findings from the three interviews. We will look into where the three different people stand on the subject of private data collection through mobile apps.

Interview with the press chief

We start the interview by asking the press chief from TÆNK about the demographic that makes up TÆNK user base: *"Jo altså vi har omkring 70.000 medlemmer og jeg tror sådan set der er de fleste grupper repræsenteret [...]. Dem der vælger at melde sig og abonnere på vores blad, det er jo nok, der er nok en overvægt af bevidste forbrugere."* (Appendix 2).

Later in the interview, the we ask the press chief where he thinks their members stand in regards to protecting their private data. Because TÆNK has been focusing on the issues regarding protecting private data throughout the last couple of years he believes that their members are very conscious about this exact problem: *"Jamen det tror jeg også de er meget bevidste om og det er de fordi vi blandt andet fordi vi har kørt kampagne lige præcis om sådan noget her."* and *"[...] det er noget vi kan mærke, vi har lige indsamlet 10500 underskrifter for en bedre beskyttelse af vores data [...] så det er noget de går meget op i".* (Appendix 2).

As seen in the quotes from the press chief it would seem that the members of TÆNK is aware of the issues with private data.

We then move on to ask what TÆNK want to do in order to better protect the users from getting their data exploited where he confirms that the goal is to get a better law regarding personal data. *"Jamen vi gerne have en lov der beskytter bedre [...] der er en lov fra 1995[...] og vi synes ikke den giver god nok beskyttelse".* (Appendix 2).

As we move on in the interview the press chief mentions that TÆNK has conducted a series of test on apps where a number of them has written in their terms and conditions the company or developer has the right to access certain data and use your personal data. When the user then choose to download the app the user, agree to give access to the data. Shortly thereafter he says: *"Vi har så også en anden undersøgelse der viser at [...] tre ud af fire forbrugere som vi har spurgt [...] læser ikke det med småt inden de downloader en app."* (Appendix 2). This contradicts the earlier statement that the members are concerned about their private data. We introduced the concept of routinisation in the theory section and in the aforementioned quote might show an example of routinisation. We cannot with certainty say that because people do not read terms and conditions they do not care about their personal data. However, we can hypothesize that, when confronted with the issues surrounding private data people will regard it as a problem, but in the day-to-day interactions, they do not care enough about it to try to avoid it. If this is the case then it can be an indication that a strong degree of routinisation is found in the practice of agreeing to terms and conditions.

Further, on in the interview the press chief mentions some of the reasons why routinisation has occurred in the first place:

> *"Sådan som vores liv er indrettet i dag så kan man jo altså,[...] jeg ved ikke om det var nogle nogle amerikanere der lavede en undersøgelse om hvor mange år af sit liv man skulle bruge hvis man skulle læse og forstå alle de her betingelser [...] og hvis du skal læse i svært juridisk sprog [...] vi har sat nogle af vores jurastuderende herinde til det [...] og de havde virkelig svært ved det [...] det var timer de måtte bruge på det."*
> (Appendix 2).

If law students who must be considered capable in the legal language have problems with it, the average user cannot be expected to understand it. He uses this argument to underline why there is a need for a new law

> *"Så er det vores syn på det at der fra starten af er nogle grundregler [...] hvor der ligesom står, at du kan ikke bare bede om at du i al evighed kan tilgå den her forbrugers private oplysninger [...] og det kan du ikke bare gøre på side 131 i svært juridisk sprog for det er sgu ikke i orden."*
> (Appendix 2)

Hypothetically speaking the changes that he proposes, simpler language so the average user can understand the terms and shorter terms and conditions may also help mitigate the routinisation as more people, presumably, would read them. Unless the routinisation has become too much of a habit to get rid of.

To sum up what has been revealed through the interview: The consumer council TÆNK has roughly 70000 members. The fact that the members pay to be subscribed to TÆNKs services lets us know that the members are probably conscious about

their private data. The main problem regarding Persondataloven is that the law is outdated, and this has allowed companies and app developers to take advantage of the lack of regulation lastly we have seen some signs pointing towards the routinisation of consent regarding terms and conditions.

Interview with the lawyer

The former interview revolved around the general problems regarding the way that the current iteration of Persondataloven, and the way developers try to exploit the routinisation of consent by making the terms and conditions unnecessarily long and difficult to understand. The interview with the lawyer will go more in to depth with the problems regarding the Persondataloven.

We start out by asking the lawyer how the current law covers the user regarding their personal data and how the users are exposed. As we have already heard in the interview with the press chief the general problem is that the users are not really cover by the law as the law is from the year 2000 and builds on a set of EU regulations from 1995 *"[...] Overordnet er problemet jo at vi ikke er særlig godt beskyttet i dag fordi teknologien er løbet så stærkt og loven halter bagefter."* (Appendix 3). As the law at current time is more than 15 years old there is a lot of possibilities it does not cover such as smartphone apps, social media and Google. The problem that this represents is that a business practice has evolved around private user data and because the law has not been updated to the evolving technology there is very little regulation *"[...]der har udviklet sig en forretningspraksis, eller forretnings modeller som indsamler forbrugernes oplysninger automatisk hver gang de bruger de her digitale platforme [...] og det er jo slet ikke reguleret."* (Appendix 3). The lack of regulation means that websites and apps does not require consent to start collecting and distributing your private data

> *"[...]altså hele de her regler om at man skal give samtykke til at ens oplysninger bliver indsamlet og videregivet, det sker jo ikke i dag [...]og der er slet ikke nogen der er nået at stoppe op og sige hov [...]*
> *skulle man ikke lige spørge hvad forbrugeren vil her"* (Appendix 3)

And this is down to the fact that the law lacks clarity on the subject because it is old and have not been updated to keep up with the technological evolution. When asked about if there are any data that the developers are not allowed to gather the lawyer questions how Google is allowed to use the method they are currently using?

> *"Vi forstår for eksempel ikke at det der sker på Googles Android platform [...] når du henter en app ned på din telefon [...] giver du automatisk samtykke til at den må hente alle dine private oplysninger på din telefon*

> *lige fra sms'er, lokalitet, kontaker og adressebøger og sådan noget og det, hvis man læser det i Persondataloven forstår man jo ikke kan være lovligt"* (Appendix 3).

The way the lawyer describes the permission system is somewhat wrong. When installing an app through the Google Play Store the app will ask for permission to access certain parts of your phone, it does not automatically grant full access. In the next sentence the lawyer explains why this practice is should not be considered legal concerning Persondataloven *"Det er ikke propotionel og usalig indhentelse og du giver ikke samtykke til det, eller i hvert fald ikke noget klart samtykke."* (Appendix 3). The lack of informed consent the lawyer mentions refers to the permission system Google uses. The developer can request whatever permit they want and the user has no way of choosing whether they want to give certain permissions when installing the app, it is all or nothing. Furthermore, there is a lack of transparency as to why a certain app for example a QR code scanner needs permission to access your phonebook and contact information.

The next issue we ask the lawyer about is how the legal limitations are when you have granted the app permission to access for example your pictures.

> *"Ja der er jo heller ikke nogle grænser [...] når man opretter en profil på Snapchat [...] eller en profil på Instagram og Facebook og sådan noget, så kan det godt være de ikke har en ophavsret [...] over dine billeder og tekst, men du giver samtykke til at de må bruge indholdet."* (Appendix 3).

What happens is that the user gives the app a right to use their pictures, and although the app or the company that owns the app does not have a copyright, you have granted them permission to use your content indiscriminately. The problem with the permission is that there are no regulations in place to keep the company from changing the terms and conditions from what you have originally agreed upon to something different:

> *"[...] men det samtykke det har man måske givet for 10 år siden da du op rettede en profil på facebook og det der så er galt det er jo at så kan de løbende ændre vilkårne som de vil uden at de skal spørge dig igen."*
> (Appendix 3)

In addition, TÆNK believes that this practice is also in violation of the current iteration of Persondataloven. The fact is in the second you install an app or creates a profile the company has access to your data, no matter if you use the app a little, a lot or not at all. On top of this, there is the problem with the IT security. There have been several instances over the last years where databases containing private data have been hacked including but not limited to the iCloud hack and the Snapchat hack. The lawyer voices concerns about Persondataloven regarding this aspect as well. The regulatory demands in the current law requiring the companies to build a

sufficiently safe system are not strict enough and this endangers the user's personal data.

As there are, have yet to come a legal case where the lines for how far the companies can use the data it is not possible to determine in practice, but the boundaries for how much the user must put up with are constantly being pushed (Interview advokat). In regards to the users, the law faces another problem. Specifically that far from all users has a problem with giving up their data through apps while others feel that it has gone too far. What TÆNK is trying to achieve is not to remove the apps and the data collection, but rather make it easier and safer for the consumer to use the apps.

The final segment of the interview is about whether or not we can make the users more aware of what data the app gets permission to if the system was more transparent. As we saw in the previous interview the there was a lack of cohesion between the members of TÆNKs actions and their behavior. They would gladly sign the partition to change Persondataloven, but only 25% apparently worries enough about their data to reads the terms and conditions. The lawyer also expresses these thoughts when recollecting a survey TÆNK has done where 80-90% found it unacceptable that Facebook wanted access to private text messages on the users' phone

> *"[...] når vi forklarer forbrugerne hvad der foregår så bliver de meget kritiske. Grunden til at de ikke er det nu er at det er svært for alle og en hver, også os der arbejder med det at gennemskue den her kompleksitet i teknologien, men også at gennemskue hvad er det man kan bruge de her oplysninger til på sigt."* (Appendix 3).

One of the things TÆNK is aiming for down the road is to secure more transparency so that the consumer has a better chance of figuring out what they are dealing with (Appendix 3).

Therefore, to sum up, there are many problems with the current iteration of Persondataloven. It does not really protect the user from data exploitation. A lot of this comes down to the fact that it has not been updated to keep up with the technological evolution. The lawyer and TÆNK actually believes that some of the practices that Google App store uses in regards to the permission system is illegal. The lawyer expresses some thoughts that we saw in the former interview as well. Specifically that the consumers get very critical of the data collection when told what is actually going on, but because of the complex situation the app companies puts them in.

Interview with the app developer

The last interview is conducted with an app developer. Where the two first interviews has been focused on the users, from a general and a legal point of view, the last interview will focus on the developer side.

The first part of the interview after the introduction is about the thoughts that the developer puts into the asking for permissions. In the answer he gives, he explains

that a certain permission they have included in an app. The permission has is problematic because it warns the user that the application can make a phone call on the users behalf, even though it is a function in the app that allows the user to make a call directly in the app. The interesting part is that the developers reason for wanting to remove the function is that *"[...] fordi at den giver en alarm over for brugeren som kan trigge noget forskelligt og gøre dem yderligere nervøse"* (Appendix 4).

The developer do not want to change the way the current Android permission system works because the end users are, in a very limited degree, concerned with what permission they give away when installing an app (Interview udvikler). He notes that if the users actually knew what they gave an app (using Facebook as an example) permission to collect they probably would not install it and that the large permission list makes the users less aware what they are saying yes to. This would be bad for the users because the developers could potentially use this to get access to every piece of private date by asking for every possible permission. On the other side, this is good for the developers, which he also confirms in the interview (Interview udvikler). The developer does not see a problem with the fact that the users are not aware of what they are agreeing to *"[...] hvis du har bedt om tilladelse til at tage dataen så har du jo bedt om lov til det, men det er ikke det samme som at brugeren har artikuleret hvad det er det faktisk betyder"*. (Appendix 4).

The developer do not experience that the current Persondatalov limits him in development. They are limited more by concern from the users or public focus on the data collection through apps that limits them *"[...] og begrænsningen er nok mere i mulige bekymringer om hvad dataen kan blive brugt til end begrænsninger i lovgivningen"* (Appendix 4). This might suggest that the developer would take all the data he could if there were no focus on the matter.

Comparative analysis of the interviews

Firstly we see that in all of the interviews there have been some mentioning of the users lack of knowledge of what they actually agree to when downloading an app.

The press chief from TÆNK seemed to see is a moral problem as seen in the quote: *"Så er det vores syn på det at der fra starten af er nogle grundregler [...] hvor der ligesom står, at du kan ikke bare bede om at du i al evighed kan tilgå den her forbrugers private oplysninger [...] og det kan du ikke bare gøre på side 131 i svært juridisk sprog for det er sgu ikke i orden."* (Appendix 2). The notion in the end is simply not okay for the app developers to make it deliberately hard for the user to comprehend what they are agreeing to. He even goes as far as swearing.

The lawyer saw it more as a legal issue *"Vi forstår for eksempel ikke at det der sker på Googles Android platform [...] når du henter en app ned på din telefon [...]*

giver du automatisk samtykke til at den må hente alle dine private oplysninger på din telefon lige fra sms'er, lokalitet, kontaker og adressebøger og sådan noget og det, hvis man læser det i Persondataloven forstår man jo ikke kan være lovligt" (Appendix 3).

Lastly the developer did not seem to see a problem in it as the user granted the developer permission to access the data *"[...] hvis du har bedt om tilladelse til at tage dataen så har du jo bedt om lov til det, men det er ikke det samme som at brugeren har artikuleret hvad det er det faktisk betyder".* (Appendix 4). The three different views of what is essentially tells us that there is a strong case for a more transparent way of showing exactly what data is being accessed as the only person to not see it as a problem is the developer who has something to gain from the users blindly agree to handing over their data. The fact that all three people mentioned some signs of routinisation of consent leads us to believe that the behavior is very common.

In the third interview, the developer mentions that the current Persondatalov does not limit him in developing apps. This confirms the concerns voiced in the other interview, namely that the current law offers very little protection for users or in any way regulates the developers. He states that it is largely the public focus that limits them and it is exactly this public focus that TÆNK is trying to create.

In the first interview, it is mentioned that they have collected 10500 signatures on a petition to give better protection of data, which was handed over to Justitsministeriet. Therefore, by trying to get a better and more updated Personatalov TÆNK is creating the public focus that may inhibit the developers.

Participatory design

In this thesis, we have chosen to use participatory design as the theoretical methodological approach when researching and testing the ideas developed during the process of analyzing the empirical data gathered throughout the writing process of the thesis. Participatory Design originate with the intention of involving users in a

testing process, to eliminate potential flaws before the design reaches its final design. In the specific case we have chosen to include, a group of participants chosen based on the demographic used in our related works section, under the sensible DTU segment. The reason being that the demographic match an active user, that actively select or deselect apps, commonly spend several hours of the days using internet driven digital platforms, as such they are faced with a great number of situations each day, where they use apps or tools that requires an user agreement to be used. (Spinuzzi, 2005, s. 164) As such, we will be able to gather a working understanding of what goes through the mind of an average user, when downloading an app, installing it, and agreeing to its terms of service.

What we hope to achieve by doing this is to visualize the hidden intuitive thought processes that takes place when a user interacts with different parts of the app store, due to the nature of the focus group, participatory design will be primarily used in the third stage of the focus group.

Focus group analysis

In this part of the analysis, we will be looking into the results gathered from the focus group. As our empirical data up until now suggests, there is a great difference in how the stakeholders might perceive their users and their behavior around digital privacy. In this following part, we will not be looking at the results from an individual perspective, meaning that we will not compare the results of the workshop before after the analysis is conducted, and then henceforth may be compared to the rest of the empirical data, thus creating a theory based of these results. The focus group consists of three members altogether each with a different geographical background. However one of the criteria from which they are selected, is based on them using a smartphone, and its functionalities beyond a non-smartphones functionalities. At the same time, we have chosen the participants from a younger to match the demography set by Sensible DTU. The difference compared to the Sensible DTU participants, is that these participants have yet to willingly agree to let themselves be tracked at all times. We have chosen to avoid putting focus on the focus group members' individual opinions, but instead approach the analysis based on the observations and thoughts the participants create in cooperation with each other. This is due to scientific research theory chosen earlier in the thesis. Since the overall goal of the thesis is to gain a general understanding of a said, demographic we also find it most reasonable to approach the participants as a group working from the same cultural based understanding of knowledge and reality. That being said we will still pay attention to individual behavior, in the event that one of the participants separates him or herself from the rest of the focus group.

Stage 1

Before the start of the focus group we made each participants fill out a short survey about their currently installed apps, and their habits when using their smartphones in relation to digital privacy. All of the participants had installed some of the most popular social media apps on their smartphones; the apps installed were

identical with the exception of one participant not having Skype, whilst another did not have Instagram. However, all of the participants had installed Facebook, as well as Facebook Messenger and Snapchat, apps, which have detailed terms of use, and collect and access a whole lot of data, which might seem private to some. 2/3^{rds} of the participants stated that they actively think about what permissions they are giving an app before installing it. At the same time, all of the participants have actively said no to install an app because of the requirements needed to install it. However, when it comes to reading the terms and conditions before installing apps, and games none of the participants do it, when asked if they read the requirements before installing anything. Just with the exception of a single participant that states he or she reads it before installing games. These surveys were conducted in order to see if the participants change their statements during the focus group interviews.

Stage 2

The second part of the workshop we the confront the focus group members with a set of task, involving looking through a number of apps with a specific function-

Choice of QR scanners.
QR code reader (TWMobile) – camera, information about wifi, other

QR code scanner (DroidLA) – unit and app history, contacts, pictures/media/files, camera, other

Barcode QR scanner (MooboHalbert) – unit and app history, contacts, pictures/media/files, camera, information about wifi, unit ID, call information, other

Threema QR scanner plugin (Threema) - camera

ality, and then letting them chose one of the following apps. They have the possibility of choosing between three different QR code readers to begin with. The focus group members the look through the three QR code readers together, and the discuss what they find appealing/unappealing in the different apps. At this point in time we consciously decided not to tell the participants to look into, what parts of the phone that different apps want to access. One of the QR code scanners did not require any requirements besides the phones camera to be able to scan the QR code itself. Meanwhile a selection of the other QR scanners had a load of extra requirements besides

Just the camera. However when discussing what app to choice, none of the participants seem to take any notice of what the app actually require, once you agree to the apps terms of service. Instead, their focus is far more focused on the visual presentation of the app. How many stars does the app have, what is the general impression of the apps visual profile, and how many ratings it have, is the things that the participants seem to notice, when discussing among themselves, and which

QR reader they should choose. One of the participants state at one time "*billederne ser rigtigt lækre ud, så tror jeg næsten også at appen må være lækker, den ville jeg vælge bare på at det*". (Appendix 5) This might also create the notion that the participants do not want to engage themselves in reading about the respective app, but instead judge it entirely from a visual standpoint. At the same, another one of the participants mentions that it would be so much easier to choose if one the QR readers were made by Google. When the moderator confront the participants as to why, this would make it easier, the other participants quickly agree with him. "*Hvis det er Google eller Apple, så downloader du det bare ude at kigge nærmere*" (Appendix 5) another interesting observation when looking at the reasoning behind downloading an app without checking what part of the phone it requires access to. From the participants statements it might seem that, brand recognition is more heavily emphasized when building trust followed closely the apps visual presentation. That alongside an expectation of one app from Google or Apple is able to co-integrate with other apps from the same developer, which once again moves the focus back to functionality that seems to be playing a large role in whether or not people concern themselves with their own digital privacy. Another point stated by one of the recipients is the fact, that the first visible reviews on the apps store page, also plays a role in whether or not the app seems appealing at first. However, this works both ways, if the reviews are extraordinarily good or bad, it creates a strong first impression from the users' perspective.

Moving on to the next part of stage 2, the participants are faced with a similar task, however instead of a QR reader; they are now listed with a series of PDF readers. The participant were faced with the following choices of PDF readers. As the previous test, they were only presented with the apps name, not the different functionalities to which it requires access.

Choice of PDF scanners:

Polaris office + PDF (infraware inc) – in-app purchases, unit- and app history, identity, contacts, pictures/media/files, information about wifi, information and Bluetooth, unit- and call information, other

Google PDF viewer (Google) – identity, pictures/media/files, other

Foxit mobile PDF (Foxit software) – in app purchases, pictures/media/files, information about wifi, unit id and call information, other

PDF tools lite (Ashk) – Picture/media/files

The reactions are the same as when given the choice of QR reader. What seems most important to the participants are still the whether they know the company brand behind the app or not. Followed by the general visual impression left at the apps store page. "*Jeg synes ikke at billeder for PDF tools lite er så tiltalende, så den vil jeg nok vælge fra*" one of the participants argue, while the rest of the group does not seem to find least unsafe app appealing at all. "*Man ved bare, at når der står lite, så er det hverken lite eller gratis*," one of the participants, argue, and the others nod in agreement. (Appendix 5) Since there has yet to be any of the participants concerning themselves with the terms of service, and mention if they make any difference in what app they would chose to install, we decide to ask them. The moderator ask whether it has any significance what permissions an app requires access to. All of the participants agreed that one of the most problematic permissions an app could ask for was to connect with Facebook. This could be due to the app would be seen as trying to intrude in the users social life on the social media, which might make it harder to separate if the user should ever wish to uninstall it. This argument is supported by one of the participants answering, the same question with, "*jeg er altid nervøs for, at den skal få min mail, og jeg skal få alt muligt spam*". (Appendix 5) In order to make the participants discuss and consider what makes them care less about the other requirements, that the app requires to be able to function, we now present them with different functions, that the apps they just installed, requires to be able to function. When first presented with the additional access the need to function, one of the participants immediately questions "*hvornår bliver jeg præsenteret for, at de har data bliver indsamlet uden at jeg ved det?*" (Appendix 5) This also indicates that despite having downloaded and used apps several times according to the answers in the survey, the participant has never discovered the additional data an app might obtain from him. The same participant then adds, "*hvis app'en ikke gør mig opmærksom på det når jeg har hentet den med en popup eller lignende, så vil jeg aldrig give det en tanke*". (Appendix 5) Meanwhile the other participants nods in agreement. This could be a sign that the user does not pay close attention when downloading and installing the app, in contrast to the arguments

made earlier in this thesis. The participants also agree that if the app is from a company, which already have apps installed on their phones, they do not think twice about installing the app. "*Hvis det er et firma jeg allerede har apps fra, så har de jo i forvejen alt om mig, så kan det være ligemeget*", one of the participants states. (Appendix 5) so another mutual agreement is that the participants place a large amount of blind trust in the more well known companies, that already have apps installed on their phones.

Stage 3

In the third and final stage of the focus group, we now present the temporary design prototype to the focus group. The participants are faced with an application, which they all have installed on their separate Smartphones and are asked to pretend they are installing it for the first time. Additionally they are now faced with the possibility of actually seeing, which parts of the phone the app requires access to when installed. They must now come to an agreement on which parts of the smartphone they wish to allow the app access. The participants are initially presented with the left column of the figure bellow. They all quickly agree that contacts is a necessary feature to be included when downloading the app, but all agree to disable location, one of the participants argues that she does not like being tracked, while the remaining does not want it enabled since they seldom use it for anything. However, they all agree that if it was a requirement to enable location they would all enable it. One of the participants states "*igen, det er et kæmpe firma, hvis de har brug for det, og det skal fungere, og i har den nok allerede i forvejen*". (Appendix 5) Once again, the participants agree that being a big well-known company grants you credibility when requiring special services to be able to use the app. An interesting notion is the fact that all of the participants agree that Facebook already are tracking them, whilst none of them seem to find it problematic.

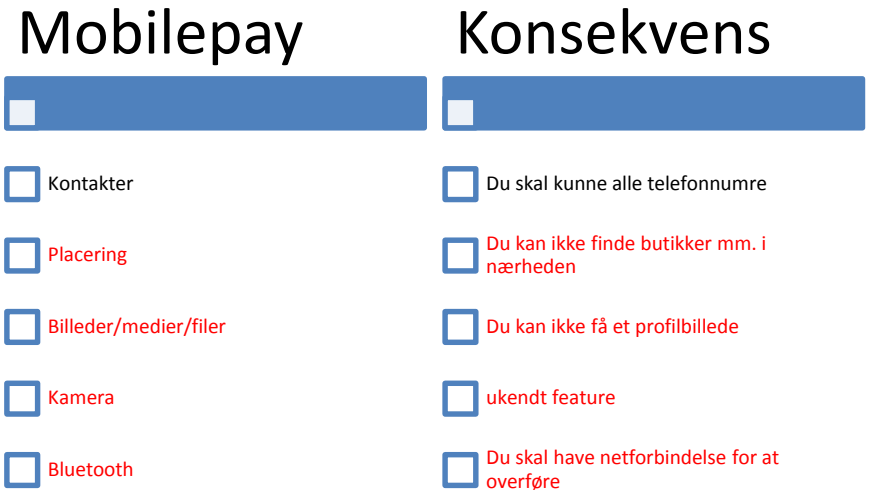
Figur 10

The next step is presenting the participants for the second column; they now have the opportunity to modify their choices, now that they know the consequences. Though when presented with the consequences none of them feel like changing their answers.

Moving on to the next app, Snapchat we follow the same procedure as with Facebook Messenger. The participants quite quickly decides that they do not want to limit the apps access to anything besides contact information. The moderator asks the participants whether they feel that Snapchat is an app they would deem as trustworthy. There is a mutual agreement that neither of the participants trust Snapchat as a company that will secure their data. "*Jeg stoler ikke på dem, men så tænker jeg til gengæld over hvad jeg bruger app'en til"* one of the participants states. (Appendix 5) In addition to this statement the others agree, and one of the other participants adds "*jeg ville aldrig turde sende meget intime billeder, af den grund hvis det havnede på nettet*". (Appendix 5) So we see quite a clear image of the participants does not trust Snapchat, but also that they do not trust that your privacy is safe whilst using a smartphone. This could also support the notion that the participants do not find that data can ever be truly private when using a digital platform. One of the participants making the point "hvad kommer på nettet bliver på nettet" backs this sentiment. (Appendix 5) When faced with the actual consequences of the different agreements, none of the choices changed, they chose to keep the tracking of contacts a disabled feature.

Figur 11

Moving on to the last of the apps, the participants face a different app compared to the two others, the app mobile pay, which is used to transfer money between its users. Compared to the two previous apps we see an entirely different pattern when it comes to the selection of functions. The participants agreed to deny the app access to all functions except the ability to go through their phones contact information. The participants reason this choice because of the apps function, simply is to send money, and additional functionality, such as finding nearby friends for at faster transfer is deliberately deselected, because "*så vigtigt er det heller ikke, det kan I hvert fald sagtens undværes*". (Appendix 5) Now despite Mobile Pay having a limited range of use compared to an app such as Snapchat, it is still quite unusual for the participants to deselect all the possible additional functions in the app. What makes this especially unusual is the fact, that out of all the apps, all the participants agree that they completely trust Mobile Pay, because its owner is a large Danish bank. One would argue that since they do not let the app access all of the required functionalities, they do not truly trust it, despite saying the opposite. This could be related to the fact that the apps entire purpose is dealing with money, a factor that might push the user into taking extra precaution, even when trusting the company more than other apps that have access to more functions.



Figur 12

In the end, the participants are asked about how much thought in general they put into protecting their data, and what sort of data their app usage might generate for the companies owning the different apps. They all agree that the mostly take their privacy and sharing of data into consideration, when the app somehow confronts them with the need to access the data. For an example if the app needs to activate GPS, or a similar feature on the phone. In this case, their decision is based on how much they trust the app in general, and whether or not it makes sense for the app to access the feature. "*Jeg tænker det udelukkende ud fra, hvor meget jeg*

stoler på app'en, og på hvor meget mening det giver, at de skal vide hvor jeg er nu for eksempel, og hvor meget jeg egentlig har brug for den app". (Appendix 5)

Despite the feature not being taken used to such an extent as originally planned during the first iteration of designing a visual aid of understanding, what different functionalities the app accesses and why, the participants were still positive about the idea. One of the participants mentions that he often seek for an easier way to understand, why his app suddenly need to enable different phone functionalities such as Bluetooth. "*nogle gange så famler du i blinde, hvad betyder det at jeg slår bluetooth fra."*

At the end of the focus group, we confront the participants with a question about their personal data, and who they think have the claim to the private data they may store in different companies care, when using their apps along with their smartphones. All of the participants says that they are aware, that a company like Google have access to all of their data, and might even be using it without their knowledge. However, they also feel that they still have the final jurisdiction when it comes to their own private data. Though they all agree that even they might not know how this data is being used, it does not bother them, as long as they are not directly confronted with it.

We will now summarize some of the findings in the analysis of the focus group. First set in relief to the thesis scientific research method all of the participants were able to obtain a mutual understanding of each of the questions asked throughout the focus group. There was not any question, which they strongly disagreed with each other, nor be able to come to a mutual agreement on their answers. In general, there were several occasions where they gained a new understanding of the questions asked, once they started sharing each ones opinion. Considering the term digital privacy, they all agreed, that even though they wished for their private data to not be shared with different companies, it was not possible. Hence increasing the notion that digital privacy is not something that is possible of obtaining, but rather a phenomenon you strive and hope to achieve.

In the third part of the focus group, we subtly tested our research design, in an attempt to test if the user is interested in actively assorting certain features when installing apps. The participants found the idea appealing and interesting, but at the same time disliked the idea of having to select or deselect features when installing the app."*Jeg tror næsten hellere jeg vil skulle gå ind og vælge det fra bagefter, en til at starte med*" one of the participants noted. (Appendix 5) This could indicate that instead of facing the user with the requirement of choosing, which features to enable or disable from the moment he or she installs the app, they should be able to access the function once the app is downloaded. At the same time the participants made it clear, that it should not be a necessary option each time opening an app, but rather an option made available for everyone during all times.

Now that all of the empirical data have been analysed we move onto the last part of the data analysis, in which we compare results of each of the different data sets, and combine the results into gain an understanding that can lead us closer to answering the final research question.

Comparative analysis

Now that we have analyzed all of the collected empirical data, we move on to the next stop of comparing it all with each other. This is done in order to obtain new knowledge and see if there is any recurring tendencies, which could make it possible to make any sorts of generalization that could help answering the research questions.

First of all looking at the terms of service, which was heavily emphasized in the survey, it is made quite apparent that the average Danish user is having a hard time understanding, what the common apps terms of service exactly entails. Despite the user not having much interest in the terms of service in general, several things strongly indicate, that it is still something that the user would find relevant, if it was more accessible. Several things throughout the empirical data indicate this. For a start, neither the survey participants nor the focus group participants found the terms of service interesting. However, as we could see in the survey, when the users are met with an example of what the terms of service allows an app like Facebook Messenger to do, 77 percent clearly indicate that they do not find it suitable for an app to collect SMS data. One could argue that this is an example of how great an amount of data are actually collected, which the user would find inappropriate if they knew that it was going on. The surveys' question regarding, whether the user felt safe knowing that the terms of service are able to dictate their rights online, also shows that the user are uncertain about what this term of service actually entails. Seeing as 70 percent is placed feeling somewhat safe and somewhat unsafe, accepting terms of service when using online services. This is also evident in the focus groups where the participants feels that they own the data they produce or store, when using different companies apps. However, as the interview with Annette Høyrup revealed, the user does not own anything at all. Her notion about users being unaware of this is supported when looking at the uncertainty of trust, in both the focus groups and the survey. At the same time interview with the app developer confirms, that the developers are able to collect the data from the users they want, as long as the users are using their apps.

One the more unexpected results discovered during the analysis was how greatly the users' trust affected their behavior, when it comes to certain apps or companies. An example being the focus group participants when asked to install a PDF reader. All of the participants agreed that almost nothing would make them choose a different PDF reader, once they discovered that one of the options where developed by Google. Despite one of the alternatives needed far less requirements to function. One of the reasons for this could be that, the users have positive experiences using the apps created by Google, thus trusting the same thing to be the case when using the PDF reader. All of the focus group participants agreed that their reason for choosing google was based on trust. However, one could argue that there might be another reason. Looking at stage number three in the focus group, in which the participants could select or deselect certain features from an app. The participants were given the option of modifying the application Mobile Pay. All of them agreed that out of all the possible apps to access, this one was by far the most trustworthy. Yet

still, it was the app, which the deselected the most functions, despite trusting it the most. This could indicate that the user in fact does not trust apps in general. However, when dealing with apps that involves a risk of losing something more relatable than your private data, the user find it less trustworthy. The same tendency is present in the first question of the survey, where the question concerns shopping online. Out of all the questions asked considering the terms of service that is the one where most people tend to read the terms.

During the empirical data collection, there are many situations where the users express that they are aware, most of their data collected without their knowledge. Which also makes it relevant to consider, whether a more approachable way of understanding what data are being gathered, when users are using different apps, is going to change their behavior. However, if we were to conclude from the previous argument about trusting in an app or company, it is possible, that if the user is able to obtain more transparency, about what sort of data an app is collecting, they will slowly transcend into being more selective before even installing their apps.

That leads to the results from the first prototype of an easier way to visualize what an app actually uses in its different requirements. The original idea of summarizing and apps terms of service, by using a simplistic visual approach were considered throughout the analysis. The initial idea of making the prototype based on when the user were about to install and app, was supported by the survey. 68 percent found the idea appealing, thus confirming that it was indeed something that might appeal a user installing an app. However, when we tested the paper prototype in practice during the focus group, a number of potential flaws became evident. As the routinization theory suggested user become annoyed when it becomes too circumstantial to repeat the same pattern several times. Applying the prototype before the download of an app conflicts with this idea, which also became apparent during the focus group. The participants expressed that they would find it too circumstantial to choose, which functions to enable or disable each time you install an app. The problem might possibly be solved, if instead of confronting the user before downloading the app, the user is able to access it after the download. Although this also creates the risk, of fewer users noticing this feature and not being as impactful, as when confronted during the download.

Conclusion

In the process of answering how the users understand data privacy and whether it is possible to change user behavior through raising awareness of the matter, we have obtained knowledge about a number of things.

Using data collection methods, we have been able to gather a wide range of empirical data, making it possible to gain knowledge concerning the problem area. By using surveys we have revealed that a significant portion of the sample representing the Danish demographic have a hard time understanding the terms and conditions of common ICT -services. This leads to a large amount whom rarely reads them, thus risking losing the legal right to their own personal data. The research results indicates that these two are linked together and that more people would read them if the content terms and conditions was made more accessible to the consumer.

A series of interviews with various experts and stakeholders, have enabled us in gaining an understanding of the different stakeholders that might influence the users experience, when using apps.

Using design theory, we have created a prototype that enables the user the gain a deeper understanding of apps technical requirements. Afterwards testing this prototype in focus groups leading to modifications to the final research design.

By using comparative analysis we have compared the different types of datasets and become able, to deduct that is possible to make the user more aware when using digital devices using a more visual research design. In additional result, we have discovered a tendency that might indicate the users' awareness decreases when using multiple apps from the same developer, and as such making the user more vulnerable.

Discussion

Through the project all the data we have collected have had one thing in common - the fact that a majority of users do not read the terms and conditions when installing applications. There are several different reason for this phenomenon. The fact that with the spread of digitalization the amount of terms and service agreements a user would have to read is overwhelmingly large and that the agreements are often written in a difficult language. As we have mentioned the user are not that well protected with current legislation on the subject. Because of this, we mean that a more transparent method for the user to precisely determine what data the apps they install has access to would be advantageous. This could potentially make a large difference in what apps would be installed. As the interviewed developer stated it is more than likely that people would not install Facebook if they knew how much access and control over private data they get. By designing a transparent method the users for the users to both view what data an app gets access to, and also giving them the opportunity to deselect certain permissions, perhaps at the cost of some functionality, it may be possible to increase the users control of their data.

An alternative approach to understanding digital privacy could be to involve the users more actively in trying to define a general concept of the term. This thesis approached digital privacy, as a term that too contemporary to be able to define in a Danish demography. Making it a more active part in the empirical data collection, could potentially have proven for it to be possible. One could argue though, that the previous research conducted in America were not able to find a definite answer, all users could relate too.

One thing is what we have deducted from the data; another thing is whether it is probable that it would have an effect on the user behavior. Both the survey data and the interviews has shown that when confronted with the fact that apps collect data from them there is a rise in awareness and critical thinking regarding data collection. As such, there is a chance that if the users are confronted with it every time they install an app we can change their behavior. Of course, even with a more transparent system we still run the risk of the act falling victim to routinisation once again. However, there are several other perspectives to discuss; regarding whether the research design created in this thesis, is a valid option in the future or not. The main concern is that the research design is a fraction of a redesign of the app store for smartphones. As such, a company like Google should be able to see a sort of profit to limit their own access to the very data, which they have become one of the largest companies in the world. After all, if they do not want to implement the feature it will be near impossible to make available for the average user, which were the target

group of this thesis. An argument in favor of Google potentially accepting the research design or a similar design into the app store design would be an increase in goodwill to their users. There is also the possibility that by making the terms of service easier to understand, that more users will more willingly accept new features.

Looking back at the process we have been through, we have discovered things that could have been conducted better. It has been mentioned in the method section, but the fact that we collaborated with TÆNK on the survey severely limited the amount of knowledge we could have otherwise gained with a survey conducted entirely by ourselves. We would likely have had a much less diverse dataset but the fact that we theoretically could have considered every factor and deduced conclusions from it. It would have helped us to design a better product to know if there for example was a difference in how the collecting of private data differed from young to old, from one gender to another or if the educational level had a saying. A future project containing a survey will almost certainly be conducted by ourselves, or we would make sure that we had full access to the entire dataset. However the advantage of collaborating with TÆNK was to be able to access their vast user panel, a survey with over 1000 participants would normally be something that were too expensive for our research funds to cover.

An important consideration when considering the physical conditions of our research design is that the focus group were conducted with paper mockups of the app permits. This might also have a limiting effect on the results from that stage of focus group, considering the participants were not using smartphone like the one they normally would do, when accessing an app in the app store. Actual mobile interface could have given us the opportunity to observe the users interact with our design in a more natural way than it was case in the project.

One of the results was that users react differently around certain apps, which somehow involves a risk of them losing something. One of the example being Mobile Pay, that the users indirectly showed very little trust, whilst still thinking of it as the most trustworthy type of app. An interesting aspect would be to research ways to make an app trustworthy towards the users. Alternatively research the conditions concerning the trust of apps in general.

Bibliografi

Apple. (05. 05 2015). *Apple user agreement.* Hentet fra Apple: http://images.apple.com/legal/sla/docs/iOS81.pdf

Berger, P., & Luckmann, T. (1966). *The Social Construction of Reality.* Anchor Books.

Bryman, A. (2008). *Social Research Methods*. New York, USA: Oxford University Inc.

Derry, J. (2013). *Vygotsky - Philosophy and Education.* Wiley-Blackwell.

Heidegger, M. (1977). *The Question Concerning Technology.* New York: Garland Publishing.

Heidegger, M. (2008). *Being and time.* New York: HarperPerennial/Modern Thought.

Husserl, E. (1999). *The essential Husserl: basic writings in transcendental phenomenology.* Bloomington: Indiana University Press.

Jalner, M. (1 2014). *Politiken*. Hentet fra Big data vil vende op og ned på din verden: http://politiken.dk/magasinet/feature/ECE2172327/big-data-vil-vende-op-og-ned-paa-din-verden/

Kvale, S., & Brinkmann, S. (2009). *Interview.* Gyldendal Akademisk.

Levy, K., Marwick, A., & Boyd, D. (14. 5 2014). *Privacy and Harm in a Networked society*. Hentet fra Datasociety: http://www.datasociety.net/initiatives/privacy-and-harm-in-a-networked-society/

Merleau, P. (2005). *Phenomology of Perception* . Routledge.

Norre, J. (1. 5 2014). *DR*. Hentet fra Rådet for Digital Sikkerhed: For mange har adgang til vores personfølsomme oplysninger: http://www.dr.dk/nyheder/viden/tech/raadet-digital-sikkerhed-mange-har-adgang-til-vores-personfoelsomme-oplysninger

Pew Research Center. (2014). *PewInternet.* Hentet fra PewInternet: http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf

Ploug, T., & Holm, S. (30. October 2013). *Routinisation of Consent in ICT services*. Dordrecht, Holland: Springer Science+Business.

Spinuzzi, C. (2005). *The Methodology of Participatory Design.* Applied Research.

Valsgaard, M. (16. 3 2015). *DR*. Hentet fra Ekspert: Dine internetvaner vil bestemme prisen på din forsikring: http://www.dr.dk/Nyheder/Indland/2015/03/16/073314.htm

Pensum litteraturliste 7. semester

Clarke, A. E. (2003). S*ituational Analyses: Grounded Theory Mapping After The Postmodern Turn.* Symbolic Interaction, 26(4), 553–576.

Creswell, J. W. (2008). *Grounded Theory Designs. In Educational Research: Planning, Conducting, And Evaluating Quantitative And Qualitative Research* (pp. 431–455). Upper Saddle River, N.J.: Pearson/Merrill Prentice Hall.

De Certeau, M. (1988). *Walking In The City. In The Practice of Everyday Lif*e (pp. 91–111). Berkeley: University of California Press.

De Laet, M., & Mol, A. (2000). *The Zimbabwe Bush Pump: Mechanics of a Fluid Technology*. Social Studies of Science, 30(2), 225–263. doi:10.1177/030631200030002002

Dourish, P. (2001). *A History of Interaction. In Where the action is: the foundations of embodied interaction* (pp. 1–23). Cambridge, Mass.: MIT Press.

Dourish, P. (2004). *What we talk about when we talk about context.* Personal and Ubiquitous Computing, 8(1), 19–30. doi:10.1007/s00779-003-0253-8

Engeström, Y. (2007). In K. Illeris (Ed.), *Læringsteorier: seks aktuelle forståelser* (pp. 81–110). Frederiksberg: Roskilde Universitetsforlag.

Goldkuhl, G. (2012). *Pragmatism vs interpretivism in qualitative information systems research.* European Journal of Information Systems, 21(2), 135–146. doi:10.1057/ejis.2011.54

Latour, B. (1999). *A Collective of Humans and Nonhumans. Following Daedalus's Labyrinth. In Pandora's hope: essays on the reality of science studies* (pp. 174–215). Cambridge, Mass: Harvard University Press.

Mingers, J. (2001). *Embodying Information Systems: The Contribution Of Phenomenology*. Information and Organization, 11(2), 103–128. doi:10.1016/S1471-7727(00)00005-1

Rabardel, P., & Bourmaud, G. (2003). From computer to instrument system: a developmental perspective. Interacting with Computers, 15(5), 665–691. doi:10.1016/S0953-5438(03)00058-4

Rogers, Y. (2004). New Theoretical Approaches for Human-Computer Interaction.
Annual Review of Information Science and Technology, 38(1), 87–143. doi:10.1002/aris.1440380103

Rogers, Y. (2011). Interaction Design: Beyond Human-Computer Interaction (3rd ed.). Chichester, West Sussex, U.K: Wiley, 222-268, 317-351, 476-504.

Star, S. L., & Griesemer, J. R. (1989). Institutional Ecology, `Translations' and Boundary Objects: Amateurs and Professionals in Berkeley's Museum of Vertebrate Zoology,
1907-39. Social Studies of Science, 19(3), 387–420. doi:10.1177/030631289019003001

Sutko, D. M., & de Souza e Silva, A. (2011). Location-aware mobile media and urban sociability. New Media & Society, 13(5), 807–823. doi:10.1177/1461444810385202

Weiser, M. (1991). The computer for the 21 century. ACM SIGMOBILE Mobile Computing and Communications Review, 265(3), 94–104. doi:10.1145/329124.329126

Wenger, E. (2000). Communities of Practice and Social Learning Systems. Organization, 7(2), 225–246. doi:10.1177/135050840072002

Pensum litteraturliste 8. semester

Akrich, M. (1992). *The De-Scription of Technical Objects*. In W. Bijker and J. Law (Eds.) Shaping Technology, Building Society: Studies in Sociotechnical Change. Cambridge, Mass, MIT Press: 205-224.

De Lusignan, S., Wells, S. E., Hague, N. J., & Thiru, K. (2003). *Managers See the Problems Associated with Coding Clinical data as a Technical Issue whilst Clinicians also See Cultural Barriers.* Methods Inf Med, 4/2003(42), 416–422.

Dent, M. (1990). *Organisation and change in renal work: a study of the impact of a computer system within two hospitals*. Sociology of Health and Illness, 12(4), 413–431. doi:10.1111/1467-9566.ep11340410

Ewenstein, B., & Whyte, J. (2009). *Knowledge Practices in Design: The Role of Visual Representations as `Epistemic Objects'*. Organization Studies, 30(1), 07–30. doi:10.1177/0170840608083014

Floridi, L. (2011). *The Philosophy Of Information*. Oxford; New York: Oxford University Press.

Jackson, P., & Moulinier, I. (2002). *Natural language processing for online applications: text retrieval, extraction, and categorization*. Amsterdam/Philadelphia: Benjamins Publishing Company.

Kalbach, J. (2007). *Designing Web navigation (1st ed.).* Beijing: Sebastopol O'Reilly.

Latour, B. (2008). *A Cautious Prometheus? A Few Steps Toward A Philosophy of Design (With Special Attention To Peter Sloterdijk*). Keynote lecture for the Networks of Design meeting of the Design History Society Falmouth, Cornwall, 3rd September 2008 Bruno Latour, Sciences-Po.

Leonardi, P. M., & Barley, W. C. (2011). *Materiality as Organizational Communication: Technology, Intention, and Delegation in the Production of Meaning*. Cresskill, NJ: Hampton Press

I T. Kuhn (Red.), *Matters Of Communication: Political, Cultural, And Technological Challenges To Communication Theorizing* (s. 101–122). New York: Hampton Press.

Levene, M. (2010). *An Introduction To Search Engines And Web Navigation (2nd ed.).*

Hoboken, N.J: John Wiley.

Morville, P. (2007). *Information Architecture For The World Wide Web (3rd ed.).* Sebastopol, CA: O'Reilly.

Pollock, N. (2005). *When Is a Work-Around? Conflict And Negotiation In Computer Systems Development.* Science, Technology & Human Values, 30(4), 496–514. doi:10.1177/0162243905276501.

Redström, J. (2006). *Persuasive Design: Fringes and Foundations*.

I W. A. IJsselsteijn (Red.), *Persuasive technology: first International Conference on Persuasive Technology for Human Well-Being*. PERSUASIVE 2006, Eindhoven, The Netherlands, May 18-19, 2006: proceedings (s. 112–122). Berlin ; New York: Springer.

Redström, J. (2008). *RE:Definitions of use*. Design Studies, 29(4), 410–423. doi:10.1016/j.destud.2008.05.001.

Rogers, Y. (2011). *Interaction design: beyond human-computer interaction (3rd ed.).* Chichester, West Sussex, U.K: Wiley.

Saffer, D. (2010). *Designing for interaction: creating innovative applications and devices (2nd ed.)*. Berkeley, CA: New Riders.

Pensum litteraturliste 9. semester

Abbott B. B. and Bordens, K. S., (2011). *Research Design and Methods - A Process Approach*,. USA: McGraw-Hill.

Bordens, K.S., Abbott, B. B. (2011). *Research Design And Methods: A Process Approach, eighth edition*. USA: McGraw-Hill.

Clarke, A. E. (2003). *Situational Analyses: Grounded Theory Mapping After the Postmodern Turn Reviewed work(s)*. Symbolic Interaction, Vol. 26, No. 4 (Fall 2003), pp. 553-576. Wiley on behalf of the Society for the Study of Symbolic Interaction

Finlay, J., Abowd, G. D., Beale, R. (2003). *Human Computer Interaction, 3rd Edition*.
Prentice Hall, 2004. ISBN 0-13-046109-1.

Foth, M. & Axup, J. (2006). *Participatory Design and Action Research: Identical Twins or Synergetic Pair?* Participatory Conference (PDC) – Trento, Italy.

Hearn, G. N. and Foth, M. (2005) *Action Research in the Design of New Media and ICT Systems*. In Kwansah-Aidoo, K., (2004) (Ed.) Topical Issues in Communications and Media Research, pages pp. 79-94. Nova Science.

Kelly, A. E. (2008). *Handbook of Design Research Methods in Education: Innovations in Science, Technology, Engineering, and Mathematics Learning and Teaching.* New York: Routledge.

Kuniavsky, M. (2003). *Observing the User Experience: A Practitioner's Guide to User Research*. USA: Morgan Kauffman Publishers.

Moreira, M. E., Lester, M., Holzner, S. (2010). *Agile For Dummies – CA Technologies edition*. Indianapolis, Indiana: Wiley Publishing, Inc.

Moreira M. E. (2013). *Being Agile: Your Roadmap to Successful Adoption of Agile*..
USA: Apress.

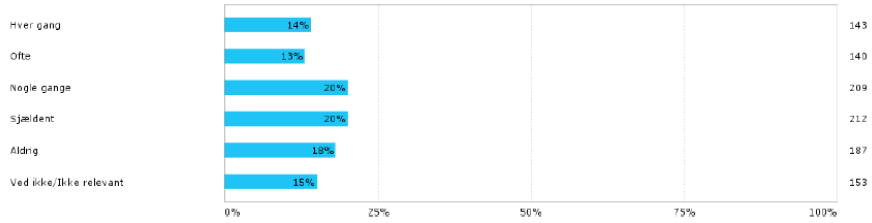
Stahl, G. (2006). *Group Cognition: Computer Support For Building Collaborative Knowledge*. USA: MIT Press.

Suchman, L. (1995). *Making Work Visible: How people work is one of the best kept secrets in America.* September 1995/Vol. 38, No. 9 COMMUNICATIONS OF THE ACM.

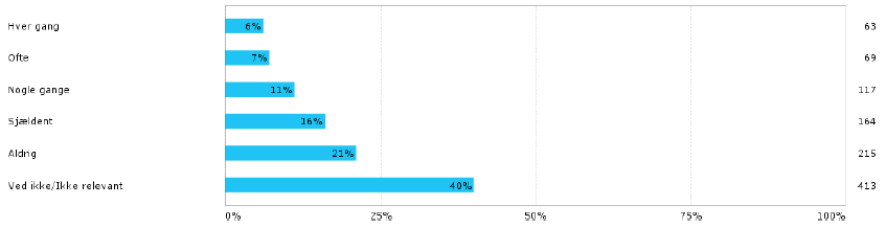
Appendixes

Appendix 1

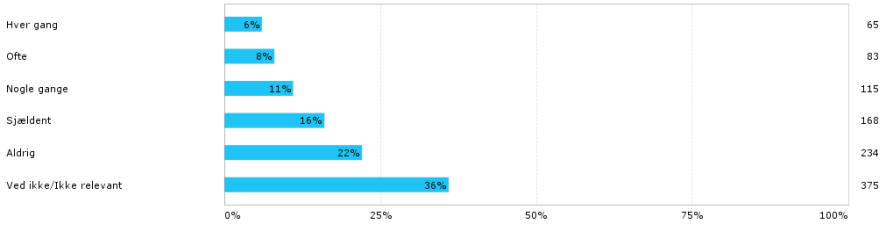
Hvor ofte læser du vilkår og betingelser på nettet, når ... - du handler på nettet (onlinesupermarkeder, online butikker sov.)?



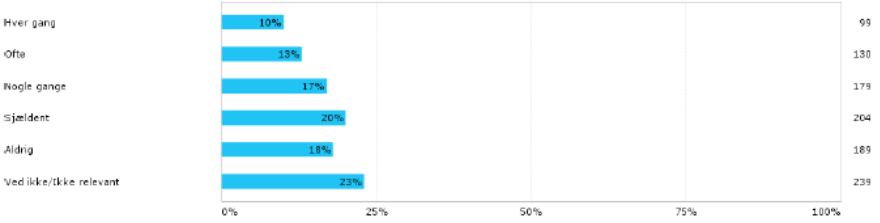
Hvor ofte læser du vilkår og betingelser på nettet, når... - når du er på facebook og andre sociale medier?



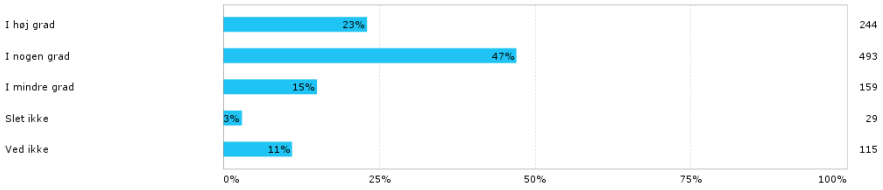
Hvor ofte læser du vilkår og betingelser på nettet, når... - når du bruger apps på telefonen?



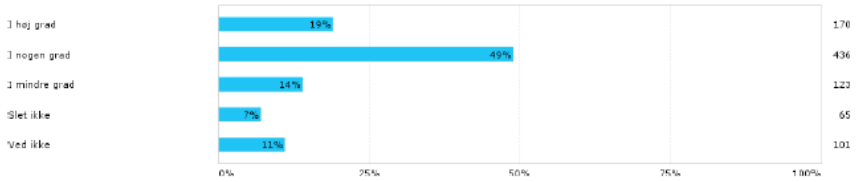
Hvor ofte læser du vilkår og betingelser på nettet, når... - når du bruger gratis onlinetjenester (f.eks. antivirus, e-mail, dropbox)?



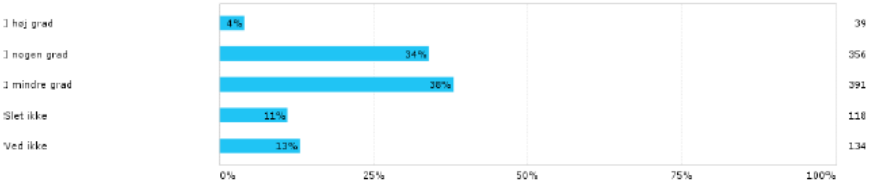
I hvilken grad oplever du, at vilkår og betingelser på nettet er svære at forstå?



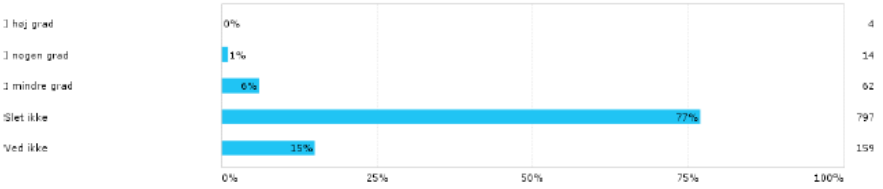
Vilkår og betingelser kan gøres nemmere at forstå ved at bruge symboler i form af f.eks. smileys, grønne og røde pile.
I hvilken grad vil visuel hjælp have indflydelse på, om du læser vilkår og betingelser?



Hver gang man opretter en profil på nettet, køber en vare online eller henter en applikation ned på sin telefon, skal man acceptere en række betingelser eller vilkår, som firmaet bag opstiller.
I hvilken grad føler du dig tryg ved, at det er disse betingelser og vilkår på nettet der fastsætter dine rettigheder i forhold til din færden på nettet?



Facebooks nyeste applikationopdatering til mobiltelefoner beder om adgang til at læse dine smsér som en betingelse for brug af appen.
I hvilken grad finder du det acceptabelt?



Appendix 2

Interviewee: *"Jo altså vi har omkring 70.000 medlemmer og jeg tror sådan set der er de fleste grupper repræsenteret [...]. Dem der vælger at melde sig og abonnere på vores blad, det er jo nok, der er nok en overvægt af bevidste forbrugere."*

Interviewee: *"Jamen det tror jeg også de er meget bevidste om og det er de fordi vi blandt andet fordi vi har kørt kampagne lige præcis om sådan noget her."*

Interviewee: *"[...] det er noget vi kan mærke, vi har lige indsamlet 10500 underskrifter for en bedre beskyttelse af vores data [...] så det er noget de går meget op i".*

Interviewee: *"Jamen vi gerne have en lov der beskytter bedre [...] der er en lov fra 1995[...] og vi synes ikke den giver god nok beskyttelse".*

Interviewee: *"Vi har så også en anden undersøgelse der viser at [...] tre ud af fire forbrugere som vi har spurgt [...] læser ikke det med småt inden de downloader en app."*

Interviewee: *"Sådan som vores liv er indrettet i dag så kan man jo altså,[...] jeg ved ikke om det var nogle nogle amerikanere der lavede en undersøgelse om hvor mange år af sit liv man skulle bruge hvis man skulle læse og forstå alle de her betingelser [...] og hvis du skal læse i svært juridisk sprog [...] vi har sat nogle af vores jurastuderende herinde til det [...] og de havde virkelig svært ved det [...] det var timer de måtte bruge på det."*

Interviewee: *"Så er det vores syn på det at der fra starten af er nogle grundregler [...] hvor der ligesom står, at du kan ikke bare bede om at du i al evighed kan tilgå den her forbrugers private oplysninger [...] og det kan du ikke bare gøre på side 131 i svært juridisk sprog for det er sgu ikke i orden."*

Appendix 3

Interviewee: *"[...] Overordnet er problemet jo at vi ikke er særlig godt beskyttet i dag fordi teknologien er løbet så stærkt og loven halter bagefter."*

Interviewee: *"[...]der har udviklet sig en forretningspraksis, eller forretnings modeller som indsamler forbrugernes oplysninger automatisk hver gang de bruger de her digitale platforme [...] og det er jo slet ikke reguleret."*

Interviewee: *"[...]altså hele de her regler om at man skal give samtykke til at ens op lysninger bliver indsamlet og videregivet, det sker jo ikke i dag [...]og der er slet ikke nogen der er nået at stoppe op og sige hov [...] skulle man ikke lige spørge hvad forbrugeren vil her"*

Interviewee: *"Vi forstår for eksempel ikke at det der sker på Googles Android platform [...] når du henter en app ned på din telefon [...] giver du automatisk samtykke til at den må hente alle dine private oplysninger på din telefon lige fra sms'er, lokalitet, kontaker og adressebøger og sådan noget og det, hvis man læser det i Persondataloven forstår man jo ikke kan være lovligt"*

Interviewee: *"Det er ikke propotionel og usalig indhentelse og du giver ikke samtykke til det, eller i hvert fald ikke noget klart samtykke."*

Interviewee: *"Ja der er jo heller ikke nogle grænser [...] når man opretter en profil på Snapchat [...] eller en profil på Instagram og Facebook og sådan noget, så kan det godt være de ikke har en ophavsret [...] over dine billeder og tekst, men du giver samtykke til at de må bruge indholdet."*

Interviewee: *"[...] men det samtykke det har man måske givet for 10 år siden da du op rettede en profil på facebook og det der så er galt det er jo at så kan de løbende ændre vilkårne som de vil uden at de skal spørge dig igen."*

Interviewee: *"[...] når vi forklarer forbrugerne hvad der foregår så bliver de meget kritiske. Grunden til at de ikke er det nu er at det er svært for alle og enhver, også os der arbejder med det at gennemskue den her kompleksitet i teknologien, men også at gennemskue hvad er det man kan bruge de her oplysninger til på sigt."*

Appendix 4

Interviewee: *"[...] fordi at den giver en alarm overfor brugeren som kan trigge noget forskelligt og gøre dem yderligere nervøse"*

Interviewee: *"[...] hvis du har bedt om tilladelse til at tage dataen så har du jo bedt om lov til det, men det er ikke det samme som at brugeren har artikuleret hvad det er det faktisk betyder".*

Interviewee: *"[...] og begrænsningen er nok mere i mulige bekymringer om hvad dataen kan blive brugt til end begrænsninger i lovgivningen"*