I am not that interesting

SOCIAL MEDIA, PRIVACY LITERACY, AND THE INTERPLAY BETWEEN KNOWLEDGE AND EXPERIENCE

Heidi Molvik Rundhovde

Master's Thesis in Information Science

Department of Information Science and Media Studies

University of Bergen

June 2013

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGEMENTS

I would like to express my great appreciation to my supervisor Professor Victor Kaptelinin for his patient and competent guidance of this research work. His valuable and constructive suggestions and willingness to give his time so generously have been very much appreciated.

I would also like to thank the participants for sharing their time and reflections. Without these contributions, this work would not be possible. Special thanks to the participants in the pilot studies. Their contributions were important for the development of the research strategy. Assistance provided by Nordahl Grieg videregående skole was very helpful in the data collection process. I appreciate their kind welcoming.

I would like to offer very special thanks to my family. Their patience, support, encouragement, and interest throughout the process have been impressive and so much appreciated.

My thanks are extended to friends and others that have supported this process in many different ways. Nobody mentioned, nobody forgotten. This help has been of great value.

ABSTRACT

Sharing of personal information on the Internet has become increasingly popular. In social media interactions users face a trade-off between the pleasure and usefulness of sharing and the need to protect their privacy. This study employs recent theory in the research area Human-Computer interaction to investigate users' privacy decisions on the social networking service Facebook from a holistic view, including aspects like emotions, dialectics, and social and temporal context. The purpose is to understand user behavior in the area of privacy and the implications of this for interaction design as well as for education of users. The analysis reveals the interplay between user experiences and rational, fact-based privacy knowledge as important for users' privacy choices. A model for privacy literacy is proposed, and application of this model on empirical data uncovers experiences of privacy divergent from the users' actual privacy situation on Facebook. This situation may explain some lack of rationality observed in privacy decisions by previous research. The presentation further identifies weaknesses in privacy literacy in areas of current importance, as well as differences in ideas and mindsets applied in the privacy process by youths and adults respectively. The observations show that users may be vulnerable to privacy risks despite a desire to behave cautiously and responsibly online and the efforts invested to reach this goal. Conclusions are drawn in the form of recommendations for designers, for educators, for users, as well as for further research.

KEYWORDS

privacy; security; social media; Facebook; privacy literacy; age differences; user experience; technology as experience; privacy for a networked world;

This page is intentionally left blank.

1. INTRODUCTION

I think we should share, that's why I'm in there. I think it is good thing. It has changed the relationships to my colleagues… I know what they are up to and what they think about this and that. And people that I haven't been talking to for years, I keep in touch and keep up with them. So, I am very fond of Facebook (#1:A1F)[1]

The Internet has given us new and meaningful ways to engage with other people. The first social media applications emerged a few decades ago, and by rapid growth these have become integral parts of our daily lives. On social networking services like Facebook[2], we share large amounts of information about our lives. We enjoy sharing; its pleasure and usefulness. Sharing of personal information has become increasingly popular.

This new way of communicating has a trade-off, though. There is a delicate balance between the pleasure and usefulness of sharing and the need to protect our privacy. The concentration of personal information on social networking sites opens up for unauthorized use of this information. Information control is complicated, and even users with high awareness towards risks may experience threats to their privacy.

Previous research on privacy has shown that user's decisions in this area are not always rational. Knowledge of privacy appears as an important, but insufficient factor influencing these decisions. By applying recent theoretical contributions within the research area of Human-Computer Interaction (HCI), this work will investigate users' privacy decisions from a holistic view including aspects like emotions, dialectics, and social and temporal context. The purpose is to find out if a more inclusive concept of privacy literacy, considering emotional, social, and dialectic aspects in addition to the rational, fact-based knowledge, can improve our understanding of users' behavior in the area of privacy.

The remainder of this introduction will elaborate the focus of this study, present its four research questions, and clarify the thesis structure.

[1] the notation used for identification of transcripts is described in the introduction to chapter 5
[2] www.facebook.com

1.1 Focus of this study

This study is aimed at understanding the influence of privacy literacy on users' choices in the privacy area. The social networking service Facebook has been used as a case for this investigation.

To understand privacy literacy, users' privacy decisions has been explored from three complementary perspectives: 1) in light of their rational, fact-based knowledge of privacy (KNOWLEDGE); 2) in light of the actual exposure of personal information resulting from these decisions (BEHAVIOR); and 3) in light of their general experience of privacy in interactions with technology (EXPERIENCE).

Users' fact-based knowledge of privacy has been explored by questions like: How well do users understand fundamental characteristics of digital information? How do users assess the sensitivity of different categories of personal information? How well do users understand the mechanisms for information control provided by the service they interact with? And the risks associated with sharing of information, what are users' conceptions of these?

Users' behavior has been explored by reviewing some of their actual privacy decisions and the consequences for exposure of personal information resulting from these.

Users' emotional experience of their interactions has been explored by questions like: What fundamental feelings characterize users' privacy interactions; uncertainty and doubts or a sense of security? How do users view themselves and the information about them online; as invulnerable or as potentially interesting in the view of a perpetrator? What timeframe and which purposes characterize users' privacy decisions?

18 Facebook users, nine youths and nine adults, have been interviewed about their privacy literacy. The interviews have focused on their rational, fact-based knowledge of privacy, but also on the emotions, ideas, and mindsets overarching their application of this knowledge in interactions on Facebook. Some of their privacy decisions on Facebook were reviewed to picture the actual exposure resulting from these choices.

To support the work, two perspectives from the last decade of research on privacy and user experiences within the research area of HCI were chosen; theory particularly suited to capture the emotional, temporal, social, dynamic, and dialectic aspects of users' privacy related interactions: 'Privacy for a Networked World' (Palen & Dourish, 2003) and 'Technology as Experience' (John McCarthy & Peter Wright, 2004).

As a result, this study proposes a model of privacy literacy. The model reflects a relation between knowledge, behavior, and user experiences, and is used recurrently throughout the presentation of

findings to mirror the weak and strong areas of privacy literacy observed. The presentation of findings also describe the participants' general privacy experience in interactions with Facebook; an experience in disharmony with their actual privacy situation. Finally, the presentation describes differences in ideas and mindsets between youths and adults; differences potentially important for their privacy decisions.

1.2 Research questions

The following four research questions have guided this work:

RQ1: Can inadequate knowledge of privacy explain why users sometimes show non-secure behavior on Facebook?

RQ2: Can users' experiences of privacy on Facebook complement the rational, fact-based knowledge aspects of their privacy literacy?

RQ3: Does teens' privacy literacy on Facebook differ from adults' privacy literacy? If so, how?

RQ4: Are some areas of the users' privacy literacy identified as weaker than others, in this way as candidates for improvement?

1.3 Thesis structure

The presentation builds on the following structure:

Chapter 2 (Background) complements the backdrop sketched in this introduction and presents previous research relevant for this work. The risks associated to sharing of information on the Internet in general and on Facebook in particular are depicted. The chapter is finalized by a presentation of the motivation for research.

Chapter 3 (Theory) describes the theoretical perspective used as a lens for this work: a rich perspective for explorations of user experiences ('Technology as Experience') and another for investigating privacy in networked applications from a dynamic, dialectic, social, and process-based perspective ('Privacy for a Networked World'). Research traditions within the area of HCI are briefly reviewed, in order to clarify the positions of the two perspectives therein.

Chapter 4 (Method) describes some basic assumptions for this study, and details the methodological approach chosen to support data collection and data analysis. The primary approach is qualitative and interpretive, yet triangulation of methods and quantitative techniques has been employed for a rich perspective on the phenomenon. This chapter also reviews the two pilot studies and the value of these for the final research design. The detailed procedures used in data analysis in the main study are presented in the final paragraph of the chapter, 4.4.2.5.

Chapter 5 (Data analysis) present the findings within each of the three perspectives used to understand privacy decisions; KNOWLEDGE, BEHAVIOR, and EXPERIENCE. The presentation is given by a combination of textual descriptions, transcripts, figures, and tables, and reflects the triangulation of qualitative and quantitative approaches used to reach these findings. The model of privacy literacy appears recurrently throughout the presentation to reflect the findings within the three complementary perspectives.

Chapter 6 (Discussion) a discussion of findings in light of each of the four research questions will be found, followed by reflections on use of the chosen theoretical perspectives. These reflections point out some elements of the theoretical contributions which were found particularly useful for investigating the research questions of this study. The chapter is finalized by an evaluation of this work based on generally accepted criteria for assessment of scientific quality in qualitative research.

Chapter 7 (Conclusions) draws conclusions from this work and present some recommendations for further research.

This thesis is submitted June 1, 2013 to the Department of Information Science and Media Studies at the Faculty of Social Sciences, University of Bergen, Norway as partial fulfillment of the requirements to the degree of 'Master in Information Science'. As privacy has been theme for several works for my master's degree, some thoughts in this thesis may be present in other submissions for this degree. In this thesis, however, they are formulated for a different context.

2. BACKGROUND

Social media are Internet sites where people interact freely, sharing information about each other and their lives. These sites appear in many forms, including blogs, social networks, wikis, virtual worlds and video sharing sites, and information is shared using various formats, like text, pictures, videos, and audio recordings (Curtis, 2013). Today, users spend more time on social networks than any other category of social media sites, and services like Twitter, LinkedIn, and Facebook has become important parts of many people's everyday lives. The increasing use of mobile devices has been an important catalyzer for this development. Applications are used extensively, application use now accounts for more than one third of social networking time across PCs and mobile devices (Nielsen, 2012).

Facebook is the most widespread social networking application on the Internet and has had an excessive growth since the early start in 2004. Member count as of February 2013 is 1.11 billion monthly active[3] users worldwide, this number is up from 360 million users at the end of 2009 (Facebook, 2013a). Norway has 2.72 million[4] Facebook users (**Table 1**). Many Norwegian users have several years of Facebook experience, as the most extensive member growth in Norway took place between September 2006 and the end of 2008[5] (Synlighet, 2012). Users continually share more information about themselves on Facebook. In 'Zuckerberg's law of social sharing', the founder of Facebook describes the increase in sharing as developing exponentially, by a doubling every year (Tsotsis, 2011).

Age	*13-17*	*18-24*	*25-34*	*35-54*	*55+*
Female	177 880	248 540	293 280	468 080	162 380
Male	182 240	269 960	297 960	419 460	152 760
Total	**359 840**	**524 020**	**608 200**	**910 500**	**323 140**

Table 1: Norwegian Facebook users (Synlighet, 2012)

2.1 Privacy on the Internet

2.1.1 Personal integrity, identity, and information security

Social media use opens for new and extensively popular ways for communicating, creating, and sharing content. At the same time, the use of these technologies challenges our control of own personal information. As our existences in the world of new digital technologies to a considerable extent are understood on the grounds of this information, privacy related aspects like personal integrity, information security, and the shaping of one's own online identity has become more important.

[3] defined as a member that has logged in to the application during the last 30 days
[4] as of September, 2012
[5] 1.5 million Norwegians registered for a Facebook account this period

In a definition of privacy[6] acknowledged by Norwegian government and legal authorities, Schartum and Bygrave (2011) describe six aspects of personal integrity. Adapting their model of privacy into this context, **Figure 1** reflects these six denoted as: *psychological integrity* (protection against no choice-situations and emotional stress); *physical integrity of body* (protecting the body against physical harm); *physical integrity of property* (protecting geographical areas like home and property); *communication integrity* (protecting the right to communicate without intrusions); *information integrity* (protecting the right to generate, adapt, and manage information about ourselves, including the right to decide upon the availability of this information to others), and *contextual integrity* (protecting our norms for the information's relevance in different social contexts).

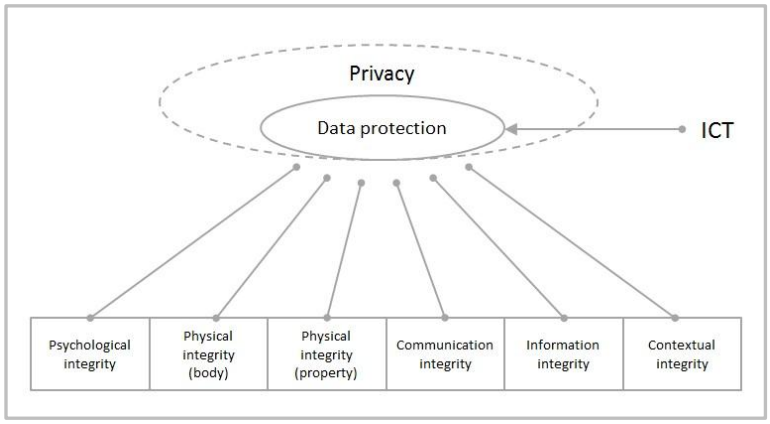


Figure 1: Six aspects of integrity (based on Schartum & Bygrave, 2011)

Rachels (1997) points to how the loss of control over personal information can violate our personal integrity by interfering with the process of organizing the social relations of our lives. Different behavioral patterns link to different types of social relations, and disclosure of information in inappropriate contexts can disrupt our system of social relations to other people; 'that is why the loss of privacy is so disturbing' (Rachels, 1997, p. 150). This view of integrity overlaps the concept of contextual integrity described by Schartum and Bygrave, and is closely related to the need to control the expressions for one's online identity. Identity is a central aspect of privacy as defined by the privacy framework chosen for this study: 'Privacy for a Networked World' (Palen & Dourish, 2003). This framework is further described in chapter 4.

Information security issues are important for the question of privacy. Lack of security yields problems for the control of personal information and by this, potential problems for privacy. Users of social media are vulnerable to security risks due to several reasons. Years of information security efforts have made hacking of state-of-the-art security systems so difficult that hackers now turn to users and the use situation (Mathiasen & Bødker, 2008). Social media sites are accessed from a variety of devices (like pc, mobile, tablets) and in different settings (like work, leisure), and this increased use in non-traditional settings introduces heightened risks of misuse (Iachello & Hong,

[6] in Norwegian: Personopplysningsvern

2007). Social networking services are typically designed for users to build a profile of themselves by concentrating personal information of various kinds on the same site. At the same time as we disclose increasing amounts of information about ourselves (Stutzman & Kramer-Duffield, 2010), this contribute to increased vulnerability for users of these services.

Vulnerabilities can be utilized in various ways. Attempts of *phishing*[7], in order to get access to a user's confidential information (e.g. bank account information, passwords) are getting more sophisticated and associated problems of *identity thefts*[8] increase continuously. Problems with *viruses* spreading through *malware*[9] in social networks is getting more and more common, as well as *scam*[10], where the scammers unceasingly apply new variations of techniques and disguises to get hold of other people's personal information. Major and not very well known current threats for social media users, however, are the problems of social engineering and coupling.

2.1.2 Social engineering and coupling of data from different sources

Social engineering is the act of manipulating people to reveal sensitive information or to perform actions they normally would not have done (NSM, 2010). Gaining confidence by manipulation can give the perpetrator unauthorized access to information or to computer systems. Social engineering is commonly a first step in a process and the final purpose may be crimes and frauds of various kinds (e.g. identity thefts, financial fraud, and unauthorized access to information systems). Access to personal information can increase a perpetrator's credibility in social engineering attemps in two ways: by making it easier to lure the victim herself, but also by making it easier to take on the victim's identity in meeting with others.

Not only information traditionally seen as sensitive (like Social Security Number and bank account number) are utilized in social engineering, expressive information like preferences, attitudes, and beliefs may turn out as very useful for a perpetrator, as well.

Coupling of information increases the risks for social engineering and other forms of unauthorized use of personal information. One, isolated piece of data about an individual may not be very revealing, yet combining many pieces of information can paint a portrait of the user's identity (Solove, 2008). Combining pieces of our online footprints can provide complete pictures of individuals, but unfortunately, this is not necessarily a picture recognized by the users (The Norwegian Data

---

[7] fraud by passing oneself off as a trusted contact (bank, internet provider, etc.)
[8] taking on another person's identity in order to gain advantages, or to impose inconvenience upon others
[9] malicious software installed on a computer without the owner's permission., e.g. viruses, Trojans, worms, spyware, adware, or other programs developed with malicious purposes in mind
[10] fraud by disguise in order to gain advantages, e.g. tricking people into handing over personal information

Inspectorate, 2013). Researchers have known this for some time, but these issues are not so well known among users in general: '…the public is coming slowly, if painfully, aware of the risks of combining personal information from multiple data sources' (Iachello & Hong, 2007, p. 100). The findings of this study indicate that this issue is still not very highly focused by users.

Research has demonstrated the power of data coupling. Kosinski, Stilswell, and Graepel (2013) found that personality traits and attributes like sexual orientation, ethnicity, gender, and political sympathies, are predictable from the rather commonly available information of Facebook 'likes'. Acquisti and Gross (2009) showed how simple, often publicly available information of an individual's place and date of birth can be exploited to predict his or her Social Security Number. Not less thought-provoking are the findings of Acquisti, Gross, and Stutzman (2011): By combining facial recognition technologies and mining of publicly available online data they identified anonymous people from an offline photo and inferred potentially sensitive data about them from publicly available online sources, among these Facebook. Actually, by combining the methods from the two latter studies, the researchers were able to infer the Social Security Number of an anonymous person by a simple photo shot on the street.

However, not only criminals are seeking the Internet users' personal information. Internet actors collect pieces of information about net users to vast data sets ('big data'). Market research and analysis firms specialize in coupling of isolated information elements to detailed profiles of users; profiles which are sold to commercial actors (The Norwegian Data Inspectorate, 2013). An example of such collection is how top-ranked Facebook applications was found transmitting user IDs to advertising and Internet tracking firms (Steel & Fowler, 2010). Recent technologies for capturing, coupling, analysis, and presentation of large data collections have increased the possibilities to utilize this information. Such activities are profitable, and by involving ample resources commercial actors' research in this area lie ahead of academic research (Jakobsen, 2013). And further, web scraping techniques allow unstructured web data (typically on html format) to be retrieved and transformed to structured data suited for analysis and storage in local databases. For example, Polakis et al (2010) describe techniques for the harvesting of email addresses coupled with other personal information from social networks. Extracting and combining data from websites can make the Internet users' personal information available in settings they were not originally intended for.

The unauthorized utilization of personal information is an issue not only at the individual level. Blurring of borders between work and leisure make social engineering a security challenge at the organizational and the national level in the years to come, as well (NSM, 2010). Social media is one of

several channels used for social engineering aiming at getting access to sensitive information in information systems (NSM, 2010, 2011). BYOD[11] policies and the use of work devices for leisure, combined with extensive use of social media and third-party applications, turn individuals' lack of risk awareness into a challenge for security at the organizational and the national levels, as well as for individuals.

2.2 Privacy on Facebook

2.2.1 An interesting case for privacy research

Access to a person's Facebook data commonly opens the door to a wealth of personal information[12]. Combined with the requirement of users' authenticity and the service's extensive popularity, this may be the largest collection of real identities in the world. Users' voluntary coupling of data from different contexts to complete profiles of themselves make personal information on Facebook highly valuable for other actors, whether these are commercial actors, cyber criminals, potential employers, or curious others.

Facebook has been criticized for its privacy policy from users as well as from governments. The company has been subject to claims and law suits from privacy watchdogs in many countries, including in the U.S. and European countries like Germany, France, Ireland, and the Nordic. In a ranking by the organization Privacy International in 2007, the service was ranked as 1 of 7 bottom companies (Privacy International, 2007). Its design has been changed on several occasions in order to accommodate complaints, but privacy issues are still reported for this service on a daily basis.

Many researchers have been studying Facebook and privacy, in the recent years particularly. Several studies show that users are concerned for their privacy on Facebook (Brandtzæg & Lüders, 2009; Johnson, Egelman, & Bellovin, 2012), and in the years since Facebook was introduced, they have exhibited increasingly privacy-seeking behavior by reducing their amount of sharing outside their network of Facebook friends (Stutzman & Kramer-Duffield, 2010). However, they do share increasing amounts of personal information with people inside this network, and this sharing increase their sharing to 'silent listeners' at the same time (i.e. third-parties, Facebook itself, and advertisers, indirectly) (Stutzman & Kramer-Duffield, 2010).

Users are often unaware of their sharing of information to silent listeners. Misunderstandings relate to the process of authorizing third-parties access to personal information, as well as to the content and

[11] Bring Your Own Device: employees use personally owned devices to access privileged systems or information at work
[12] like name, date of birth, contact information, education, preferences, network of friends, romantic relationships, sexual preferences, political orientation, interests, cultural taste, and movements in the physical world

volume of the information actually accessed (Besmer & Lipford, 2010; King, Lampinen, & Smolen, 2011; Wang, Xu, & Grossklags, 2011).

Disclosures of personal information tend to increase extensively through the use of third-party applications. Information is shared not only through the user's own third-party activity, but through the activity of her Facebook friends, as well. Large amounts of personal information are transmitted from Facebook to external entities (Besmer & Lipford, 2010; Wang, et al., 2011) and 'there is a potential for a malicious application to quickly spread and harvest' user data through the use of third-party apps (Besmer & Lipford, 2010, p. 69). Third-parties do not always apply the standard authorization process recommended by Facebook, but rather redirects the user to websites outside Facebook (Wang, 2012). A further problem relates to the splitting of Facebook architecture in two separate privacy contexts (read more about Facebook architecture in the next subsection, 2.2.2), as third-parties can override users' global (Facebook Core, 2.2.2) privacy settings (Wang, et al., 2011).

Facebook users are offered a rich set of mechanisms for information control; however, rich privacy settings do not necessarily provide a high level of protection. Users tend to find the privacy settings difficult to understand (Brandtzæg, Lûders, & Skjetne, 2010; Brandtzæg & Lüders, 2009; Stutzman & Kramer-Duffield, 2010), and high granularity in settings are found giving the paradoxical effect of increasing users' willingness to share sensitive information, even in cases where the objective risks of disclosure increased (Brandimarte, Acquisti, & Loewenstein, 2012). Studies of privacy settings often relate to settings in Facebook Core only.

The privacy settings for Facebook Core are found as better suited for protection against the 'outsider threat' (strangers, people outside our network of Facebook friends) than for the 'insider threat' (avoid sharing with selected subsets of friends in our network dependent on context) (Johnson, et al., 2012). And finally, Facebook users tend to underestimate the audience size for their posts, generally by a factor of three (Bernstein, Bakshy, Burke, & Karrer, 2013).

In practice, Facebook posts shared for 'public' availability are accessible for the general Internet public. These posts are accessible through searches and navigation on the Facebook service; through search engines on the Internet; and also through web sites dedicated to search for information from social network services[13].

[13] examples are http://www.weknowwhatyouredoing.com/; usaface.net; http://ukface.net/; www.spokeo.com http://en.wikipedia.org/wiki/Openbook (website); and http://www.pleaserobme.com

2.2.2 Architecture and information control

This subsection reviews some aspects of the Facebook architecture central for this work.

The Facebook service is made up of two main parts; the site's core functionality, *Facebook Core*, and a platform for integration of software from third parties, *Facebook Platform*. Facebook Core allows users to share personal information in a one-to-many fashion through a personal profile and a homepage called a Facebook wall[14]. Users also communicate through a chat/messaging service suited for one-to-one communication between single users. In Facebook Platform, users share information about themselves to other users as well as to third-party developers, through their own and also their friends' use of third-party applications. Personal information is shared in many forms (profile data, 'likes', photos, status updates, and comments) and formats (text, photo, video, web links).

By this splitting of the service's architecture, users face *more than one privacy context* in their interactions with Facebook. Separate mechanisms for information control yields for these two, main building blocks; privacy settings in Facebook Core regulates the information flow between Facebook users (friends and non-friends), and privacy settings in Facebook Platform regulates the flow between users and third parties (Wang, et al., 2011). Additionally, Facebook provides a set of mechanisms for regulation of information security, here denoted as Facebook Security.

By integrating their applications with Facebook, third-party developers get access to the website's millions of users. Anyone is allowed such access through a published and uniform interface, the Graph API. Facebook invites developers to use a standardized interface for collecting the users' authorizations for access to the personal information they want to include in their application design. This gives a standardized visual layout for situations where different third parties ask for access to different sets of personal information[15]. Figures 2-5 on the next page show examples of the user dialogue in Facebook Platform[16]. Facebook further encourage developers to utilize the users' own data to personalize the use experience of the application and by this integrate the application activity deeply with the users' interaction in Facebook Core: 'Facebook profile data can be used to personalize the user experience in your app so that it feels familiar, relevant and trusted by default' (Facebook, 2013b).

Previous research has shown that users find information control mechanisms in both building blocks as difficult (subsection 2.2.1). The standardization and integration of the interface between them may create further problems by blurring the transition from one privacy context to the other.

---

[14] Facebook Wall was changed and renamed at the time of data collection for this study. It is now called Facebook Timeline

[15] third-parties can ask for access to 63 different information/behavior permissions from users (Wang, 2012) and as of March 2012, more than 9 million third-party apps and websites were integrated with Facebook (http://newsroom.fb.com/Platform)

[16] Figures 5 and 6 illustrate a development in the authorization process turning visual focus from protection to entertainment

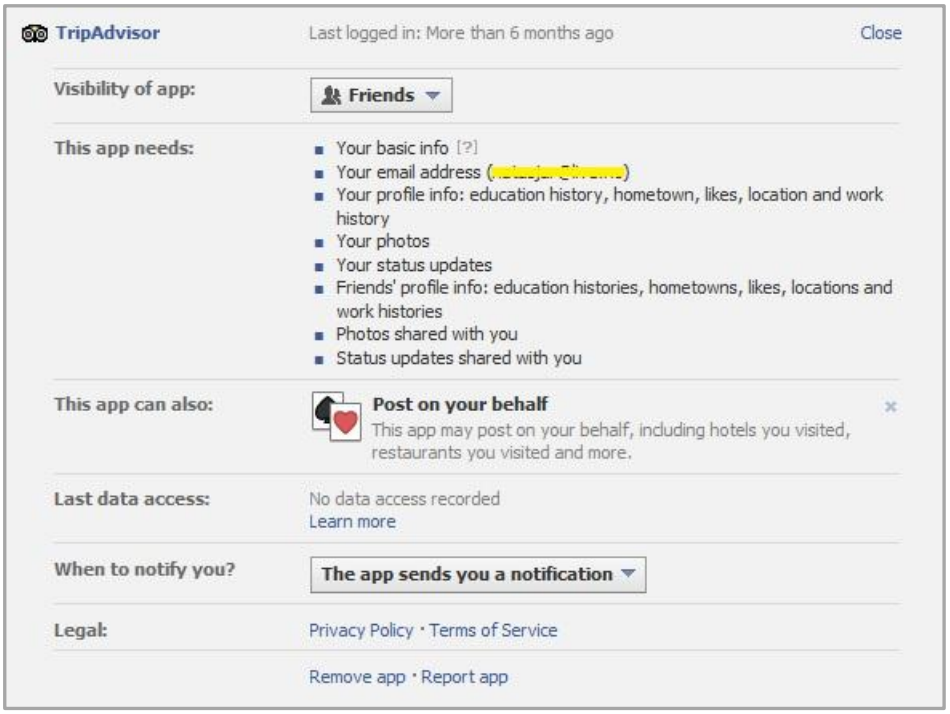


Figure 2: Facebook Platform: privacy settings for sharing through own use of third-party applications (sample application)

Figure 3: Facebook Platform: privacy settings for sharing through friends's use of third-party applications (default values)

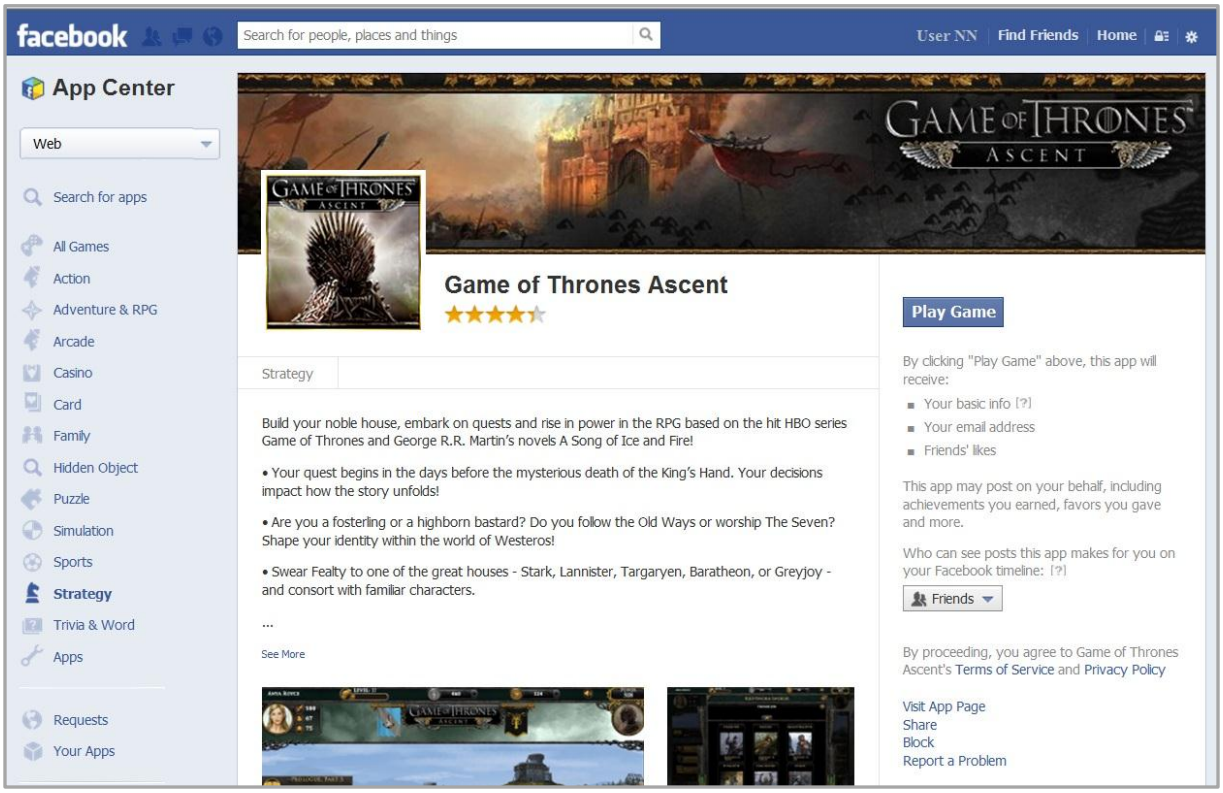


Figure 5: Facebook Platform - authorizations page for third-party application (current design)

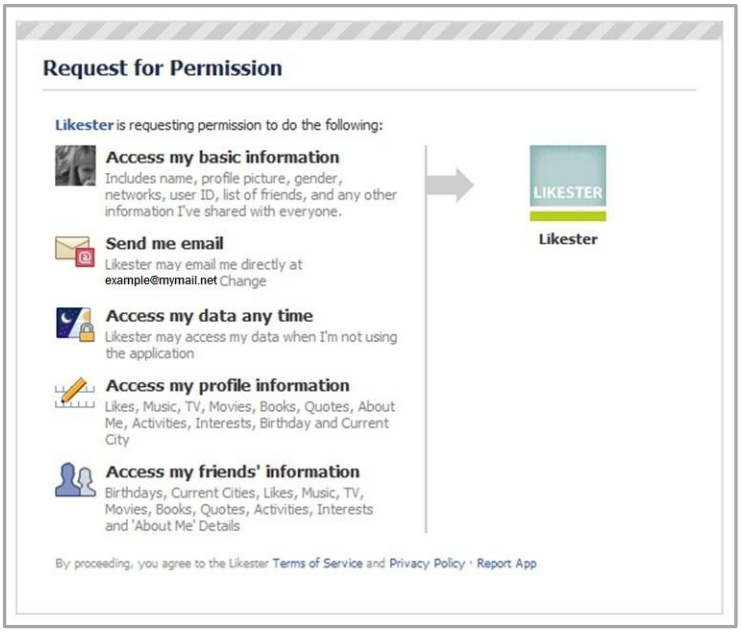


Figure 4: Facebook Platform - authorizations page for third-party application (old design)

2.3 Privacy decisions and rationality

In the light of the issues related to users' privacy situation on the Internet in general and on Facebook in particular, rational, fact-based knowledge of privacy are assumedly important for their ability to make competent privacy decisions.

However, users' privacy decisions are not only rational (Acquisti & Grossklags, 2005; Berendt, Günther, & Spiekermann, 2005; Iachello & Hong, 2007). Acquisti and Grossklags (2005) point to knowledge as crucial for privacy decision making, but also to the importance of individual factors like motivation, preferences, and past choices[17].

And further, Iachello and Hong states that 'privacy interacts with other social concerns, such as control, authority, appropriateness, and appearance' (2007, p. 4). Brandimarte, et al. (2012) found that a feeling of control increase users' willingness to share sensitive information, despite increasing risks. Besmer and Lipford (2010) showed that social interaction and expectations influence the users' granting of access to personal information to third-parties. And King, et al. (2011) found aspects of experience as consistent predictors for privacy concerns related to third-parties, where knowledge and behavior were not.

Bawden (2008) discusses aspects of the concept digital literacy as introduced by Paul Gilster[18], and states that 'digital literacy is not about… technology itself. It is about the ideas and mindsets, within which particular skills and competences operate…' (2008, p. 19).

These examples of previous research indicate that further explorations of privacy experiences may be important to understand users' behavior in privacy situations. Recent perspectives on user experiences within the area of HCI strengthen this impression by providing a more dynamic view of privacy including aspects like dialectics, temporal qualities, and the users' shaping of a social identity (Palen & Dourish, 2003). And also emphasizing a holistic view of users as humans feeling, sensing, and making sense of their interactions with technology (John McCarthy & Peter Wright, 2004).

By applying these perspectives, this study has been aimed at exploring a concept of privacy literacy which includes the emotions, ideas and mindsets that users bring into their encounters with technology, as well as their rational fact-based knowledge.

[17] they further emphasize the importance of the users' cognitive resources and the problem of bounded rationality
[18] Paul Gilster: *Digital Literacy* (1997)

2.4 Research motivation

Even if privacy has been an important research theme for some time, is a need for further research is recognized. In a review of previous research on security decisions for home computer users, Howe, Ray, Roberts, Urbanska, and Byrne (2012) point out how considerable effort has been directed at investigating the usability of security tools, yet less at elucidating how users understand privacy and security threats and their potential consequences. They recommend the use of a qualitative methodology to provide rich explanations and descriptions of users' perceptions and choices. They further recommend assessing the impact of demographics on privacy behavior, age in particular. In their review of privacy research in HCI, Iachello and Hong (2007) point to the need to gain a deeper understanding of the factors influencing users' privacy behavior, and to investigate the social and dialectic aspects of privacy, in particular.

Previous research has presented findings relevant for some of the areas of privacy literacy investigated in this work (this chapter). To the best of my knowledge, no works based on empirical data have been aimed at gathering findings from different areas of user knowledge into a common model of privacy literacy. This work is thought of as an initial exploration of such a model. The purpose is to clarify aspects of literacy crucial for users' behavior in the privacy area. Insights in user behavior can increase our ability to develop software accounting for the users' actual needs.

A deeper understanding of users' privacy behavior would be beneficial for the Norwegian public debate about privacy and information security. By aiming at understanding users' choices by exploring the relations between privacy decisions, knowledge, user experiences, and age, this study hopefully contribute in this direction. As described earlier in this chapter, the question of users' privacy choices affects security not only at the individual level, yet at the organizational and even at the national level, as well. Improving our understanding of privacy behavior can be useful for regulation and education within the privacy and information security area. These insights can be passed on in order to support users' awareness to and understanding of their own online privacy, as well.

This page is intentionally left blank.

3. THEORY

This chapter presents the theoretical perspective chosen for this study. The perspective is based on two recent contributions to HCI research which are turning to the emotional, interactional, and dialectical to understand users' privacy interactions with technology: *Privacy for a Networked World* (Palen & Dourish, 2003) and *Technology as Experience* (John McCarthy & Peter Wright, 2004).

Section 3.1 presents a review of privacy research in HCI. Section 3.2 looks into the foundation of the tradition of *personal privacy research* and positions the *Privacy for a Networked World* framework within this tradition. Section 3.3 reviews the development of the concept of the *user experience* and relates the second contribution, the *Technology as Experience* framework, to this setting. Section 3.4 summarizes the theoretical perspective for this study.

3.1 Privacy research in Human-Computer Interaction

Iachello and Hong (2007) have surveyed research on the topic of privacy in the HCI area in the past decades. They describe a general, mutual influence between technology developments and the theorizing about technology. Technological innovations, our use of these, as well as the social expectations incumbent on the technologies, all tend towards shifts in focus for technology research. Three main technological and theoretical shifts within HCI the last 3-4 decades have introduced changes in research on and conceptualizations of privacy:

1960-80:	The non-discretionary era: focus on centralized personal data management
1980-2000:	The self-determination period: focus on users' discretionary use of technology
2000-today:	Implicit interaction: focus on interpersonal communication and behavioral analysis

Within the research community, these shifts are more generally referred to as the *three waves of HCI*. The earliest phase, the *first wave*, was characterized by command-based and simple WIMP/GUI[19] interfaces (Sharp, Rogers, & Preece, 2007). Computers, programs, and centralized computing were highly focused. A view of the user as an information-processing unit analogous to the computer dominated the research area until the 1980's. The transition to the next phase was identified and described by Bannon (1991) as a shift 'From Human Factors to Human Actors'. Bannon strongly criticized the view of users as depersonalized, passive, and naïve. He described the way people was treated during the first phase as '…at worst, idiots who must be shielded from the machine, or at best, as simply sets of elementary processes or "factors" that can be studied in isolation in the laboratory' (1991, p. 1).

[19] WIMP = Windows, Icons, Menus, Pointing devices and GUI = Graphical User Interfaces

In the *second wave*, a view of users as human agents achieving their meaningful goals in a real-life contexts came into focus. The users' values, motivation, and practices, as well as the contexts these practices were situated in, became important. Seen as the experts of the area of application, users were more commonly included as participants in the design of technologies. Typical interfaces in this period were advanced GUI's, web interfaces, as well as speech-, gesture- and touch-based interfaces (Sharp, et al., 2007). Technology use at the workplace, communities of practice, and the social interaction taking place between users were important aspects in this picture.

Bødker (2006) describes characteristics of a new shift in focus at the end of the 1990's, which may be referred to as a *third wave* of HCI [20]: During the last 10-15 years, a range of new technologies have appeared; pervasive and mobile technologies; technologies based on implicit interaction[21]; augmented reality, and the use of wearable and tangible interfaces. The use contexts and application types are broadened and intermixed. Technology has spread into most areas of our everyday lives and culture, flowing across contexts, and blurring the traditional borders between workplace and leisure, rationality and emotion, as well as between the public and private spheres. These technological developments also bring new elements of human life into HCI theorizing; elements like culture, interaction and dialogue in a social, cultural, and historic context. A stronger focus on the users' experiences of their interactions with technology includes new human skills and abilities, as well as an expansion of the cognitive to the emotional, in research.

The theoretical and technological shifts came to influence research on privacy, as well (Iachello & Hong, 2007). In the first phase of centralized data management, *the non-discretionary era*, privacy research was characterized by the top-down approach that was typical for IT in the 60's and 70's. Focus was kept on data protection mechanisms in central computing systems, data owners in charge of the management of personal data, and the specification of unambiguous rules for handling of data use limitations. In the 80's, *the self-determination period*, advances in personal computing turned focus to the discretionary user, to trust, and to the users' right to decide upon the use of their personal data (informational self-determination). In the third phase, *the period of implicit interaction*, emergence of the Internet has enabled new forms of communication and an increasing fluidity of personal information, and given rise to a new focus on interpersonal privacy in everyday interactions and communication. New interactions in non-traditional settings, as well as the character and amounts of

[20] Bødker questions the assumption of a' true' third wave of HCI, but denote these new elements of HCI by the concept of a third wave

[21] automated interaction based on situational context rather than on the user's direct manipulation by GUI's

personal data collected, heighten the risks for misuse and introduce new challenges to research on privacy.

The question of privacy spans the social, the technical, as well as in the regulatory, and these issues have been researched from various perspectives across disciplines. A common definition of this concept has not been agreed upon. Privacy research in HCI is also closely intertwined with security research, with research within the area of *Usable Security* in particular. Presenting an inclusive overview of previous research in the privacy field would be out of scope of this work, however an overview of trends and works in privacy research in HCI and CSCW[22] are presented by Iachello and Hong (2007); an overview of research on 'Usability and Security for Home Computer Users' in Howe, et al. (2012); and a presentation of theories and views on the concept of privacy are found in Solove (2008, ch. 1-2), for example.

Irwin Altman[23] and Alan Westin[24] both developed theories of privacy which have stimulated research on this topic from the 1970's. Their research originates from different disciplines, from social psychology and law, respectively. In Altman's theory, a process perspective on privacy in its social environment is emphasized, whereas Westin's work focuses on information privacy and the classification of privacy in states and functions (Margulis, 2003). These classical works became sources for two main directions of privacy research within HCI; Data Protection and Personal Privacy research. *Data Protection* research draws on Westin's theory, and focuses on privacy in the relationship between individuals and large organizations like governments or commercial entities. Typically, research questions center on the problem of regulating for what purposes and at what time individuals' personal data are used by these organizations. In contrast, Personal Privacy research is focused on interpersonal relationships and questions of how people manage their privacy in relation to other individuals. *Personal privacy research* has its origin in Altman's works on privacy in the physical world, and his theory was later adapted by Palen and Dourish into an analytical framework for privacy in IT settings; 'Unpacking Privacy For a Networked World' (2003). The next section presents a further look is into these theoretical contributions.

3.2 A social-systems orientation towards privacy

In his work on privacy in the physical world, Irwin Altman (1975, ch. 1-3) take an ecological, social-systems orientation towards the concept of privacy, where the social, physical, cultural, and temporal contexts of the privacy process are important aspect for understanding the concept. Defined

[22] Computer Supported Cooperative Work
[23] Irwin Altman: *The Environment and Social Behaviour:Personal space, Privacy, Crowding, and Territory* (1975)
[24] Alan Westin: *Privacy and Freedom* (1967)

as 'the selective control of access to the self or to one's group' (1975, p. 18), privacy is an *interpersonal, dynamic, dialectic,* and *goal-oriented boundary regulation process,* where a person or a group control (restrict or seek) their interaction with others by means of four *behavioral control mechanisms.*

These boundary regulation mechanisms are: *personal space* (changing communications with others by alterations of the area immediately around the body); *territorial behaviors* (regulating by possession, marking and defense of physical objects and areas); *verbal and nonverbal behavior* (what people say, by words or body language, to others to make themselves more and less accessible, and how they do that); as well as *cultural mechanisms* (regulating by customs, norms, and styles of behavior in a cultural group). The process is goal-oriented in striving to reach the momentary, desired level of privacy, which is an internal, personal state based on 'past experiences, immediate possibilities, and general personal style' (1975, p. 8). When the regulation process fail to reach the optimum level of privacy, the level of interaction achieved give more (*crowding*) or less (*social isolation*) interaction than the desired, transient goal of the regulation process prescribes.

The regulation of interaction on a continuum from closeness to self to closeness to social environment is one major function of the privacy process. This *interpersonal function of privacy* is an important end by itself, yet additionally supports the two other main functions of privacy; the function of self-definition and the function of self-identity[25]. *Self-definition* relates to the definition of one's self by social comparison; comparing self to others in order to clarify and define own feelings and perceptions. *Self-identity* is defined as:

'... a person or group's cognitive, psychological, and emotional definitions and understanding of themselves as beings… one's capabilities and limitations, strengths and weaknesses, emotions and cognitions, beliefs and disbeliefs' (1975, p. 49)

Altman's theory from the 1970's describes privacy and privacy regulating mechanisms for interactions in the physical world. The technological innovations from the last decades has changed and complicated the privacy process. Through the introduction of pervasive technologies, information processing are integrated into everyday objects and activities, and new representations of personal information have appeared; digital photos, text, audio recordings, location data, biometrical data, etc. Grudin (2001) describe how information may change when it is converted to digital format; transient information becomes permanent (*persistence*); local information becomes *globally available;* digital

[25] drawing on Erving Goffman's classical work on human behavior *The Presentation of Self in Everyday Life* (1959)

information tend to spread rapidly (*virality*), and may be left *desituated*.[26] Digital information can have new audiences in another place and time than initially intended for and new interpretations of the information emerge. Further, as human states (physical, social and emotional) can be difficult to capture and represent digitally, and as software-based interpretations of information may differ from interpretations made by human processes (biological, psychological and social), this might change the characteristics of the information in the processes of converting it to and managing it in digital form.

These transformations of information imposed by IT complicate the privacy regulation process, and potentially aggravate the negative consequences of insufficient privacy regulation. By this, they set the question of privacy in a new light. Palen and Dourish (2003) further focus how technology mediates action in a different way than the physical, everyday environment. Interaction in the virtual world eliminates the regulating mechanisms tied to the physical presence of interacting parties, and mechanisms like closing the door, leaving the range of vision/hearing, and closing the blinds, are no longer valid options. Consequently, when entering the virtual world, new mechanisms for regulation of the privacy process are needed.

3.2.1 Privacy For a Networked World

Palen and Dourish (2003) adapted Altman's theory into an analytical model for approaching privacy for networked settings. Like Altman, they frame privacy as a boundary regulation process where people bargain their privacy continuously by managing goals in tension. By regulating the flow of personal information, people aim at achieving their momentary goals. Information disclosure is not a mere threat, but a desirable tool that help us in social purposes like managing others' conceptions of our selves, and shaping our identity, as well. The dynamic process of privacy regulation takes place in a cultural, historical, and social context. The process is dialectic; in the sense that regulation is governed by the tension between the user's own expectations and the expectations of others participants in the interaction. Users continuously bargain and optimize their accessibility along a spectrum of openness and closedness to achieve the desired privacy state.

New technologies introduce a need for new behavioral mechanisms for regulation of the privacy process. Palen and Dourish's model extends Altman's thoughts with the concepts of *privacy boundaries* and *disclosure genres*.

[26] when pieces of information are removed from its originating environment, important context information like the time and place of action, and the attention and intentions of the actor may be lost

Users regulate their open- and closedness to others along three different dimensions; the boundaries of disclosure, time, and identity. *Privacy boundaries* represent points of balance (and resolution of conflict) between competing goals. Boundaries change dynamically as the context changes. The boundaries are described by the tension of goals that they are representing. Three boundaries are central to privacy regulation: *Disclosure boundary*, where privacy and publicity are in tension. In trying to maintain both a private and a public façade, we regulate privacy by avoiding information disclosure and by selectively disclosing information; *Identity boundary* is the boundary between self and other, and includes the identity of both parties involved in the information exchange; and the *Temporality boundary* is the time-associated boundary that reflects how current privacy management is oriented towards events in the past and future. The tensions of the three privacy boundaries are not resolved independently; they interrelate and influence each other mutually as parts of the same continuous privacy process.

IT has the ability to disrupt and destabilize regulation of the boundaries by a repertoire of potential roles in the privacy process: as causing change, disruption, or establishment of boundaries; as spanning boundaries; as a mean to manage boundaries; or as process context. The concept of boundaries can help us understand the different roles technology can play in the privacy process. Technology itself 'does not directly support or interfere with personal privacy; rather it destabilizes the delicate and complex web of regulatory practices' (2003, p. 133). **Table 2** summarizes central aspects of the concept of privacy boundaries.

Boundary	*Goals in tension*	*Purpose of regulation*	*Samples of disruption*
Disclosure boundary	privacy vs. publicity	controlling the degree of information disclosure	· information disclosure by others (e.g. friends/ third party) · information persistence
Identity boundary	self vs. others	controlling the display of identity and others' interpretations of our self	· desituating information (e.g. time, place or intention lost in mediation) · information persistence
Temporality boundary	past, present and future interpretations of and actions upon disclosed information	controlling the current privacy process in light of experiences of and expectations to interpretations of disclosed information	· the rapid distribution of information · information persistence

Table 2: Privacy boundaries in the 'Privacy for a Networked World' framework

Palen and Dourish also introduce the concept of *disclosure genres*, which are patterns of privacy management that represents a given point of balance between the three privacy boundaries. 'At any given moment, the balance between self and other, privacy and publicity, and past and future must have a single coherent and coordinated resolution' (2003, p. 133). Genres are socially constructed, and

reflect that there is a relationship between how we disclose information and our expectations of the use of it. These patterns of privacy management set expectations around a given technology arrangement, and contribute to its integration into recurring social practices.

This analytical framework present a more nuanced understanding of privacy issues than some traditional concepts of privacy[27]. The perspective covers the users' need to protect and shield personal information on the one hand and their deliberate use of information technology for social purposes, on the other. By viewing privacy as a social, dynamic and dialectic process in its real-world contexts, this perspective turns focus to users coming to encounters with technology bringing their whole life. These concepts can assist analysis of privacy in identifying the social arrangements implicit in a given technology design, and in determining if these implicit arrangements match the actual expectations that users bring into their interactions with technology.

3.3 Understanding user experiences

Historically, there has been a high attention in HCI research on the instrumental and technical aspects of technology; on individual problem solving, user goals, task flows, utility, as well as on traditional usability concepts[28]. Technological developments have increased the focus on the non-instrumental qualities of the technology. The use contexts and application types brought in by leisure use of technology, has strengthened the expectations to the esthetics, ethics, and emotions of the users' interactions. And research in this area has contributed to an increasing understanding of the correlations between usability and user experience, and of how non-instrumental aspects tend to impact measurable, instrumental outcomes (Löwgren, 2013; Sharp, et al., 2007).

However, exploring the concept of user experience is not new in HCI. From the early 80's researchers have been trying to approach this concept (Blythe, Overbeeke, Monk, & Wright, 2005, Introduction). One reason for the rather slow adoption of this as a research topic are the lack of clear concepts and models, and the problems of measuring user experiences, as opposed to usability. In the last decade, several researchers have been aiming at clarifying this concept.

Norman (2004) recognize both cognition and emotions as important for users' assignment of meaning and value to an interaction. His three-layered, hierarchical model for emotional design reflects a close relation between these two. The model, based on the last decades of research in cognitive science, describe three layers referring to different levels of brain activity. The lowest,

[27] like views of privacy as a static, rule-bound process, a process of social withdrawal aimed at protecting information against surveillance and misappropriation

[28] effectiveness, efficiency, learnability, memorability, usefulness and security (Sharp, et al., 2007)

visceral level is the affective level. The visceral level communicates with the middle, behavioral level, and both levels receive signals from the sensory system of the body. Based on this input, these two layers control the body's motor system. The upper, reflective level, intellectualize the activity registered and processed in the two lower levels. Together, the three levels of brain activity controls human behavior and emotions, and good designs should aim at an integration of the three.

Hassenzahl, Diefenbach, and Göritz (2010) have contributed in the exploration of the concept of the user experience, by construing an explanatory model of experience. Hassenzahl (2013) describe experience as subjective, holistic, situated, dynamic, and worthwhile. He separates *experience*[29] (meaningful, personally encountered events) from the *knowledge* coming out of the experience[30]. He further separates the *immediate, moment-by-moment experience* from our *memorized stories from experiences*. A similar distinction as the latter is made by Forlizzi and Battarbee (2004, p. 263). In their interaction-oriented approach they separate *an experience* (an experience with a known beginning and end, which may inspire behavioral and emotional change) from *experience* (the constant, conscious stream of self-talk in product interactions). In their user experience concept, Forlizzi & Battarbee include the user's overall conceptions of quality of the product interaction, as well as the emotions and reactions evoked in the user during an interaction.

The sensual and emotional aspects of the users' interaction can be difficult to understand, to get access to, and to represent in a manner suitable for systematic analysis. McCarthy & Wright introduce an integrated framework to support this process: The 'Technology as Experience' framework (John McCarthy & Peter Wright, 2004; John McCarthy & Peter Wright, 2004; Wright, McCarthy, & Meekison, 2005). In this framework, four characterizing aspects (threads) and six central (meaning-making) processes of the user experience are explored. In Wright, et al. (2005), *experience* is separated from the *knowledge* that come out of it, by referring to the confusion of the user experience concept with concepts like subjective feelings, behavior, activity, social practice, and knowledge. The user experience has commonly been treated as an individual construct in the HCI research literature. An individual-centered view may leave out qualities like ethical implications and communication, which are typically social or communal by nature (Löwgren, 2013). McCarthy and Wright's pragmatist view is rooted in second generation HCI, and by focusing on the felt experience in a social and cultural context, they bridge the individual to the collective (Bødker, 2006). In the following subsection, their framework is presented in more detail.

[29] in Norwegian: opplevelse, in German: erlebnis
[30] in Norwegian: erfaring, in German: erfahrung

3.3.1 Technology as Experience

The "Technology as experience" framework is developed to see relationships between people and technology in 'all their potential value, meaning, and vitality' (John McCarthy & Peter Wright, 2004, p. 79). People interact with technology in more and more areas of their lives, and a range of different technologies are deeply embedded into many peoples everyday lives. We not only use technology, we live with it. Our interaction with technology is imbued with values, needs, desires, and goals, and technology use become a 'felt' experience to the user. To understand users' behavior, their preferences and choices, it is vital to focus not only the rational, logical, and utilitarian considerations of technology use, rather we should look towards the *sensual*, *emotional*, and *intellectual* aspects of the interaction together, to understand the users' experiences in a holistic perspective. And further, in the interaction with technology, our subjective *values, needs, desires,* and *goals* contribute to the *meaning* we make of the experience, as do the *cultural context* in which the experience takes place.

This holistic view on the user and the interaction reveal the image of an experience as more than the mere activities taking place within the start and the end of an interaction. A basic foundation for this framework is the recognition of users' experience as extending the current use situation:

...we also recognize that the feeling-life does not begin and end with the immediate quality of an experience, rather it extends across space and time to the sense we make of experience in terms of our selves, our culture, and our lives (2004, p. 42)

To support the analysis of experiences from this holistic perspective, McCarthy and Wright present ten framework components interwoven to an integrated whole: the four threads of experience, and the six sense-making processes.

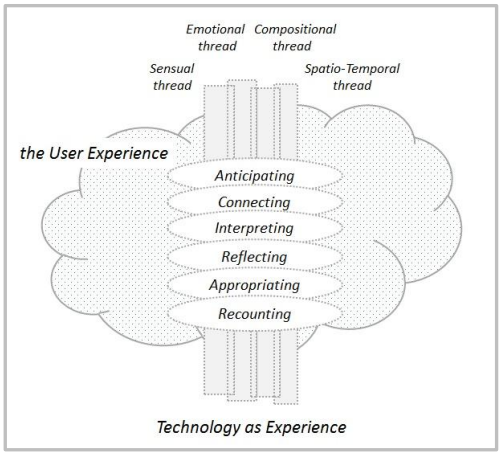


Figure 6: Technology as Experience – an integrated framework

The *four threads of experience* are the *compositional* thread (seeing the elements of an experience as a coherent whole), the *sensual* thread (looking for feelings associated to the design and the overall atmosphere), the *emotional* thread (analyzing the emotions that color the experience), and the *spatio-temporal* thread (observing effects of time and place). The authors characterize these four threads not as fundamental elements of an experience, rather as ideas that contribute to sensitize analysis to the various aspects of the experience.

Weaving the four threads together, the *six sense-making processes* remind us of further aspects to look for when analyzing experiences; *anticipating* (bringing prejudices into the experience), *connecting* (immediate sensing the situation), *interpreting* (working

out what is going on and how we feel about it), *reflecting* (examining and evaluating the interaction), *appropriating* (aligning the new experience with earlier experiences and with our sense of self), as well as *recounting* (telling stories about the experience). These processes are not mutually exclusive; they do overlap, and no clear boundaries between should be expected to be found.

The four threads provide different perspectives for viewing the user experience in analysis and the users' meaning-making is emphasized in the six processes. Yet, instead of isolating separate elements of experience, McCarthy & Wright focus on bringing out the interaction and interdependencies between the framework elements: '[A reductive approach] is not our intention. Rather we intend to connote a space within which things can be juxtaposed, related, separated, coalesced, but never isolated' (Wright, et al., 2005, p. 46).

The ten framework components help us focusing studies of the people-technology relationship on the emotional quality of the interaction. By providing pragmatic tools for thinking, the framework supports the researcher in considering the emotional, intellectual, and sensual aspects of experiences with technology. **Figure 6** illustrates the framework of interwoven components, as I see it.

3.4 Theoretical perspective for this study

The main focus of this study is how users' privacy literacy[31]affects their privacy decisions. Based on an instrumental view of users, fact-based knowledge of privacy has been subject to investigation. But privacy decisions are not always rational (section 2.3); this inspires a look for further factors with the potential of influencing users' decisions.

Mathiasen and Bødker (2008) found that users' experiences of security in interactions differed from their actual security situation; being secure was not the same as having a secure experience. To the extent that privacy decisions are influenced by a privacy experience diverging from users' actual privacy situation, decisions may be inadequate to protect privacy. In this light, the role of experience aspects like emotions, reflections, attitudes, and former experiences are subject to investigation in this study, as well.

Experiences are not knowledge (section 3.3), but knowledge may come out of user experiences and supplement users' fact-based knowledge of privacy. The *Technology as Experience* framework provide ways to get access to experiences and help preserving a holistic view of users and the way they make meaning of their interactions. This perspective was chosen as part of the theoretical foundation for this work.

[31] within educational research the literacy concept is debated. Here, the concept is used merely as a generic term for competences assumedly strengthening users' capability to protect their privacy

To complement this experience-oriented perspective, the *Privacy for a Networked World* framework from personal privacy research has been chosen. This framework '…takes a step back and asks how users come to manage and know about privacy' (Lampinen, Stutzman, & Bylund, 2011, p. 2442). Personal privacy research focus how people manage their privacy with respect to other individuals, and provides models suitable for explaining privacy decisions which are highly situational and depending upon the social and historical context of the people involved (Iachello & Hong, 2007). This situation is common for many interactions in social media; information of various kinds is shared, often spontaneously, to audiences from a mix of social contexts. The Privacy for a Networked World framework is directed at capturing the dialectic, social, and temporal aspects of privacy interactions in particular; aspects that this study has been aimed at investigating.

The two perspectives are turning to the social and interactional to understand users' technology use, and can increase sensibility to the dynamic and dialectic aspects of users' encounters with technology. And also the focus on identity found in both perspectives may be important for an analysis of users' privacy decisions.

This study focuses the consequences of privacy breaches for integrity (**Figure 1**), and typical security issues are included to the extent that they are targeted at privacy (section 2.1). As security mechanisms are the basic tools for privacy protection, privacy and information security are closely related. This is the reason why much of the HCI privacy literature is intertwined with that of usable security (Iachello & Hong, 2007). And further, a common understanding of the term for privacy used in the interviews, *personvern*[32], includes issues traditionally thought of as information security issues. Assumedly, from the informants' point of view, the concepts of privacy and security overlap; it all comes down to a question of protecting data against coming into the hands of unauthorized others.

This work is assumed to fit into the HCI research traditions personal privacy research and usable security.

[32] for further details about the Norwegian privacy concept *personvern* refer f.ex. to (Personvernkommisjonen, 2009) and to (Schartum & Bygrave, 2011)

This page is intentionally left blank.

4. METHOD

A research method can be understood as a strategy of inquiry upon which the research design is based. This strategy includes a selection of techniques for handling of empirical data, as well as a set of research practices and an underlying philosophical stance (Bryman, 2008). This chapter reviews the methodological choices for this study. As a start, section 4.1 details the problem area and the research questions. Section 4.2 describe the qualitative and interpretive approach chosen for the study, and section 4.3 elaborate how two pilot studies ahead of the main study was used to test and develop the research design methodologically as well as thematically, in an iterative and data-driven process. Finally, section 4.4 describes the data collection process based on qualitative interviews and a purposive sample where participants[33] were chosen based on the criteria age and level of Facebook activity. This section further details how analysis of data was carried out in two main phases; a qualitative phase succeeded by a phase characterized by the use of more quantitative analysis techniques.

Research projects collecting personal data are obliged to apply for approval of research design ahead of data collection (NESH, 2006). This study has been approved by the Norwegian Privacy Ombudsman for Research (NSD, 2011). In the research process, protection of the participants' integrity and rights to co-determination has been emphasized, by acquiring informed consents ahead of data collection, as well as by aiming at conducting interviews and transcribing, analyzing, and presenting the empirical material in a respectful way. Interview data has been anonymized and stored in compliance with NESH guidelines.

4.1 Basic assumptions

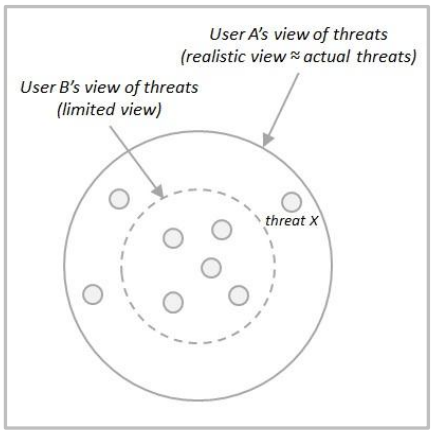


Figure 7: Different views of threats in the interaction

This study focus on cases where social media users disclose personal information in ways that expose this information to risks. I see two problematic situations potentially causing non-secure behavior. **Figure 7** and **Figure 8** draw a picture of the problem area, and illustrate a situation where two users (A, B) are both exposed to a threat (X) in their interactions.

The first problem relates to the privacy decision that is likely to follow a user's recognition of an actual threat. User A is aware of threat X, and this threat is included in user A's *realistic view* of threats (**Figure 7**). When user A recognizes the threat, she is

[33] the terms participant and informant are used interchangeably throughout this presentation

facing a privacy decision (**Figure 8)**. She can choose to take protective actions to prevent the negative consequences of the threat (giving up sharing the information; adjusting her privacy settings before sharing; or choosing other protective action available), or alternatively, she can choose to ignore the threat and go on disclosing the information without any protective actions. Users ignoring a recognized threat deliberately expose themselves to risks. To prevent blunders, violations, or dangers associated with non-secure behavior, we need to learn more about these decisions. In this study, I raise the question if inadequate KNOWLEDGE of privacy can explain why some users in this way deliberately expose their personal information to risks?

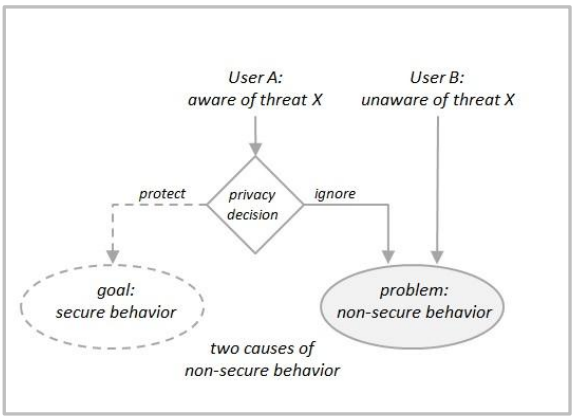


Figure 8: Problem overview: two sources of non-secure behavior

The second problem relates to the situation where a user is unaware of her information being exposed to threats. As threat X is outside of user B's *limited view* of threats (**Figure 7**), she is not likely to reach a privacy decision (**Figure 8)**, and remains unaware of her personal information being exposed to the risks represented by threat X. Again, I raise the question if inadequate KNOWLEDGE can explain why some users in this way unwittingly expose their personal information to risks?

Additionally, I raise questions about the role of the users' EXPERIENCES for their privacy literacy. For example, can an experience of feeling secure influence the user to make a non-rational decision; choosing to disclose information even when her fact-based knowledge calls for the opposite? Or, can elements of the user experience explain why a user is unaware of a given threat in her interaction? And further, the users' previous experiences, do these bring in knowledge that is important for the two situations?

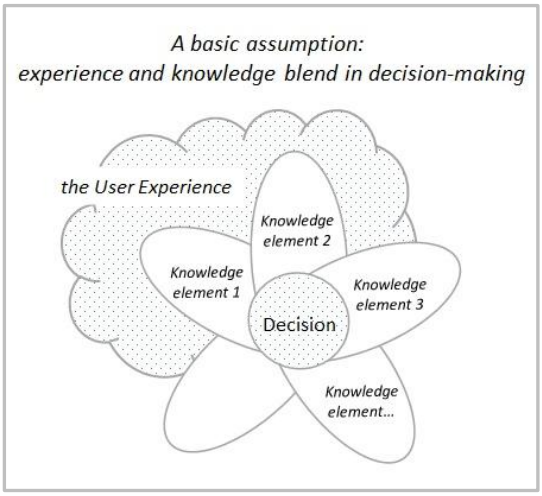


Figure 9: A basic assumption for privacy decisions

Based on the theoretical perspective drawn up in the previous chapter, **Figure 9** illustrates a basic assumption for the following exploration of users' privacy literacy; EXPERIENCE and KNOWLEDGE blend in decision-making. The users' privacy decisions are framed by the experience they have when interacting. Elements from this user experience potentially influence how they perceive and manage privacy related situations. And, previous user experiences can influence the current, by bringing in new knowledge to the users' privacy literacy.

This assumption reflects an understanding of knowledge and experience as complementary in users' privacy literacy; an understanding of emotional elements from the user experience as supplementing the user's rational, fact-based knowledge. Working with the empirical material, I have focused on 1) mapping out the participants' knowledge based on a selection of privacy knowledge elements; 2) exploring a possible relation of this knowledge to the participants' choices in actual privacy situations on Facebook; and 3) exploring the participants' user experiences to uncover elements of these potentially influencing their privacy situations further.

4.2 A qualitative and interpretive approach

This work has been based on a qualitative and interpretive approach. One of the most recognized advantages of using a *qualitative* research approach is its potential to open up for unexpected knowledge. The research process is flexible, and research design is commonly revised throughout the project as new knowledge is required, and the approach is useful in research in areas needing to develop new hypotheses and insights (Bryman, 2008). A qualitative approach is particularly suitable in studies focusing on capturing people's experiences, values, attitudes, and interactions in a socio-cultural context, and to explore the social meanings they assign to phenomena in their lives (Malterud, 2002). An *interpretive* perspective is commonly associated with the conception of reality as a social construct. Rather than owning an objective existence in reality, a social phenomenon is seen as produced and continually revised through social interaction and the meanings that people assign to it through their interaction (Walsham, 1995). A qualitative and interpretive approach is well suited for this study's research questions, related to participants' meaning-making in their privacy experiences, 'imbued with values, needs, desires, and goals' (John McCarthy & Peter Wright, 2004) within a social and cultural context.

4.2.1 An iterative, data-driven process

A qualitative research style usually implies a research process based on inductive reasoning, building theory from empirical data (Bryman, 2008). A practice of iterated collections and analyses of empirical data, adjusting interview guide and sampling strategy when needed, can contribute to strengthen the study's overall validity (Malterud, 2002). An inductive, data-driven and iterative approach has been employed in this study. With two pilot studies[34] preceding the main study, three main iterations has been run through. Additionally, smaller iterations has been done within the frames of the main study. Qualitative interviews have been used as the primary method for data gathering.

[34] a small, trial run of the study, to make sure that the proposed method is viable (Sharp, et al., 2007)

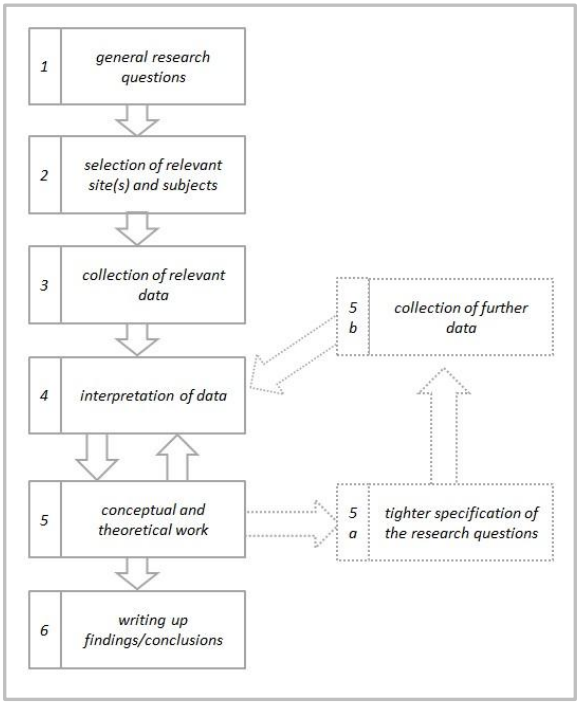


Figure 10: An outline of the main steps in qualitative research (Bryman, 2008)

As illustrated in **Figure 10** (depicting Bryman, 2008, figure 16.1), such iterative approach to data collection and data analysis is commonly employed in qualitative research. The figure reflects the iterative refinement of the thematic aspects of a study, focusing on tighter specification of the research questions in the iterations, followed by collection and interpretation of further data.

In this study, research design has developed iteratively along the *methodological* as well as the *thematic* dimension. Methodologically, research design developed iteratively by a reconsideration of the chosen data collection method after pilot studies, as well as by an iterative development of the data gathering techniques employed in the interview guide. The thematic aspects developed iteratively by a gradual refinement of research questions and the interview guide. The remainder of this chapter details these developments further.

4.2.2 Data collection method

If you would like to know how people understand the world and their lives, why not ask them? This question[35] opens Kvale's book about the qualitative research interview. Conversation is a basic form of human interaction, an interaction providing possibilities to learn about other people, as well as a way to get access to their experiences, emotions, attitudes, and the world they live in (Kvale, 2001). In HCI, both quantitative and qualitative techniques have been used to gather users' preferences and attitudes to privacy. The qualitative approaches are most used in probings of personal privacy dynamics, and the personal interview is a commonly employed method (Iachello & Hong, 2007).

The method selected for data collection should be the most relevant for, by this revealing the best validity for, the research questions (Bryman, 2008; Malterud, 2002). Based on an expectation that the conversational form of personal interviews would give access to the knowledge, experiences, emotions, and attitudes focused by the research questions, *qualitative interviews* were chosen as the primary data collection method for this study.

[35] translated to English, Kvale's original quote in Norwegian

At an early stage, the use of focus groups was considered. However, due to the risk of poor data from this method for a rather sensitive research topic like privacy (Iachello & Hong, 2007), the method was rejected. Another approach considered at that time is contextual interviews. Privacy can be hard to rationalize (chapter 2); what people say they want not uncommonly differs from what they actually do in practice. In contextual interviews, the researcher watches the participants' actual use of the technology. Choosing this method could solve the need for sufficient context for questions about privacy (Iachello & Hong, 2007), and would include a potentially profitable element of observation in the interviewing process. However, asking participants for access to their day-to day use of their personal Facebook account would require them to share quite personal information with the researcher. By this reason, contextual interviews were not chosen as the primary data collection method. Finally, a *triangulation*[36] of methods, by combining qualitative interviews with a diary study, was decided upon and tested out in a first pilot study, unfortunately without any success. Experiences from the two pilot studies are further detailed in the next section.

To account for the above mentioned need to include sufficient context for the interview questions, specific cases in the form of *use scenarios* were included in the interview guide. Participants were invited to discuss these concrete, but impersonal cases in the qualitative interviews. Use scenarios were employed in a way that has a lot in common with the vignette technique used in surveys. Finch (1987) accentuates several advantages associated with the use of vignettes to get access to attitudes in a sensitive area; they clarify questions by anchoring them in specific situations, they permit a certain amount of distance between the question and the participant, and result in a less threatening context. And further, to get access to elements of the participants' actual behavior on Facebook, the interviews were focused on their *static behavioral choices in the form of privacy settings*. A walkthrough of a selection of their privacy settings is assumedly found less sensitive for participants than disclosing the personal information they dynamically share with their friends in their daily use of the Facebook service.

4.3 Pilot studies

The study was originally designed to make use of *in-depth interviews preceded by a diary study*, where the participants' own selection of authentic examples of privacy-sensitive situations from daily Facebook use was to be included. This combination of methods, by Bryman (2008) described as diary interviews, were successfully employed by Mathiasen and Bødker (2008) in their study of secure

[36] the process of combining several data collection methods (Bryman, 2008)

experiences. The data cross-checks involved in triangulation of collection methods can provide additional validity to the empirical data material.

For a three weeks period, the diary interview design was tested out in a first pilot study. Participants were asked to report examples of situations they perceived as potentially sensitive to their own privacy, or to the privacy of others. Data could be reported quite flexibly: as text and images in the form of notes, text messages, emails, photos, or screen shots. The goal was to grasp concrete situations that could be used to elicit the participant's thoughts and attitudes in subsequent personal interviews. Written instructions were provided to the participants, describing the intentions and the procedure for the pilot. However, participants reported that no privacy-sensitive situations were observed during the period, and this pilot of diary interviews ended up giving no empirical data.

Based on this experience, the choice of data collection method was reconsidered. The diary study part was abandoned. Personal interviews was chosen as the primary data collection method for the study, based on an expectation that face-to-face contact with the informants could reveal the empirical material needed to answer the research questions. To find out if this expectation was valid, I decided to do a second pilot study to get thorough experience with qualitative interviews. A preliminary version of the interview guide was developed based on the research questions at that time, and four participants volunteered as test interviewees in this second pilot; two adults and two teens. Each pilot interview lasted for 1 hour +/-, and the interviews were audio recorded. The second pilot study provided an opportunity to test out different techniques for getting access to the informants' attitudes, experiences, and reflections, as well as a way of iteratively developing the interview guide and the research questions. This iterative development of the research design is described in subsections 4.5.1 (thematic developments) and 4.5.2 (methodological developments), respectively.

4.3.1 Developing the research theme

The thematic aspects of the study developed gradually throughout the research process. Pilot studies, in particular, influenced the formulation of research questions and interview guide.

The earliest version of the interview guide was based on research questions not yet narrowed down to issues related to privacy literacy. At this stage, the research questions were raising general questions to which factors that influence our privacy experiences and privacy decisions on Facebook. In the pilots, the impression of the knowledge factor's potential importance was strengthened. Some interview questions did not work out very well, possibly due to an implicit expectation to the participants' level of knowledge. Knowledge aspects like the third parties' access to personal data; the potential cooperation between commercial actors on the Internet; and the possibility of combining data from multiple online sources, appeared as potentially significant. This increased focus on knowledge provoked curiosity as to the relations between knowledge and experiences, and the possible influences

of these on the users' privacy-related interactions in social media. On this background, four main themes for the study were described, and later versions of the interview guide were built around these themes [37]. The four themes are: 1) *General information of Facebook usage*; 2) *Skills, knowledge & competences*; 3) *Behavior, choices & attitudes in actual use situations*; and 4) *Experiences, reflections, & motivation*. The presentation of findings in section 5 is organized according to the four themes.

In general, the interview guide was developed throughout the second pilot study. Some revisions were applied in relation to the first four interviews of the main study, but following these, the interview guide was kept unchanged for the rest of the data collection process. The changes applied in the main study was mainly about changing sequence of some questions (leaving the most sensitive questions to the end of the interview, for example), as well as leaving out and reducing the volume of some questions to avoid too lengthy interviews. The research questions were revised recurrently throughout the research process as well, gradually shifting against their final state (section 1.2), where they are focusing on privacy, knowledge, user experiences, behavior, and age.

4.3.2 Developing the research method

An important lesson learned from the pilot studies is that privacy is a complicated area for the users, and a challenging theme to investigate. As mentioned, the absence of empirical data in the first pilot brought forward a reconsideration of the main data collection method for the study. In the second pilot, conducting the interviews revealed a difficulty of enticing free reflections related to this topic. These difficulties appeared as partly related to the privacy concept's sensitivity, and partly related to the rather abstract character the ideas of this concept tend to have in peoples' minds. To improve the odds of collecting a fruitful empirical material in the main study, I found it useful to put some effort on refining the interviewing techniques throughout the second pilot study.

Subsequent to each interview, the interview guide was reviewed and revised, and gradually became more compatible with the complexity of the research topic. Reflections of the efficiency of different questions gave rise to the testing of different interviewing techniques, and also new questions based on thoughts and reflections from the pilot study participants were merged into the guide. The most important methodological changes to the interview guide in this phase was:

- *Clarifying and simplifying questions* making them understandable for informants of all ages and knowledge levels
- *Repeating questions from different angles* throughout the interview, to increase validity of data

[37] some notes from this process are included in appendix A (Norwegian only)

- *Extend use of direct questions and concrete examples* giving the informants explicit starting points for reflections
- *Incorporating new questions* based on thoughts and contributions from the participants
- *Testing and incorporating a diversity of interviewing techniques* in order to elicit participants' attitudes and reflections. **Table 3** present techniques tested with success, and included in the interview guide

Technique	*Description*
General impersonal scenarios	General examples not related to persons. Present examples of general privacy-sensitive situations, impersonal, but assumedly relevant to the participant. Ask for reflections, emotions, and assumed choices in a similar situation.
Specific impersonal scenarios	Concrete examples of other people's privacy choices. Present examples of other peoples' privacy-sensitive situations, assumedly relevant to the participant. Ask for reflections, emotions, and assumed choices in a similar situation.
The outsider perspective	Viewing self throught the eyes of a potential perpetrator. Ask the participant to view herself through the eyes of a potential perpetrator. Ask for reflections and perspectives of themselves in the perspective of this malignant outsider
Rankings by use of Likert scales (scenarios, self-reported knowledge, etc.)	Present a liste of (e.g.) privacy-sensitive scenarios. Ask the participant to rank these by level of gravity using a Likert scale. Ask for reflections and emotions related to each scenario
Review of privacy settings	Walkthrough of the informants own privacy settings on Facebook. Ask for reflections, emotions, and reasons for choice of settings.
Other aspects	• Inviting a relaxed and open-minded atmosphere, where - it is comfortable to talk about unsuccessful situations, undesirable disclosure, etc., - focus is kept on positive incidents and situations the participant handled with success, as well • Varying focus between threats and incidents on a general level, and more concrete situations requiring the participant to focus on own reactions, thoughts, and choices • Presenting concrete examples early in the inteview, to concertize and evoke the participants' thoughts and reflections on the topic of privacy

Table 3: Interviewing techniques

Likert-type rating scales are good to elicit a range of responses that can be compared across respondents, and is an essential tool in HCI for measuring aspects as opinions, attitudes and beliefs related to the user experience (Kaptein, Nass, & Markopoulos, 2010; Sharp, et al., 2007). The use of these scales in interview questions introduced a simple, quantitative element to the study. For some questions, the participants were asked to choose between a number of predefined answers, usually five alternatives. And commonly, they were asked to complement their choice by thoughts and reflections on the issue, too. In this way, some quantitative value was assigned to the qualitative nature of the data in the study.

In the process of revising the interview guide, the guide gradually became more structured. To avoid closing the dialogue too much to my own, predefined categories, focus was kept on leaving

room for reflections in answers by extensive use of follow-up questions, and by shifting between closed[38] and open questions.

4.4 Main study

When no new information is brought in by collecting additional data, the point of saturation (informational redundancy) is found (Qual. Research Guidelines Project, 2011). The process of sampling, collecting, and analyzing data in pilots and in the main study, went on until this point of saturation was reached. Interviews, review of audio recordings, and transcriptions were processed in parallel throughout the data collection process, allowing information from high-level analysis to inform subsequent data collection decisions. As detailed previously (4.3), the data collection process was designed throughout the pilot studies primarily. This section reviews the sampling part of the data collection process; how sampling was designed, and how this design translated into practice (4.4.1). The subsequent process of detailed data analysis was separated into two main phases; a first, qualitative phase where the method *Systematic Text Condensation* was employed, was succeeded by a second phase characterized by the use of more quantitative analysis techniques. These two analysis phases are further described in subsection 4.4.2.

4.4.1 Data collection

4.4.1.1 Designing the sampling process

Purposive sampling is the process of selecting participants purposively in order to recruit the participants most relevant for the research questions. This is the most often recommended approach in qualitative research, attempting to 'establish a good correspondence between research questions and sampling' (Bryman, 2008, p. 458). The sampling strategy chosen for this study initially aimed at combining two purposive sampling methods; intensity sampling and snowball sampling.

Intensity sampling is 'the process of selecting or searching for rich or excellent examples of the phenomenon of interest' (Qual. Research Guidelines Project, 2011), where focus is kept on information-rich, but not extreme cases. To capture these rich examples of the phenomenon of interest, a set of *selection criteria* are specified; for this study defined as age and level of Facebook activity.

The major selection criterion related to participants' *age*. Young people are early adopters of social media, and from the very beginning Facebook was an arena for the youth, primarily. This trend has changed over time, and by the end of 2009, adult users made up the strongest growing group of users (Brandtzæg & Lüders, 2009). Assuming that an individual's degree of experience with social media

[38] e.g. questions based on the use of Likert scales, where informants indicate their level of agreement with a given statement by way of an ordinal, usually five-value, scale (the use of Likert scales are furthered detailed in subsection 4.4.2)

influences her privacy choices and strategies, the age selection was aimed at recruiting users below 20 years of age, and another group of users above 45 years of age, in order to do age-based comparisons of the findings within the two groups.

Another selection criteria used has been the participants' *level of Facebook activity*, defined as a minimum Facebook friends count of 150[39], a minimum number of 5 weekly logins, as well as describing their own Facebook activity as 'using Facebook actively' (determined at the participants' own discretion). The sampling strategy included an additional selection criterion of former experiences (aiming at including participants with negative privacy experiences from Facebook use). However, sampling by this criterion was not successful in practice.

In *snowball sampling*, the information-rich cases described by the above criteria, would be identified by the benefit of people well-informed about the phenomenon, and in this way able to point out others as good examples for study. Following a chain of people leading up to such cases, this method can be useful for identifying a small number of key cases that are exemplars (Qual. Research Guidelines Project, 2011). Snowball sampling is commonly used for populations (like the huge, diverse, and volatile population of Facebook) lacking a sampling frame[40] from which a specific sample can be selected.

Some general challenges associated to this choice of sampling strategy are discussed in chapter 6.

4.4.1.2 Sampling in practice

As few people volunteered to participate, recruiting informants for the study turned out as quite challenging, assumedly due to the topic of the study. As to *intensity sampling*, the two selection criteria age and level of Facebook activity was presented in the invitation[41] to participate, and was successfully attended to in the sampling process. Selection based on the third criteria, former experiences, was planned for after snowball sampling. This was based on an expectation of participants to register in sufficient volumes for further selection. In practice, however, this strategy was too optimistic; the snowball never started to roll. Several attempts to roll the ball gave few results in both age groups, and the volumes of volunteers were not sufficient for selection based on the third selection criteria. In this situation, the *snowball sampling* strategy was abandoned[42].

For recruiting of adults, the invitation was presented on a dedicated web page, and the link to this page was distributed to a large number of randomly chosen people. The link was spread through

[39] the average count of Facebook friends for a Norwegian user at the time of recruiting was in the range of 150-250 users
[40] a listing of all units in the population (Bryman, 2008)
[41] appendix B (in Norwegian only)
[42] out of 18 participants, only 2 were recruited by snowball sampling

different channels; Facebook, Twitter, as well as through personal contacts who kindly contributed by distributing information about the study in their own personal Facebook networks. Additional contacts with organizations with large audiences of relevance for this study, did not give results. In time, however, the extensive distribution of the invitation paid off, as adult participants from various contexts gradually volunteered for participation. In recruiting of youth participants, I was given useful support from the administration of a local high school. The invitation was distributed to all pupils through the school's intranet, and participants were included in the study based on a 'first come, first served' principle.

In sum, sampling for this study is based on *intensity sampling* by the two criteria *age* and *level of Facebook activity*. Recruiting was sufficient to reach the level of saturation in data collection and analysis, but the total volumes of volunteers were not sufficient for selection based on the third selection criteria; former experiences. The research questions were adjusted according to this situation. The two groups of informants are presented in more detail in section 5.1.

4.4.1.3 Interviews

Data collection for the main study was carried out winter 2011/2012. 19 informants were interviewed, and all interviews were audio recorded. Due to technical problems, one recording was rejected, and data from 18 interviews are included in the empirical material for the study.

As the interview guide, the research questions, and the interviewing techniques had been testet and refined iteratively in the two pilot studies, no major changes to the research design was introduced in in the main study. Some adjustments applied to the interview guide as a result of the first 3-4 interviews (section 4.3). Following these initial adjustments of sequence and scale of the collection of interview questions, interviewing typically entailed asking identical questions in a predefined sequence. As the interview guide additionally were combining open and closed questions, the interview process was carried out as one might characterize as semi-structured interviews with some structured features.

4.4.2 Data analysis

In qualitative analysis, large volumes of data can be input to analysis. A main challenge for the researcher is to find a good way of coping with these volumes. A systematic approach to data analysis will expectedly contribute to the quality in the final results. Systematics will support in keeping an overview of the material and the analysis process, as well as in taking a step backwards in analysis whenever this is useful. Experiences from the second pilot indicated an approximate length of each interview of 1 hour. In the main study, interview lengths varied, depending on how much reflections and thoughts each participant wanted to share. 18 interviews resulted in approximately 22 hours of audio recordings. To handle this volume, a systematic approach to data analysis was required. The

empirical material was thoroughly prepared for analysis, and the choice of analysis method accommodated for the goal of the study, the qualitative nature of the data, as well as the theoretical foundations for the data analysis. This subsection deepens these choices and details how the analysis was carried out in practice. The theoretical model developed to support data analysis and the procedures related to the problem of measuring knowledge are presented, as well.

4.4.2.1 A data-driven approach

The 'Technology as Experience framework is 'not a method for analyzing experience, rather it is a set of conceptual tools or a language for thinking and talking about experience' (Wright, et al., 2005, p. 52). And as to 'Privacy For a Networked World', researchers within the HCI community currently focus on bridging the gap between theory and practice related to this framework (Lampinen, et al., 2011). The two theoretical frameworks chosen for this study do not provide detailed instructions for analysis, yet describe ideas, concepts, and a frame of understanding, increasing sensibility to the social, emotional, dynamic, and dialectic aspects of technology use. Lacking well-developed instructions, the data analysis was performed as a typical data-driven process, and more than one analysis method was employed in this process to gain a thorough understanding of the empirical material. Methods and practical analysis procedures are further described in the following paragraphs.

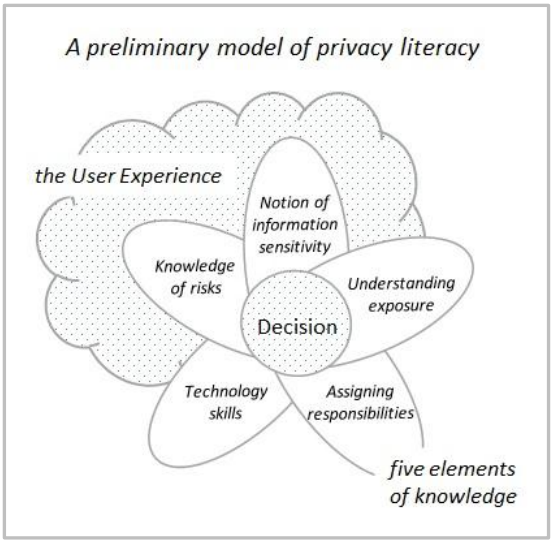


Figure 11: Privacy literacy: A preliminary model

Based on **Figure 9**, a preliminary model of privacy literacy was developed to clarify main focus before entering the data analysis (**Figure 11**). Five tentative knowledge factors was added; *Technology skills; Knowledge of risks; Notion of information sensitivity; Understanding exposure;* and *Assigning responsibilities*. The analysis was concentrated on testing the validity of these knowledge factors, as well as on uncovering potential new pieces of the privacy literacy puzzle. The selection of knowledge factors was developed by reading previous studies of issues related to these issues; research as mentioned throughout this work, as well as in Howe, et al. (2012), and Iachello and Hong (2007). The factors *Understanding exposure* and *Notion of information sensitivity*, in particular, has been inspired by Rotman (2009), as well as by the three aspects of privacy described in DeCew (1997, pp. 74-80).

4.4.2.2 Preparing data for analysis

Before going ahead with the interpretative analysis, raw data was prepared for analysis by transcription and autocoding[43]. This process had a partial overlap with the interview process.

The audio files were transcribed *in verbatim*. A written, word-by-word translation of each file was produced, resulting in complete textual versions of each interview. An audio player software, Express Scribe[44], was used to support the transcription process. Dedicated symbols were used to indicate hesitations, pauses, humor, etc., in the conversation. The transcriptions were given a standardized form as to headings and fonts, in this way suited for import into a CAQDAS[45] tool. NVivo10[46] software was used to autocode the data material.

4.4.2.3 Analysis methods

'Your findings acquire significance in our intellectual community only when you have reflected on, interpreted, and theorized your data. You are not there as a mere mouthpiece.' (Bryman, 2008, p. 554). The empirical material was ready for a process of interpretation and theorizing after transcription and autocoding. At the outset, the analysis process was based on the method *Systematic Text Condensation* (Malterud, 2002, 2003), a method theoretically anchored in phenomenological analysis[47]. This analysis method is well suited for studies like this, aiming at developing an understanding of the informants' experiences and lifeworld in a particular area. It provides a data-driven approach to analysis, making it suitable for studies without a well-developed, instructive theoretical foundation for analysis, aiming at development of descriptions and concepts. And further, it is well suited for inexperienced researchers, as it emphasize reflexivity and systematics rather than extensive theoretical training (Malterud, 2003). In brief, Malterud[48] describes four main phases of data analysis:

1. *Disentanglement: Uncovering core themes*
    - Reading the collection of transcriptions consecutively, to get a general impression of the empirical material. In this process, core themes appear intuitively

[43] in the autocoding process, the material is read into a software tool, and automatically structured. This indexing process assists sorting and organizing the empirical data
[44] http://www.nch.com.au/
[45] CADQAS tool = Computer Aided Qualitative Data Analysis Software
[46] http://www.qsrinternational.com/
[47] as described in Giorgi, A. *Sketch of a psychological phenomenological method,* in Giorgi, A.(Ed.) *Phenomenology and psychological research* (1985)
[48] translated to English, Malterud's original descriptions in Norwegian

2. *Coding: Moving from themes to meaningful concepts*
    - Organizing, sorting, and tagging/coding the data material according to themes. Through identification and classification are relevant parts of the texts separated from irrelevant
3. *Condensing: Transforming codes to meaning*
    - Further abstracting the meaningful concepts from the previous phase. Codes are synthesized and condensed to subgroups through interpretation, and in this process, descriptions of a more general form are developed for each subgroup
4. *Recontextualization: Advancing condensations to descriptions and concepts*
    - Validating of the findings by recontextualizing them to the empirical material and to the theoretical perspective for the study. Selecting quotes to illustrate and anchor the generalized descriptions, developing these into content descriptions for each subgroup

More techniques were employed in the data analysis, as well. After several iterations of the phases of Systematic Text Condensation, the overall picture of the empirical data indicated strong common features within, as well as between, the age groups. To develop this picture further than the mere qualitative analysis provided for, the analysis was continued by use of other, more quantitative techniques. Triangulation of data analysis methods is a common approach in HCI (Sharp, et al., 2007), and its practical application in this study is further described in the next paragraph, Data Analysis in practice.

4.4.2.4 Data analysis in practice

Recurring iterations of data analysis was done in two main phases separated by methodological approach; the first, qualitative phase was followed by a second phase of a more quantitative character.

In the first phase, the four stages of Systematic Text Condensation were applied. As a start, complete set of transcriptions was read consecutively. In this walkthrough, core themes appeared from the material, and were added to themes established ahead of data collection (*Disentangling)*. This step, performed once to kick off the analysis, brought the following tentative themes further to the next phase: *Knowledge vs. Insight*; *Control; Responsibilities; Intimacy, Former experiences; Information types; Attitudes vs. Behavior; Consideration;* and *Trust.*

In the following, focus iteratively shifted between the *Coding***,** *Condensing***,** and *Recontextualization* steps. Codes were gradually developed for each core theme, in a recurring process of splitting, sorting and rearranging the text material. The codes were successively transformed to subcategories, and more general impressions for each subcategory were developed. The theoretical perspective chosen for the study was used as a guide in this process. However, after recurring iterations, the analysis process gradually developed from the qualitative character as Malterud (2003) describes, into a next, more quantitative phase. At the outset, the empirical data had some predefined,

quantitative features, as a combination of Likert scale rankings and free reflections was chosen as one of several techniques in the interview guide (paragraph 4.3.2). And further, as I got more familiar with the empirical material, clear common features became apparent in the data, making them more quantifiable. This subsequent phase of analysis was characterized by counting, comparing, and summarizations in many iterations, recurrently validating the results against transcriptions to ensure they do not disconnect from their origin in the quantification process. The findings of this study are built in a typical bottom-up, data-driven process.

The final results are presented by tables and diagrams, in addition the text-based descriptions commonly characterizing presentation of a qualitative data (chapter 5). Tables and numbers in this presentation are for illustrative purposes only, and claim no statistical significance. The NVivo10 software was used to support efficiency in the sorting and retrieval of data throughout the analysis process. Data was structured gradually throughout the iterations, and to allow for comparisons between age groups, separate, but identical, data structures were developed for the two groups[49]. Management of analysis results was further supported by use of spreadsheets, mindmapping software, and text based descriptions. An analysis log was maintained to keep track of the process. The following paragraph details some aspects of the analysis procedures.

4.4.2.5 A challenge in data analysis: measuring knowledge

As described in the previous paragraphs, a simple version of Likert scale rankings has been used to support measuring of knowledge in this work. For some interview questions, the informants were asked to rank their answers on a five-point scale. This applies to questions related to self-reporting of knowledge in particular, but rankings were used for other questions, as well. In analysis of data, Likert scales were used as a tool for evaluating the participants for knowledge factors not based on self-reporting, rather on the researcher's interpretation and assessment of results. This procedure do not provide objective measures for individuals' knowledge, yet provides a way of quantifying the results which allows for comparisons as well as indicating differences and similarities between individual informants, as well as between the two groups of adults and youths.

The same scale was used in all interview questions based on rankings. The values were generally presented as text values, not as number values. The Likert scale used in interview questions consist of the following five values: very good (5); pretty good (4); good (3); not so good (2); and poor (1). In the presentation of the results, the expressions medium value, weaker, and stronger are used. In these cases, the five values are converted to a three-point scale, in order to set off tendencies in the data. The

[49] one of these data structures is shown in Appendix C

conversion was done by merging value 1 and 2 to *low*, and to let value 3 represent *medium***,** and merging value 4 and 5 to *high*. Generally, and also anticipating the course of events, **Table 4** summarizes the aspects included in the measurement of each of the six knowledge factors of privacy literacy proposed in this study.

4.5 Research method – a review

This study has been carried out with a qualitative, iterative, and data-driven approach to data collection and data analysis. Data was collected in qualitative interviews, and informants were sampled purposively based on their age and level of Facebook activity. The research design was developed gradually, as two pilots were conducted ahead of the main study. Data collection and analysis was done iteratively, and triangulation of methods was introduced in both phases by complementing the qualitative main approach by quantitative techniques.

Knowledge factor	*Component*	*Description*
TECHNOLOGY SKILLS	Technology skills: all areas	the answers in all skill areas were converted from the five-point to a three-point scale as described in paragraph 4.4.2.5. The figure show the distribution of the set of all answers on this three-point scale (in percentage)
	PC and Internet use	self-reported value
	Facebook use	self-reported value
	Facebook privacy settings	self-reported value
KNOWLEDGE OF RISKS	Knowledge of risks (overview)	reflects the final image of knowledge of risks (the adjusted value) converting answers to the three-point scale (see 4.4.2.5)
	Knowledge of risks (self-reported)	self-reported value
	Knowledge of risks (adjusted)	estimated in analysis: the self-reported knowledge of risks was adjusted by individual risk awareness profiles construed by: reviewing complete transcriptions from the interviews, building a qualitative impression of each informant's ○ general risk focus (to what extent are the informant focusing on threats in general and assigning importance to these) ○ knowledge of actual threats (which threats did the informant mention and express familiarity to, and to what extent was each of these assigned importance) ○ attitude to preventive actions (to what extent is the informant prepared to accept the costs related to preventive actions) each individual profile was summarized in text form, and then translated to a risk awareness rank on the five-point Likert scale used in the informants' self-reports
NOTION OF INFORMATION SENSITIVITY	Self-identifying information Access-enabling information Expressive information	estimated in analysis: by reviewing complete transcriptions, a qualitative impression was built of each informant's ○ each participants' view of the importance of protecting the respective information the answers were ranked on a three point scale: *High, Medium, Low*
UNDERSTANDING EXPOSURE	Understanding exposure in general	estimated in analysis: by reviewing interview data, building an impression of each informant's ○ understanding of the general concepts data persistence and data virality ○ consideration of these aspects in privacy decisions and the answers were ranked on a three point scale: *High, Medium, Low*
	Understanding exposure in Facebook Core	estimated in analysis: by reviewing interview data, building an impression of each informant's ○ understanding of the level of exposure allowed for in default privacy settings for own Facebook wall (example) ○ understanding of the change in privacy context when sharing on another user's Facebook wall (example) ○ understanding of Facebook's privacy settings, and how these are configured (interview data) and the answers were ranked on a three point scale: *High, Medium, Low*
	Understanding exposure in Facebook Platform	estimated in analysis: by reviewing interview data, building an impression of each informant's ○ understanding of increased exposure and potential risks related to accepting apps unconditionally (example) ○ understanding of increased exposure and potential risks related to accepting app asking for extensive auth.'s (example) ○ understanding of the relation between Core functions and Platform functions on Facebook (interview data) and the answers were ranked on a three point scale: *High, Medium, Low*

Knowledge factor	*Component*	*Description*
	Understanding exposure in Facebook Platform revisited	estimated in analysis: after the walkthrough of the informant's actual exposure in Facebook Platform, the value estimated for Exposure in Facebook Platform was adjusted for each informant ○ being unaware of central aspects of own exposure in Facebook Platform ○ expressing an attitude and experience of own exposure in Facebook Platform in mismatch with the actual exposure
ASSIGNING RESPONSIBILITES		estimated in analysis: by reviewing interview data, building an impression of each informant's ○ view the responsibility of other parties like the service provider and public authorities for protecting own information against misuse (interview data) ○ view own responsibility for protecting own information against misuse (interview data) ○ view the main responsible for protecting own information against misuse (interview data) and the answers were separated by agree/disagree that the main responsibility lies with the user
ACTUAL EXPOSURE ON FACEBOOK	Protecting information on Facebook (overview)	this figure is an informal illustration of the findings in the three areas of Facebook use and is not based on accurate numbers from the analysis of exposure
EXPERIENCES OF PRIVACY ON FACEBOOK	Experiencing vulnerability on Facebook (overview)	estimated in analysis: by summing the values estimated for The basic experience of security, Views of self as a potential target, and Notion of information sensitivity for own, personal information.
	The basic experience of security	estimated in analysis: by reviewing complete transcriptions, a qualitative impression was built of each informant's ○ basic sense of security and these impressions were ranked on a three-point scale: a *basic sense of security*; *a moderate sense of security; and a basic sense of insecurity*
	Views of self as a potential target	estimated in analysis: by reviewing interview data, a qualitative impression was built of each informant's ○ view of self as a target for a potential perpetrator these impressions were represented on a three-point scale: *probably not interesting; possibly interesting; and probably interesting*
	Notion of information sensitivity for own, personal information	estimated in analysis: by reviewing complete transcriptions, a qualitative impression was built of each informant's ○ each participants' view of the importance of protecting their own, personal information and the answers were ranked on a three point scale: *High, Medium, Low*

Table 4: Detailed procedures for measuring knowledge in data analysis

5. DATA ANALYSIS

This chapter presents the findings uncovered in the analysis of empirical data. Analysis has been concentrated on the three main themes of privacy literacy reflected in **Figure 11**; KNOWLEDGE, BEHAVIOR, and the user EXPERIENCE, to see if the joined forces of this trio improve our understanding of the research questions (section 4.1). The chapter is organized according to these three themes.

As a start, section 5.1 introduces the informants and some characteristics of their Facebook use. Section 5.2 looks into the results from measurement of five elements of their privacy KNOWLEDGE; *Technology skills* (5.2.1), *Assigning responsibilities* for protecting information against misuse on Facebook (5.2.2), *Knowledge of risks* (5.2.3), *Notion of information sensitivity* of three categories of information (5.2.4), and finally, their *Understanding of exposure* of information on this social networking service (5.2.5). As a review of the findings in this section, each of these knowledge elements is evaluated as strong, improvable, or weak, respectively (5.2.6). In addition to text based descriptions and transcripts from the interviews, results are presented by use of simple quantifications in figures and tables. Quantifications are used for illustrative purposes only; the use of numbers and figures do not claim any statistical significance. Refer to paragraph 4.4.2.5 for descriptions of the detailed analysis procedures. Each transcript in this presentation is identified by a combination[50] of:
1) Transcript number 2) Age group (Youth/Adult); 3) Interview number[51], and 4) Gender: (Female/Male).

Section 5.3 reviews some decisions made by participants' in their actual use of the Facebook service; decisions that do have consequences for the exposure of their personal information on the Internet. These representations of actual BEHAVIOR, associated to *Facebook Core* (5.3.1), *Facebook Platform* (5.3.2), and *Facebook Security* (5.3.3), respectively, strengthen and supplement the impressions of informants' knowledge gathered in the analysis of KNOWLEDGE. A review is found in paragraph 5.3.4.

In a third perspective, section 5.4 elaborates the participants' EXPERIENCES of Facebook use by investigating the emotions and attitudes involved. This investigation deepens and reinforces the understanding of the informants' knowledge developed in the two preceding sections. A *basic sense of security* (5.4.1) and an *experience of invulnerability* (5.4.2) were found as pronounced aspects of the

[50] as an example, the identifier **(#1:Y6F)** translates to: Transcript 1; Youth group - Interview 6; Female informant
[51] a separate numbering sequence is used for each age group: 1..9 for adults and 1..10 for youths (one youth interview was rejected due to technical problems)

overall experience. Subsection 5.4.3 raises questions to the fragility of the general experience, and 5.4.4 sums up findings from this section.

Section 5.5 finalizes the analysis chapter by reviewing the findings from this study.

5.1 Informants

To reveal potential differences related to age, knowledge**,** behavior**,** and user experiences were investigated in two groups of informants. In tota1, 18 participants contributed[52]; 9 young people from 16 to 18 years of age, and 9 adults aged 46-59. Genders have proximate representation within both groups. All participants use the service actively, most teens as perpetually available online and adults typically as logging on and off the service several times a day. Except 2 young participants, all contributors view Facebook as their preferred and most used SNS.

Friends count	*Teens*	*Adults*
151-250	1	3
251-350	0	4
351-750	5	2
750 <	3	0

Table 5: Facebook friends counts

Table 5 reflects the size of the informants' networks of Facebook friends. On the average[53], young participants had approximately twice the number of Facebook friends as adults. Peak friend counts observed were 1200/500 and the lowest 232/150, for teens and adults respectively.

Member since	*Teens*	*Adults*
2007	4	5
2008	2	1
2009	3	1
2011/12	0	2

Table 6: Membership durations

All participants except two had Facebook membership duration of 2-5 years at the time of interviewing (**Table 6**). The remaining (both adults) had 9 months, and 7 weeks of membership, respectively. All informants maintain a *personal user profile*[54] on Facebook.

Communication	*Teens*	*Adults*
Wall	0	4
Wall and chat	0	4
Chat	9	1

Table 7: Preferred way of communicating

Except one adult using the service mainly as a tool for self-presentation for professional purposes, all participants use the service as most personal users do: to stay in touch with friends and family, and to participate in the mutual sharing of photos, links, status updates and comments in a variety of social contexts. Young participants prefer personal messages and chat[55] to communicate with other Facebook users; adults

[52] refer to subsection 4.4.1 for more information about the sampling process and informants
[53] average/median 656/540 for youths vs. 301/320 for adults
[54] as opposed to maintaining a *Facebook Page*
[55] the functions for exchanging personal messages asynchronously and online chat are merged to one, common function on Facebook

generally prefer to communicate by sharing on their Facebook wall, using personal messages as a supplementary method for communication (**Table 7**).

The sample of informants assumedly includes some participants more interested in the question of privacy in social media than the average Norwegian social media user. The young informants was recruited from a local high school with digital technologies as a particular area of commitment, and some potentially take more interest in technology related questions than the average teenager. Similarly, about one half of the adults, by virtue of their educational or occupational experience, assumedly take more interest in this study's topic than most people. The young participants were recruited from different branches of study, and with one exception adults have different occupational backgrounds.

5.2 Knowledge

This section presents findings related to the measurement of each of the five elements of KNOWLEDGE from the preliminary model of privacy literacy in **Figure 11**; *Technology skills* (5.2.1), *Assigning responsibilities* (5.2.2), *Knowledge of risks* (5.2.3), *Notion of information sensitivity* (5.2.4), and *Understanding exposure* (5.2.5). A brief review is presented in 5.2.6.

5.2.1 Technology skills

As measuring each informant's technology skills separately would be beyond the scope of this study, the evaluation of this knowledge element was based on the participants' self-reports. Participants were asked to rank their knowledge within three areas of Technology skills - *knowledge of PC and Internet use*, *knowledge of Facebook use***,** and *knowledge of Facebook privacy settings* - using a five-point Likert scale[56]. To give a general impression of self-reports, **Figure 12** reflects the pattern of all answers in all skill areas[57]. Informants generally ranked their Technology skills as *high to medium* and the youth rated their skills somewhat higher than adults. The following subsections describe each skill area in more detail and show an exception from the general pattern in one of the areas.

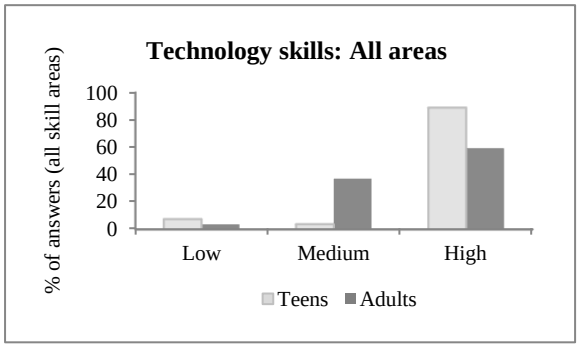


Figure 12: Technology skills: All areas

[56] the scale used is: *very good, pretty good, good, not so good,* and *poor*

[57] to create this model, as well as similar models in this chapter, answers were converted to a three-point scale. Refer in general to paragraph 4.4.2.5 for a description of the detailed analysis procedures

5.2.1.1 Knowledge of PC and Internet use

The young participants view themselves as competent users of PC and the Internet, and characterize their knowledge as *pretty good* or *very good* (**Figure 13**). Adults generally report high knowledge in this area too, yet a few ratings by the middle level value *good* are reported, as well. The high ratings in this area may reflect a participant group of experienced technology users. Most participants have a quite long Facebook membership duration (section 5.1) and describe themselves as experienced users. In the words of one of the young participants:

> *I would say that [my knowledge of PC and Internet use] is 'pretty good'... I have been using a PC for a great many years* (#2:Y6F)

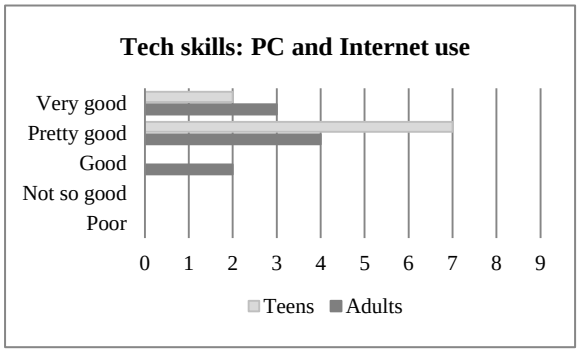


Figure 13: Technology skills: PC and Internet use

Three adult informants ranked their knowledge lower than the others for all areas of self-reported knowledge. Two of these have a short Facebook membership duration; 9 months and 7 weeks. The third adult seems to assess his knowledge by more strict criteria than others. This informant did not give an impression of lower knowledge than the others throughout the interview.

Many participants stress that rankings in this area express knowledge of functionality, rather than knowledge of a technical character. Two informants, one from each of the age groups, demonstrated technical knowledge throughout the interview.

5.2.1.2 Knowledge of Facebook use

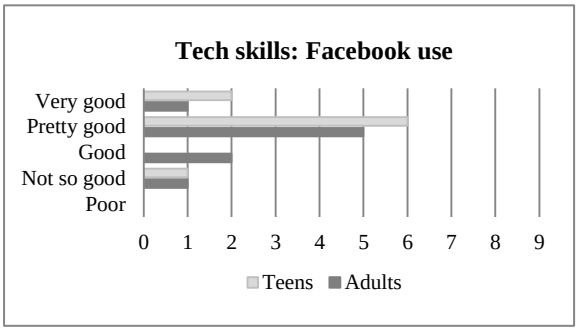


Figure 14: Technology skills: Facebook use

A similar rating is seen for the area *knowledge of Facebook use*. The young informants view themselves as competent users of Facebook, as adults do too, but with a slightly lower rating. Overall, 14 of 18 participants rank their knowledge in this area as *pretty good* or *very good* (**Figure 14**).

5.2.1.3 Knowledge of Facebook privacy settings

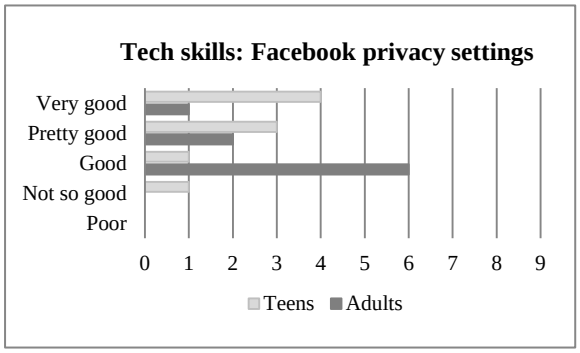


Figure 15: Technology skills: Facebook privacy settings

Some more pronounced age differences are visible in the area *knowledge of Facebook privacy settings.* Most young participants rank their knowledge as *very good* or *pretty good*, and express a familiarity with these settings in general (**Figure 15**). On the other hand, two thirds of the adults rank this knowledge by the middle level value *good*.

Informants in the youth group typically described Facebook privacy settings as straightforward:

> *I think [the settings] are very clear and straightforward, so I think I am in pretty good control of… how you [take care of] your privacy on Facebook* (#3:Y4M)

However, several participants reflected upon the high rate of changes the privacy settings, and the need to constantly update their knowledge that these changes bring about:

> *I have been [a Facebook] user for a couple of years… so I am quite familiar with settings and things. But Facebook updates [the functionality] continually, so… you have to start over from scratch at times* (#4:Y3F)

About one half of the adults find knowledge of Facebook privacy settings as not very important, as long as they restrict the information being shared on Facebook:

> *[privacy settings] might not be what I have been emphasizing the most… there is [no information] in there that I cannot answer for, and there are no pictures that… are crossing any lines. So… I have not spent too much time on [learning them]* (#5:A1F)

5.2.1.4 Technology skills – a review

Most participants describe their *Technology skills* as very *good* and *pretty good* within the areas *knowledge of PC and Internet use* and *knowledge of Facebook use*. Exceptions from this are made for a few informants with a short Facebook membership duration, as well as one (assumed) case of under-reporting. Age differences were observed in the area *knowledge of Facebook privacy settings* in particular, where 2/3 of the adults use the middle level value good, whereas 2/3 of the youth rated it as *very good* and *pretty good.* Values in the *not so good* and *poor* categories were rarely used in reporting of Technology skills.

5.2.2 Assigning responsibilities

Who has, in the informants' view, a responsibility for protecting their personal information against misuse once shared? And how do they view their own responsibility as compared to other parties like the service provider and public authorities for privacy and information security (legislation, the Norwegian Data Inspectorate, etc.)?

One young informant sums up her answer in a way typical for participants in both age groups:

> *Well, the main responsible is me, obviously… And next comes Facebook; they are obliged to provide… privacy settings that protect… the information we share against misuse… [Public authorities] have to be part of it, too, I think. We need better information on how to protect ourselves, at the same time as they should impose restrictions on what people may or may not do* (#6:Y3F)

Informants do, with a very few exceptions, agree that the main responsibility for protection of personal data against misuse lies with the user. Most of them view the service provider (Facebook) and the public authorities as sharing a joint responsibility. They all recognize themselves as the main responsible for protecting the information they share against misuse and no one expects other bodies to protect their personal data in place of themselves. In sum, the informants do recognize a central responsibility for protection of their own, personal data against misuse.

5.2.3 Knowledge of risks

The informants' knowledge of risks was evaluated based on self-reports, as well as on an additional tuning of the self-report scores by individual risk awareness profiles construed in data analysis. As reflected in **Figure 16,** *Knowledge of risks* for 2/3 of the informants was found *high.* Some differences between the age groups were observed, which are detailed in 5.2.3.1.

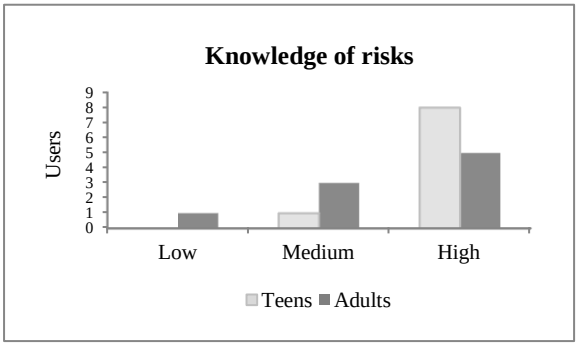


Figure 16: Knowledge of risks: overview

The individual risk awareness profiles were created from a collection of all statements of risk awareness expressed by each informant throughout the interviews. The profiles were used to supplement and adjust the self-reported knowledge scores (5.2.3.2). In addition, these profiles gave valuable information about what threats the informants know and recognize as important. The informants' views of threats are summarized in the paragraphs 5.2.3.3 to 5.2.3.5.

5.2.3.1 Knowledge of risks as reported by the informants

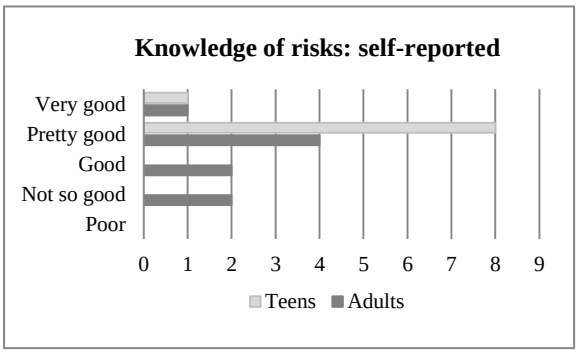


Figure 17: Knowledge of risks: self-reported

Participants were asked to rank their risk knowledge by the five-point scale. All young informants ranked this knowledge as *pretty good* and *very good* (**Figure 17**). The adult rankings were more distributed throughout the scale; one half of the adult group ranked their knowledge as *pretty good* or *very good*, and the other half rank as good or *not so good*. Three of the four adults in this latter half are the same informants that ranked their knowledge lower for self-reported knowledge in general, this means that two of the four lower rankings may be closely related to a low level of technology experience and a third is most probably due to an element of under-reporting.

5.2.3.2 Tuning knowledge scores by individual risk awareness profiles

To complement the image of risk knowledge collected by the informants' self-reports, additional analyses of the risk knowledge expressed throughout the interviews were carried out. The analyses resulted in individual risk awareness profiles for all informants. These profiles were used to adjust the self-reported risk knowledge scores, with the purpose of passing these scores through a simple validation process. The correspondence between the self-reports and the risk knowledge expressed in interviews were quite high, and adjusting self-report scores by individual profiles did not suggest any major changes. A one-step downgrade of the scores for two young participants, as well as a one-step downgrade and a two-step upgrade for two adult participants, resulted from this process. In sum, the suggested adjustments did not change the general impression from **Figure 16** of participants generally aware of risks (**Figure 18**). Still, some risks get less attention from the informants than others; the informants' views of threats are developed in the next paragraphs.

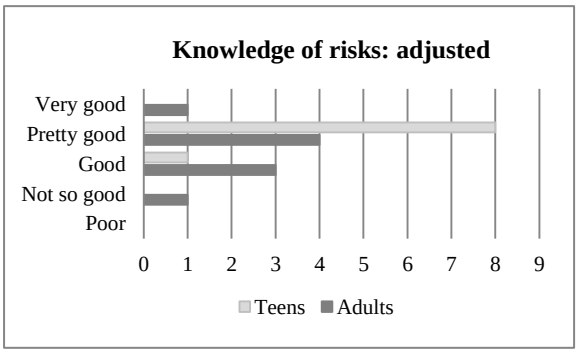


Figure 18: Knowledge of risks: adjusted by individual risk awareness profiles

5.2.3.3 Most focused threats

When assembling data for the individual risk awareness profiles, an overview of all privacy threats in focus during the interviews was recorded. A further analysis of this overview gave information indicating which threats are known to and recognized as important by informants. An overview of the

most focused threats is presented in **Table 8**, and the *least focused threats* in **Table 9**. High concurrence in foci was observed across age groups and the views are presented as common for both groups. Column 1 in the tables, the 'Focused by' column, reflects how many of the total of 18 participants that were focusing on the current threat in the interview.

ID thefts were identified as the top threat, mentioned by all informants, and commonly brought up several times throughout the interviews:

> *… it is really grave… like getting a mental roofing tile in your head… a 'Facerape' would be bad enough… Identity theft is truly a worst case scenario* (#7:A4F)

Commercial infringements and spam came secondly. The two age groups differed in perspectives in this area, and some aspects are further detailed in a separate paragraph (5.2.3.5).

Focused by	*Threat*	*Description*
18/18	ID thefts	Identity thefts[58]. Also included are integrity violations by someone assuming to be you on Facebook; like creating a fake Facebook profile, or the unauthorized use of a valid Facebook profile[59]
17/18	Commercial infringements and spam	Utilization of personal information for commercial purposes (advertising, resale), incl. mass distribution information (spam)
15/18	Fraud	Financial fraud. Misuse of bank account number or payment information. Also in focus: Nigerian Scam[60]
15/18	Data virality	Integrity violations by undesirable dispersion of personal information
14/18	Conceived vulnerabilities in Facebook Core or Platform	Undesirable exposure of personal information due to Facebook core functionality/complexity, or software by 3rd parties via Facebook Platform
13/18	Physical security (person)	Violations of person/body, i.e. stalking, abuse, assault
13/18	Hacking	Computer hacking, user account hacking
11/18	Physical security (property)	Violations of property, i.e. housebreaking, thefts
10/18	Data persistence	Integrity violations by undesirable storage of personal information
9/18	Malware (computer viruses)	Malicious computer programs with ability to replicate and spread to other computers

Table 8: Most focused threats

[58] refer to subsection 2.1.1 for definitions
[59] also referred to as 'Facerape'
[60] one of the most common types of confidence frauds for monetary gain, based on advance fee payment

Data virality and data persistence are general characteristics of digitized information rather than actual threats, but these phenomena were stressed as threats by many informants and by this reason included as separate categories of threats. These aspects are further explored in paragraph 5.2.5.1.

Conceived vulnerabilities in Facebook Core and Facebook Platform were focused in both age groups, but from different angles. Young participants tended to focus on complexity and volatility in the privacy settings in Facebook Core, whereas adults were more concerned about lack of control over personal information by undesirable sharing through third party applications in Facebook Platform.

Physical security was focused by both groups; adults as focusing mostly on protection of home and property, the young participants' focused primarily on their own, as well as their friends' physical security.

5.2.3.4 Least focused threats

It is interesting to look into the threats that were the least focused in the interviews, as well. **Table 9** reviews the threats focused by a maximum of 3/18 participants. A striking property of this table is how it incorporates threats of current importance. For example, the Norwegian National Security Authority characterize *social engineering*, *phishing*, and *malicious links* like Trojans as major threats currently and in the years to come (NSM, 2010), but the focus on these seems low among informants.

Focused by	*Threat*	*Description*
3/18	Malware (malicious links)	Malicious software hidden in web links, i.e. Trojans, spyware
3/18	Coupling	Undesirable (and possibly unauthorized) access to personal information by combining data from multiple sources
3/18	Subscription services	Undesirable registration on subscription-based services
3/18	Social engineering	Manipulation/elicitation by misuse of personal information
2/18	Cookie tracking	Tracking of a user's web interaction by downloading bits of text (cookies) to a web browser
2/18	Malware (session hi-jacking)	Exploitation of a valid computer session to gain access to a computer system
2/18	Malware (keylogger)	Unauthorized software logging of user keyboard strokes
2/18	Phishing	Digital snooping for personal information by passing oneself off as a trusted source

Table 9: Least focused threats

Another matter worth noticing is how threats typically named by key terms from the security area are found in this table of low-focus threats. Threats like *cookie tracking*, *keylogging* and *session hi-jacking* was mentioned solely by two informants with more technical interest and competence than the other participants. These threats were not mentioned by alternative terms either. These findings

demonstrate a low focus on particular threats among participants, and may indicate a lack of knowledge of these threats, as well.

5.2.3.5 Age differences in views on commercial infringements of personal information

Commercial infringements of personal information, was focused from different perspectives by adults and young participants (**Table 10**). The adults expressed high concerns for the service providers' undesirable utilization of their own data in advertising, and for the unauthorized resale of data to third parties, in particular. Young participants on the other hand, focused primarily on spam in the form of excessive advertising based on personal information. They generally found excessive advertising very annoying.

> Some would claim that people pay for their Facebook membership by their own personal information, as they have to provide this information to create a user account and to get access to services like third party applications. What do you think about this assertion?

Figure 19: Personal information as means of payment

All informants were asked to comment on the statement in **Figure 19.** Just a few young participants felt familiar with the idea of personal information as means of payment for services. Most adults found this assertion reasonable:

I find [the assertion] appropriate… It is uncomfortable, but very appropriate (#8:A4F)

Different views on commercial infringements	*Teens*	*Adults*
Commercial use of personal information: main concern	spam	misuse
Recognize the idea of personal information as means of payment for services	2/9	8/9

Table 10: Different views on commercial infringements

Except a few mentioning a potential income for Facebook from advertising, the young informants generally had few ideas of how Facebook is making money by providing a free service to hundreds of millions of users:

I have not thought about that… I don't know if Facebook earns any money from our sharing of information… I don't think they do that, actually (#9:Y6F)

5.2.3.6 Knowledge of risks – a review

The analysis of participants' *Knowledge of risks* reveals a quite high awareness of risks among informants in general, among youths a little higher than for adults. Validation of the self-reported knowledge scores by individual risk awareness profiles did not change the general impression of the knowledge scores from self-reports, yet provided useful information about the most and least focused threats. The overviews of threats revealed how some threats of current importance, like *social engineering*, *coupling,* and *phishing*, get a rather low focus within both groups of informants. And further, the young informants expressed low concerns for the potential misuse of personal information for *commercial purposes*, and generally keep a high focus on protecting their own as well as others'

physical security. As to *conceived vulnerabilities in Facebook Core or Platform*, young people generally focused on Facebook Core, and adults expressed higher concerns for the potentially undesirable disclosure of information through Facebook Platform.

5.2.4 Notion of information sensitivity

Are some categories of personal information viewed as more or less vulnerable for misuse as others? To get an impression of their notion of sensitivity of different kinds of personal information, three information categories of were introduced to the informants; self-identifying, access-enabling, and expressive information. Each category was introduced by a brief description, and concretized by examples of information elements of this category that is typically shared on Facebook. From this starting point, informants were asked to what extent they want to limit others' access to the information category in question. In general, *self-identifying* and *access-enabling information* were viewed as of high to medium sensitivity, whereas *expressive information* was valued distinctly lower. The informants' views of sensitivity for the three information categories are detailed in the following.

5.2.4.1 Views on self-identifying information

Self-identifying information (SI) reveals elements of your identity and tell others who you are. This category was exemplified by name, date-of-birth, education, profession, family relations, health, and private economy. The young informants view this information having *high* sensitivity, whereas the adults view it as of medium to high sensitivity (**Figure 20**). Informants in both age groups emphasized security risks as their main consideration related to sharing of SI (**Table 11**), and identity thefts was the most often mentioned risk.

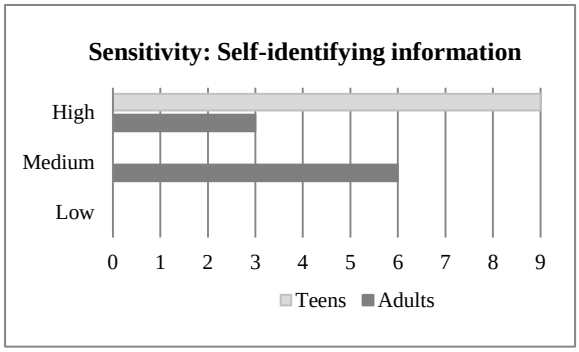


Figure 20: Notion of information sensitivity: Self-identifying information

Name and date-of-birth are mandatory information when registering for a user account on Facebook. All participants have registered for a Facebook account using their real name. Some of the young informants emphasized how they intentionally left their middle name out, in order to make it more difficult for others to use their name in searches for further information on the Internet. Facebook provides the option of hiding year of birth from the user profile, and several informants utilize this

functionality. Showing the complete date-of-birth are considered as sensitive by some, as this makes up the first six digits of the 11-digit social security number[61] used in Norway:

> *… year of birth is … one factor in the social security number… By removing this, you are cutting back on available information… [The SSN] is… key to a lot of services… like… internet banking for instance* (#10:A8M)

Information sensitivity: main consideration	*Teens*	*Adults*
Self-identifying information	security	security
Access-enabling information	security	security
Expressive information	identity	identity

Table 11: Notion of information sensitivity: main consideration

Health and economy are information elements that most (16/18) participants wants to restrict others' access to; due to risks of misuse for some or due to the personal character of this information for others. Sharing information about education and occupation was generally seen as unproblematic.

5.2.4.2 Views on access-enabling information

Access-enabling information (AI) provides access to people in various ways, in the real world, or on the Internet. This category was exemplified by telephone number, address, current location, and information about a future location and when you plan to stay there.

As reflected in **Figure 21,** all informants rate AI as of *high to medium* sensitivity. The young participants, though, did express an even higher focus on protecting information of this kind throughout the interviews. A similar focus on protecting information from this category was not observed among the participants in the group of adults.

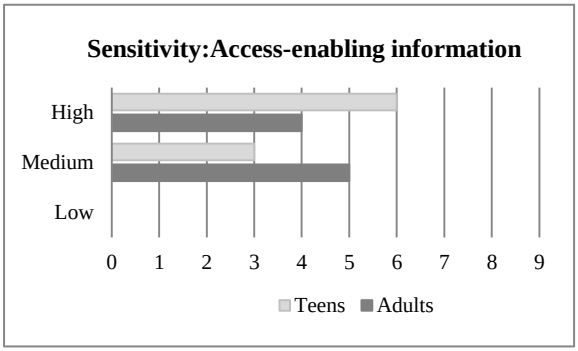


Figure 21: Notion of information sensitivity: Access-enabling information

The young participants keep a high focus on limiting access to address or location information in order to protect their physical security; their own, or their friends' security. They say they are likely to share information about their location, but not as specific as the exact address or exact time of day. One informant describes how she finds it safer to geotag public places rather than tagging exact, private addresses:

[61] in Norwegian: *Personnummer*

Exact address… I would not share that with everybody. If I do, it would be easy to seek me up… if I go to town with a friend, or to the movies…okey, but… I rarely share the exact address that I am staying at… (#11:Y10F)

Others describe how they share location information by using fake location names instead of exact geotagging, and in this way disguising the message for others than its intended recipients. Young participants keep a high focus on protecting their mobile phone number and email address, as well, yet the motivation for protecting these information elements seems to be to avoid annoying spam, rather than to protect their security.

Four adult participants find it important to limit others' access to their address, mobile phone number, and email address. Five adults find it not so important to restrict access to this information, as this information would be possible to retrieve from other websites, for instance like the yellow pages. Location information is higher valued among the adults, the focus on restricting access to this information is mostly due to a purpose of protecting physical property:

… my location, I rarely share that, and my future location…never… if we write that we go on vacation, our house is left empty, you know (#12:A3M)

5.2.4.3 Views on expressive information

Expressive information (EI) is information about who you are, your likes and preferences. This category was exemplified by your likes and dislikes, how you spend your time, political viewpoints, as well as religious beliefs. All participants share information of this category with other Facebook users, as well as with third-parties.

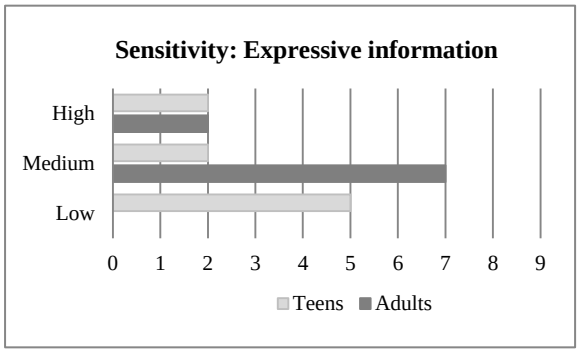


Figure 22: Notion of information sensitivity: Expressive information

As shown in **Figure 22**, EI was rated lower than SI and AI by participants in general, and youths rated this information type lower than adults. Youths view this primarily as *low to medium,* whereas most adults rated it as *medium*.

As to security issues particularly, the overall expression of sensitivity throughout the interviews was even lower than these numbers reflect, though. The previously mentioned focus on security issues seemed to fade when the informants were talking about expressive information. One of the adults answers similar to many participants when asked about what use he thinks others could do of his Facebook information if they had access to it:

... they probably would find out... that I ... like [interest]... and that I do have some opinions about [topic], - they are welcome to use that! ...@@@[62]*... if they want to. ... I don't really know [how this information could be misused]* (#13:A3M)

However, the participants' focus on identity and personal integrity was pronounced for EI as compared to SI and AI, especially among adults. Adults expressed a high focus on carefully selecting information for sharing with the purpose of presenting themselves in a way they find appropriate.

5.2.4.4 Notion of information sensitivity: a review

The three categories of information are viewed differently by the participants with regard to sensitivity. *Self-identifying* and *access-enabling information* were given *high to medium* sensitivity. *Security risks* are in focus when assigning importance to these categories. Young informants generally assess SI and AI a little higher than adults. *Expressive information* was assigned *low to medium* sensitivity, and adults generally assign EI a higher sensitivity than youths. Access restrictions to expressive information are most likely based on integrity considerations and the purpose of shaping one's own digital *identity*.

5.2.5 Understanding exposure

In order to understand the audience for the information we share about ourselves on the Internet, we need *a general understanding* of how information transforms in character when going from the physical to the digital world. And, in order to understand the audience for the information we share on Facebook in particular, it is vital to understand the exposure mechanisms on this service as well: exposure to other users via *Facebook Core*, and to third parties via *Facebook Platform*. To protect our privacy, we need to understand the rich selection of settings that Facebook offers its users, and how this service's sharing mechanisms work for a given combination of settings in different privacy contexts. The impression of knowledge in each of these three areas is detailed in the following paragraphs. Some variations were observed between areas, as well as between age groups.

5.2.5.1 Increased exposure - a basic condition when digitizing information

Data virality and data persistence are typical characteristics of digital information. Attention was drawn to these characteristics in the interviews to find how well known these are among the informants and whether they are taken into account in sharing decisions on Facebook. A *high* level of knowledge was uncovered for adults and a *high to medium* level for the young informants.

[62] in data transcriptions, the @ symbols translates to small (@), moderat (@@) and loud (@@@) laughter respectively

Adults generally express a familiarity with the two phenomena, and also report to take them into consideration when sharing their personal information (**Figure 23**). Data persistence gets a particular focus in this group. Young participants give a more ambiguous impression as to understanding these general concepts of exposure. Some do not have sufficient understanding of the concepts, and some say they do not consider them in their sharing-decisions (when understood). About one half of the young informants say they understand *and* consider these concepts when sharing information about them:

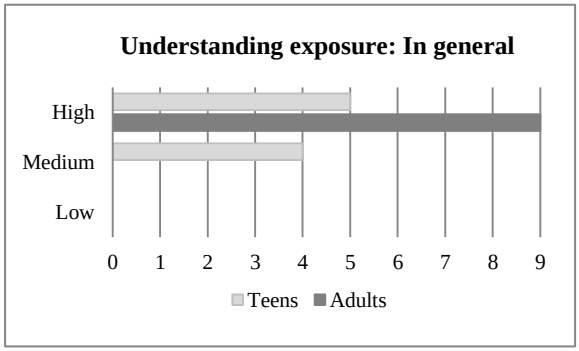


Figure 23: Understanding exposure in general

> *... I do think a lot about it, if it is possible to completely remove [the information], or if people can change, delete or copy it… in the future… when I apply for a job, it would be no fun if [the employer] could simply 'Google' my name and discover… a lot…* (#14,Y6F)

Data virality, especially the wide and rapid spread of photos, was given a particular focus in the group of young participants.

5.2.5.2 Understanding exposure in Facebook Core

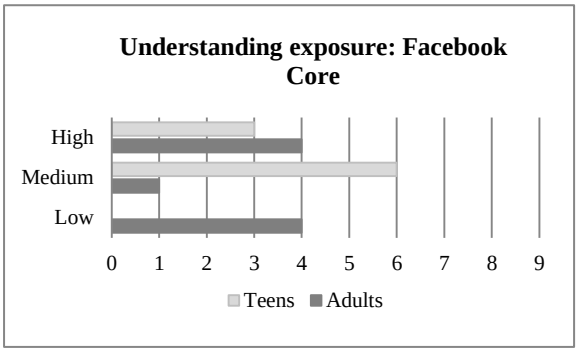


Figure 24: Understanding exposure in Facebook Core

Marketed by the slogan "the more you share, the more social it gets", it is not surprising that Facebook's default privacy settings are configured for a high level of exposure. Users who do not change their settings from default values display their personal information to a wide audience, sometimes unwittingly. Using Facebook's standard settings leave information accessible by the general public of Facebook users[63].

Understanding exposure in *Facebook Core* appeared with *medium to high* knowledge for the youth and more dispersed throughout the scale for adults (**Figure 24**). The adult group was split between *high and low* knowledge for this area.

[63] 'public' exposure is default for most settings, yet restricted to 'friends-of-friends' for account holders below the age of 18

When introduced to the example of a typical Facebook user[64] sharing with default privacy settings, most young participants immediately recognize the high level of exposure and potential risks involved. Y3K points to some risk factors:

> *… if she didn't limit the availability of her profile… they have access to all they need… if… she checks into a location…she has a photo of herself… they can easily find out who she is… they know how old she is… telephone number… just fragments of the information she is sharing may put her at risk* (#15:Y3K)

Among adults, the number recognizing this issue was lower; one half of the adults recognized this as a potential problem. The remaining adults were not familiar with the default settings, or the level of exposure these settings are configured for.

Facebook offer users a rich set of privacy and security settings. Many informants find these challenging to get acquainted to. The large count of settings, spread out on a number of webpages, complicates the choice of a suitable combination of options. Issues were also raised as to validating how particular options will work out practice. Yet another challenge stems from the frequent changes made to the settings (mentioned also in 5.2.1.3). Information about changes and recommendations on preventive actions are typically received through Facebook friends. Lacking one, central source of advice, the information and tips available is quite random. Advices circulating on Facebook might be hoaxes just as well as useful recommendations:

> *… there is an abundance of fictitious recommendations, but… if I receive a serious warning… I am likely to go in [to my privacy settings] and check; … did I tick that [box]?* (#16:A4K)

Despite the rapid change in the privacy settings, one half of the informants have changed their privacy settings only once since they first registered for a Facebook account.

The transitoriness in privacy settings due to alternation between different privacy contexts (chapter 2) is a further complicating factor. As much as 2/3 of the informants were not aware of their own privacy settings being superseded when sharing information on another user's Facebook wall.

The next paragraphs take a look at issues related to information exposure in a third privacy context: the use of applications in Facebook Platform.

---

[64] presented as a user sharing information regularly, has name, date-of-birth, some information about interests, and sometimes location information present on her profile

5.2.5.3 Understanding exposure in Facebook Platform

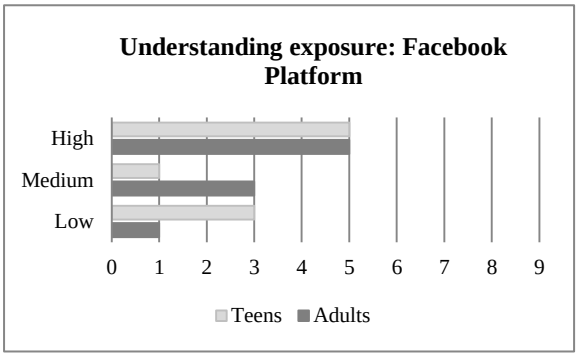


Figure 25: Understanding exposure in Facebook Platform

Users may have problems recognizing the transferal of control between Facebook and the different third-party service providers offering services through Facebook Platform, and also to recognize the situations where they grant third parties access to their own, personal information.

As exposure of personal information amplifies through the use of third-party applications (chapter 2), it is interesting to find out if the informants understand the transferal of control and how third-party activity increase potential risks for their privacy.

The analysis of informants' understanding of exposure in Facebook Platform revealed a rather ambiguous impression: One half of the informants in both groups demonstrated *high* knowledge in this area, the other half spread between *medium* and *low* **(Figure 25)**. No significant differences related to age groups were uncovered.

5.2.5.4 Understanding exposure: a review

In this first round of analysis, the overall impression of participants' *Understanding exposure* was rather ambiguous. The results spread on all three levels of knowledge.

The strongest level of knowledge was found in *exposure as a general phenomenon.* This area is well understood among adults, and less, but still quite good, by the young participants. A *medium to high* knowledge was found for youths in understanding *exposure in Facebook Core***,** yet the impression for adults was more ambiguous. Participants in both age groups say they find this area complicated. The impression of understanding *exposure in Facebook Platform* appeared as ambiguous for both age groups. This area seemed well understood by 2/3 of the informants. Among that last 1/3, issues of increased exposure and potential risks in use of third-party applications seemed less familiar.

In sum, the understanding of *exposure in general* appeared as weaker among youth than adults; *exposure in Facebook Core* was indicated as a potential problem area, for adults in particular; and *exposure in Facebook Platform* was indicated as a potential problem area for both age groups.

5.2.6 Knowledge – a summary

Five elements of the preliminary model of privacy literacy were investigated in this first round of analysis focusing on KNOWLEDGE measurements. Two knowledge elements were found as *strong* in both groups: *Technology skills* (self-reported) and *Assigning responsibilities*. Three elements, *Knowledge of risks, Notion of information sensitivity,* and *Understanding of exposure,* appeared as *improvable*.

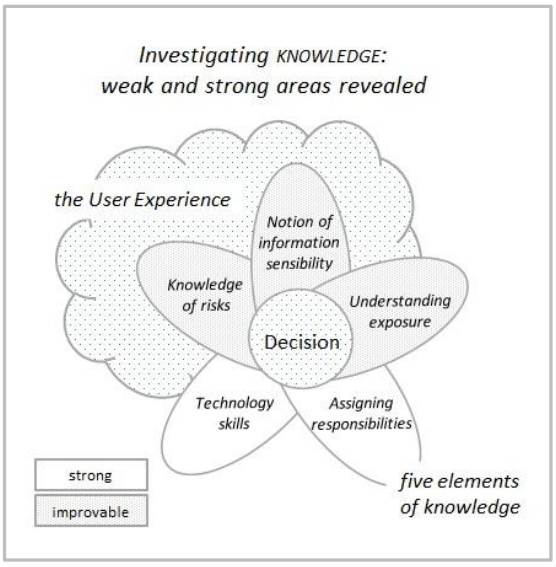


Figure 26: Privacy literacy: Weak and strong areas uncovered in analysis of knowledge

For *Knowledge of risks*, the informants' level of risk awareness seemed satisfying, whereas the analysis of the most and least focused risks uncovered a low focus on some risks of current importance, like *social engineering*, *coupling*, and *phishing*.

Investigating *Notion of information sensitivity* revealed a room for improvement for all three categories of information, yet *expressive information* was particularly poor valued, especially as to the risk of security breaches.

The analysis of *Understanding exposure* left an ambiguous impression. This area seemed quite familiar to one half of the informants; yet other participants seemed to have a weaker understanding of exposure. The youth showed a weaker understanding of *exposure in general* than the adults; *Facebook Core* appeared as a potential problem area for adults in particular; and *Facebook Platform* as a potential problem area for both age groups.

In sum, the analysis of KNOWLEDGE uncovered three knowledge elements as potential problem areas for the informants' privacy: Knowledge of risks, Notion of information sensitivity, and Understanding exposure (**Figure 26**). To develop a richer understanding of these potential problem areas, they were further investigated from the perspectives of BEHAVIOR (section 5.3) and the user EXPERIENCE (section 5.4).

5.3 Behavior: Information exposure in actual Facebook use

This section presents findings from the investigation of some of the decisions informants have made in use of their own Facebook account, focusing on the level of exposure of personal information that these choices bring about. Three areas of information control were investigated: 1) mechanisms for information control between users in Facebook Core (friends and non-friends); 2) mechanisms for information control between users and third-parties in Facebook Platform; and 3) Facebook mechanisms to control information security.

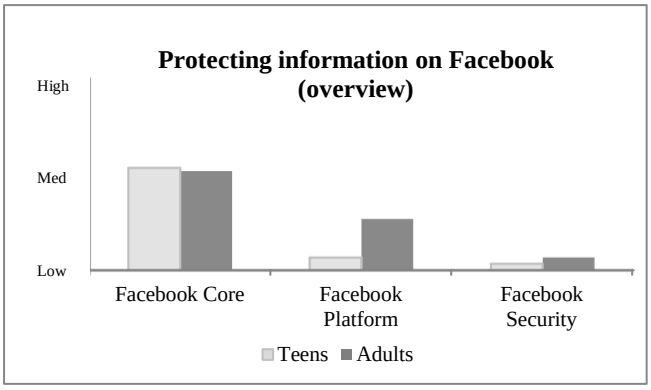


Figure 27: Protecting information on Facebook (overview)

The risks involved in information exposure depend on the character and volume of the information exposed. Information content is not subject to investigation in this study and no conclusions related to actual level of risks will be drawn. The analysis concentrates on informants' explicit actions to protect personal information, as well as on their authorization of others' access to this information. These measures are assumed as relevant indicators of actual exposure.

Figure 27 provides an informal[65] illustration of informants' use of protection mechanisms to control information exposure on Facebook. A *medium* level of protection was found for mechanisms in *Facebook Core* and a *low* level of protection was uncovered for the mechanisms in *Facebook Platform* and for use of *Facebook security functions.* The findings uncovered for Facebook Platform led to a reconsideration of one of the knowledge elements investigated in the previous section and also revealed significant age differences in exposure of information. These findings are further detailed in the following.

5.3.1 Exposure to other users in Facebook Core

A wide variety of settings to control information exposure is provided in Facebook Core. Two categories of settings were analyzed: settings for *Facebook wall* (sharing by the user as well as by friends) and settings for the *user profile data*. A third area was looked into as well; the user's policy for accepting friend requests, which tells us who gets access to the information once shared.

[65] this figure is merely illustrative and not based on accurate numbers from analysis. Accurate numbers for each subarea are presented in figures in subsections 5.3.1, 5.3.2, and 5.3.3, respectively

A *medium* level of exposure was found for *Facebook Core*. **Figure 28** show the results for individual settings investigated. Having a look at the numbers, most young participants and a half of the adults have restricted[66] access to their own wall posts. Of those sharing with a wider audience, three share with 'friends-of-friends' and three share with 'public'. The latter three are all adults, and two of them chose this setting unknowingly, as they misunderstood the functioning of the privacy settings. This was done by accident rather than by choice, and was not a reflection of the users' deliberate publishing of own information to a wide audience.

> *... if you get into the driver's seat and publish[67], you are in control… what is left then, is the problem of others writing… about you, or tag you in these… may I call it… undesirable photos* (#17:A8M)

This informant expresses an issue related to restricting the information other people share about him on Facebook. From the numbers in **Figure 28**, informants generally keep a higher focus on restricting their own wall posts, rather than on this latter issue. About 1/3 have restricted access to others' posts on their own wall and 2/3 have restricted access to tagged[68] posts.

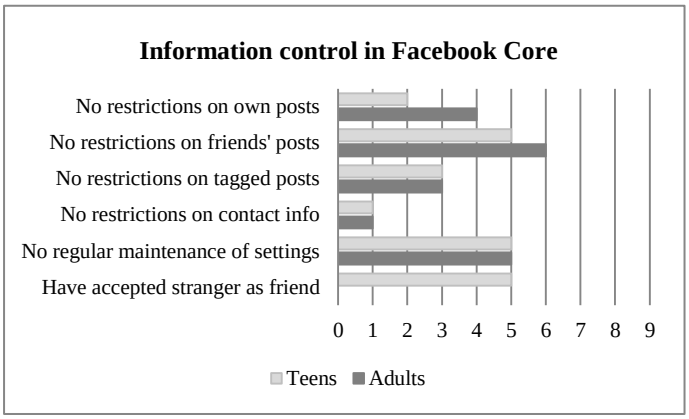


Figure 28: Actual exposure: Information control in Facebook Core

A brief walkthrough of the *contact information* registered on the informants' user profiles was made. Disclosure of access-enabling information was found relatively *low*. Most participants had restricted all elements that were reviewed[69]. Two young participants had registered their parents' credit card as payment information. Payment information have no privacy settings (this element is hidden for other users by default), but may be subject to security breaches, though.

On Facebook, your privacy is only as secure as your weakest friend. A considerate *policy for accepting friend requests* can help protecting data against security threats related to other users' actions and also in keeping unauthorized others away from personal information. One half of the young

[66] in this presentation, 'restricted' and 'restrictions' refer to limiting information access to Facebook friends or less
[67] here thought of as actively controlling the content as well as the audience of the information you share about yourself
[68] tagging refers to inserting a link to a person's Facebook profile into a piece of text, or on a photo
[69] these privacy settings for contact information on the user profiles were checked: email address, IM screen name (ID on other social media), address, phone numbers, website, and payment information (credit card)

participants say they have accepted a friend request from a stranger. This is done occasionally only; befriending strangers are rare. When receiving a friend request from somebody they do not know, most youth say they try to find out who this is (ask the sender in a personal message, ask friends, or investigate connections by looking for friends in common with the sender). Most adults say they just ignore friend requests from users they do not recognize and none has accepted a stranger as a friend. And also, *the total count of Facebook friends* has consequences for exposure. As seen in the beginning of this chapter (**Table 5**), youths generally have twice the count of Facebook friends as adults, and consequently have a higher level of exposure within the network of Facebook friends.

Summing up, the analysis revealed a medium exposure for the informants in *Facebook Core***.** A small, but potentially significant age difference in understanding the exposure mechanisms was observed, as two adults share their wall posts with the public without recognizing doing this. The young participants is slightly more restrictive than adults as to access to information for people *outside their network* of friends, yet have a higher degree of exposure than adults *inside this network*.

5.3.2 Exposure to third-parties in Facebook Platform

Personal information from user profile and wall posts is subject to exposure through the use of applications in *Facebook Platform***.** Exposure to third-parties originates from the users' own use of applications and also from their Facebook friends' use of applications.

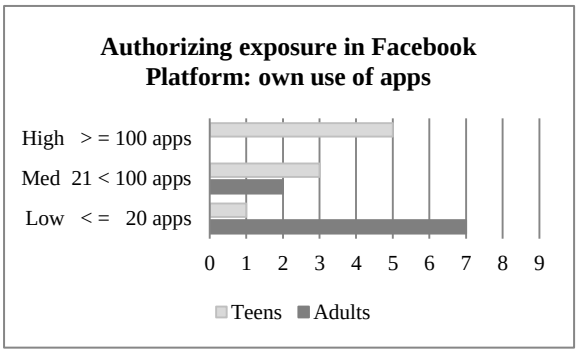


Figure 29: Actual exposure: authorizing exposure in Facebook Platform (own use of apps)

Each informant's *sharing through their own application activity* was reviewed by walking through the list of applications currently authorized to access information on their personal account. (**Figure 29**) sums up three levels of exposure, based on the count of authorized applications per participant. The young informants had a significantly higher[70] count of authorized applications compared to adults. Young informants had *high to medium* exposure, whereas the adults were found primarily in the low exposure category. Peak application count observed were 197 (youth), and the participant with the lowest count had authorized only one third-party application (adult).

None of the informants had chosen to *deactivate platform applications* in general, a selection in the privacy settings that blocks all sharing of information with third-parties from taking place.

[70] average/median 112/121 for youths vs. 22/16 for adults

Sharing through friends' application activity are controlled by editing the list of information elements available for sharing in the privacy settings for Facebook Platform. 17 elements of personal information are included in this list, and the elements can be enabled or disabled separate from each other. Most (15 of 17) information elements are enabled for sharing by Facebook default. To explore their sharing of information through friends' application activity, this list was reviewed for each informant. This walkthrough revealed a *high* degree of exposure through friends for all participants except one (**Figure 30**). This adult, particularly experienced with Internet and social media and using a considerate information protection strategy, had limited the list to two information elements; one young informant had extended the list by one element; whereas 16 of 18 participants used Facebook's default setting of 15 elements for sharing of information through their friends' third-party application activity.

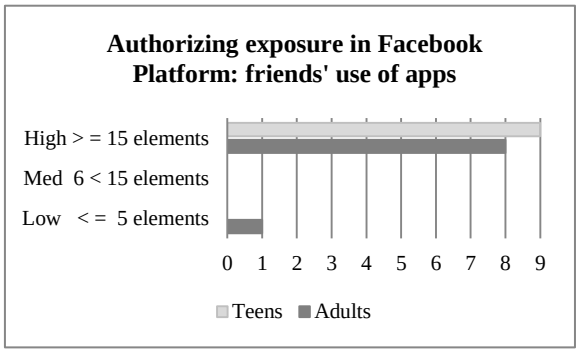


Figure 30: Actual exposure: authorizing exposure in Facebook Platform (friends' use of apps)

In this review of actual exposure to third-parties in *Facebook Platform*, many participants earned new knowledge about exposure. In the light of these observations, a new examination of the knowledge element *Understanding exposure* seemed relevant. The next paragraph pays a revisit to the informants understanding of exposure in Facebook Platform.

5.3.2.1 Understanding exposure in Facebook Platform - revisited

Informants' actual exposure of information in Facebook Platform was *high*; higher than most participants assumed ahead of the review. The review uncovered a distinct lack of knowledge. *More than one half* of the participants discovered unanticipated aspects of exposure related to *their own use* of applications, and *more than 2/3* was caught by surprise by the high level of exposure originating from *their friends' application activity*.

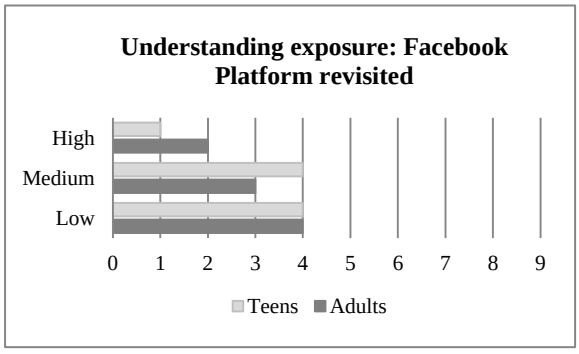


Figure 31: Understanding exposure in Facebook Platform - revisited

Adjusting the image of *Understanding exposure in Facebook Platform* from the first round of analysis **(Figure 25)** according to this lack of knowledge changed the impression remarkably (**Figure 31**). The image now shows a *low to medium* level of knowledge for a majority of informants.

Most informants were unaware of central aspects of their exposure of information in Facebook Platform. Some were surprised by the fact that they were using third-party applications at all and others were surprised by the total count of applications authorized for their account. Some were surprised to find that information is exposed through friends' use of applications in the first place and others were surprised by discovering the volume and content of this exposure as such. How this situation be explained? Responses pointed to several explanations:

First, the authorization process for third-party applications can be difficult to understand. Some find it difficult to accept authorization requests as the consequences of accepting are poorly explained. Some understand the authorization process as a standard procedure; read one, and you have read them all. Still others think that the privacy settings for Facebook Core are overriding the authorizations for third-parties. Mistakes like these can lead users to authorize applications unwittingly or to authorize applications without understanding the consequences of doing this. When introduced to an authorization page asking for extensive rights to access information one of the adults describes a feeling of uncertainty evoked by this request:

> *...I do not accept requests like this… because I do not know what it is. I may have done that…unwittingly at times… [the thought of accepting this]makes me feel unsure, so I do not do that* (#18:A6M)

This informant expresses how the feeling of uncertainty makes him reject the request. This is not the case for all participants. Uncertainty related to the authorization process was commonly described, but accepting or rejecting the application when facing this uncertainty seemed to vary. An 'accept and forget'-strategy to handle the uncertainty was mentioned by several informants.

Secondly, the acceptance of an application can be based the faulty assumption that Facebook is offering it or vouching for it:

> *… I think many people trust this… as long as [the application] is under the Facebook logo… they accept…The first really mean app has… not yet arrived… but might as well come… and let millions of users install Trojans…* (#19:A8M)

This dislocation of trust from Facebook to third-party service providers may stem from the standard Facebook layout often used in the authorization process interface. This potentially makes the transition from one service provider to another less noticeable for users. In the transcript above, the informant also focuses on how the extensive acceptance of third-party applications among users in general potentially opens the door for malicious software. In the latter case, Facebook's intention of 'utilizing community' in their vision of the Social Graph would re-emerge with the signs reversed.

A *third* aspect relates to the need to recall authorizations for applications no longer in use. Many informants seem to miss out on the fact that authorizations granted to third-parties yield until they are explicitly recalled. In the application list, a mark is shown on those not in use in the last six months:

> *@@ I didn't have a clue that I had [authorized] this many @@ … it is more than six months ago…yes… @ … most of them, actually* (#20:Y5K)

Among youths particularly, significant differences were observed between the count of applications authorized and the count of applications in current use. The most pronounced discrepancy observed was 197 applications authorized vs. 2 applications in use in the last six months.

A *fourth* and last aspect relates to the informants' familiarity with Facebook's privacy settings for Facebook Platform. Few gave the impression of visiting the administration page for third-party applications on a regular basis. In addition, most participants were unfamiliar with the dedicated page for controlling the information exposure through friends' third-party activity.

5.3.3 Protecting information by Facebook's security functions

Use of *Facebook security functions* was reviewed in the analysis, as well. The results show that most participants *do not use* these options to protect the information on their Facebook account. The use of three different settings was examined: 1) Browsing Facebook on a secure connection (HTTPS), 2) Using email/SMS notifications when an unknown browser is used for logging into the account (login notifications), and 3) Using a security code when an unknown browser is used for logging into the account (two-step login verifications).

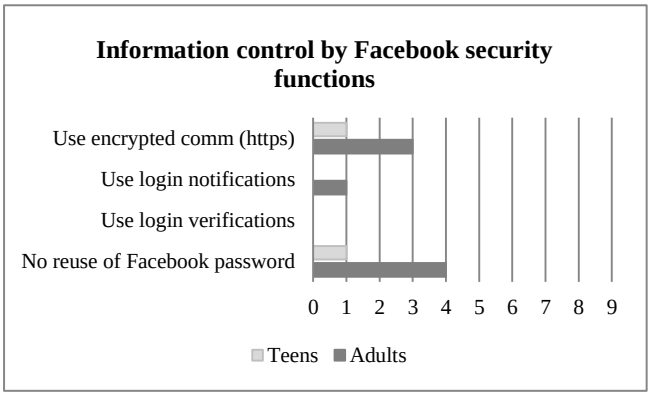


Figure 32: Actual exposure: Information control by Facebook security functions

Figure 32 shows that four informants used a secure connection and one participant had login notifications activated. Otherwise, the security functions were not in use.

Informants were further asked if they use one password for logging into Facebook exclusively. More than 2/3 of the participants reuse their Facebook password on other services on the Internet.

5.3.4 Behavior – a summary

The analysis revealed *medium* exposure for informants in *Facebook Core***.** Adults are slightly more visible outside their network of Facebook friends, whereas young participants expose themselves to a larger audience within this network. A small, but potentially significant age difference in disfavor of the adults was identified related to the exposure of own wall posts.

Exposure to third parties seems as a particularly complicated area. The review of settings for informants' *own use of applications* in Facebook Platform uncovered a *high to medium* volume of applications authorized for young informants and a *low to medium* volume for adults. Except one adult, exposure in sharing through *friends' application activity* was *high* for both groups.

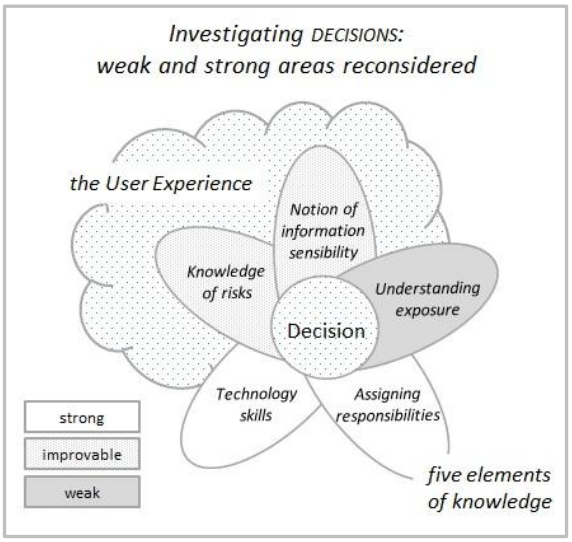


Figure 33: Privacy literacy: Weak and strong areas reconsidered by behavior

Most participants gained new knowledge in the walkthrough of their privacy settings for third-party applications. Uncertainties associated with the authorization process as well as a dislocation of trust from Facebook to third-party service providers, may lead to unintentional granting of access rights to third-party applications. Another aspect relates to the low focus on recalling authorizations for applications no longer in use.

Many informants were unfamiliar with the privacy settings for Facebook Platform. This indicates that the self-reports for *Facebook privacy settings* (section 5.2) was too optimistic, at least with regard to the settings for Facebook Platform. The measurement of KNOWLEDGE related to Understanding exposure (section 5.2) indicated *Facebook Platform* as a potential problem area. In the cross-checking to actual behavior described in this section, this finding was strengthened and confirmed. The revisit uncovered insufficient (*low* or *medium*) knowledge by 15/18 informants, as compared to 8/18 in the first round of analysis. Based on this, the assessment of the knowledge element *Understanding exposure* in the model showing weak and strong areas of privacy literacy is changed from *improvable* to *weak*. The change is shown in **Figure 33**.

A review of the use of *Facebook security functions* showed that most participants *do not use* these options offered by Facebook to protect the information on their Facebook account. More than 2/3 on the informants reuse their Facebook password on other web services.

5.4 Experiences of privacy on Facebook

This part of the presentation focuses on the informants' overall EXPERIENCE of privacy, by looking into the 'constant stream of self-talk that happens when they interact with' Facebook ('experience', Forlizzi & Battarbee, 2004, p 263).

Two features potentially important for the informants' privacy were uncovered in analysis; a *basic sense of security* and an *experience of* low *vulnerability*. **Figure 34** presents an image of the general privacy experience by combining the impressions of these two features, picturing users perceiving themselves as rarely or occasionally exposed to risks on Facebook.

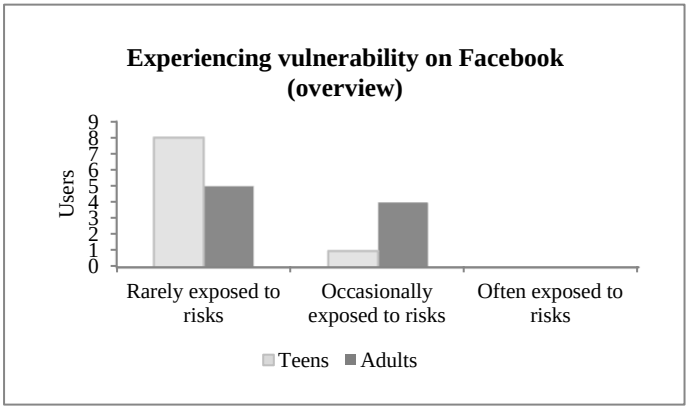


Figure 34: Experiencing vulnerability on Facebook (overview)

The two features of the privacy experience are described in the following: subsection 5.4.1 describes the basic sense of security and control, and subsection 5.4.2 details some aspects of vulnerability, the participants' notion of low sensitivity for own, personal information in particular.

Subsection 5.4.3 questions the fragility of the general privacy experience, as the concrete experiences ('an experience', Forlizzi & Battarbee, 2004) many participants had when participation in this study might come to 'inspire behavioral and emotional change' in a longer run (2004, p. 263). Subsection 5.4.4 reviews the findings related to experience.

This analysis suggests the introduction of one additional knowledge element in the privacy literacy model developed in the previous sections: *Managing vulnerability*. It also led to a reconsideration of the analysis of the knowledge element *Notion of information sensitivity* presented in section 5.2.

5.4.1 A basic sense of security

A *basic sense of security* and a feeling of being in control of their own privacy were running as a recurring theme in the interviews for both age groups. The sense of security was stronger among the youths than in the group of adults (**Figure 35**). And the high-quality exercise of one (or few) preferred information protection strategy(-ies) appeared as an essential basis for this security experience.

The most important information protection strategy applied is the careful selection of information for sharing: 16 participants emphasize such *self-censorship* as a main strategy (**Figure 36).**

A feeling of control was commonly associated to the practice of self-censorship:

> *... this is certainly something I know about my own publishing, or presence as a person on the Internet,... I am [in control of] the staging now... what I give access to, I know this is of a non-sensitive character... This is indeed... fundamental to my understanding: what I... put out there... are things that I do not have any problems to share* (#21:A8M)

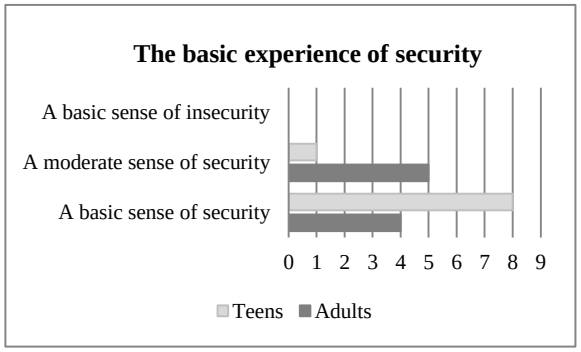


Figure 35: The basic experience of security and control

A two-fold purpose for self-censorship was found among informants: personal presentation on one hand and protecting information against misuse on the other. Adults' self-censorship had a general turn against self-presentation and the shaping of an online identity. Self-censorship was commonly characterized by terms like 'staging' and 'playing a role':

> *... I have this role to play... I am a public person on Facebook... on Facebook, I am <her workplace position>... and at all times, I am answerable for everything in there* (#22:A1F)

Many adults talked about self-censorship as the shaping of information for public presentation; some having public presentation as an aim in itself, others focusing on preventing potential embarrassment in case their Facebook information of some reason become publicly available in the future This focus was different among youths, more commonly focusing on protection strategies to restrict information access to their network of Facebook friends only.

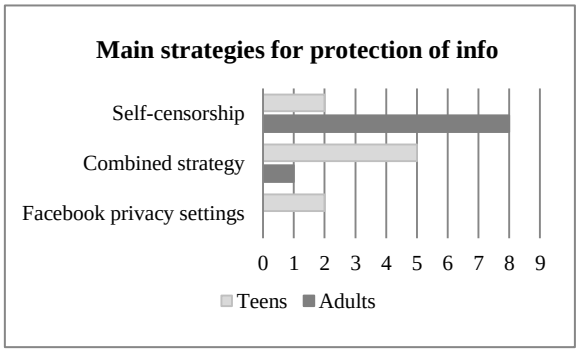


Figure 36: Main strategies for protection of information

The pronounced focus on identity and personal integrity among adults was replaced by a similar focus on security issues among the youths. Young informants expressed a strong focus on protecting personal data against misuse; to avoid threats to their personal, physical security (stalking, abuse) and identity thefts, in particular. Computer security (hacking, password security) and fraud were emphasized, as well.

> *... my address... they probably could have used this to pay me a visit, or do something to me 'face-to-face'... or... they could... steal my identity and try to pass themselves off as me* (#23:Y4M)

When asked about their main protection strategy, one half of the youth informants say they depend on a *combined strategy* to secure the information on their Facebook account; self-censorship combined with the *use of privacy settings* (**Figure 36**):

> *I have made sure that if complete strangers search for my name, they are allowed to see my profile picture and nothing else. They cannot get into my personal profile* (#24:Y9F)

One adult explicitly mentioned the use of privacy settings as a supplementary protection strategy, about one half of the adults considered self-censorship as sufficient in its own right:

> *I guess my settings are quite open, but my strategy is not putting too personal information out there* (#25:A3M)

In addition to the main information protection strategy, two other aspects of experience appeared as important for the basic sense of security; *trust* and a *primary audience view.* These are visited briefly in the next two paragraphs.

5.4.1.1 Supporting decision-making by a primary audience view

Many users have a high count of Facebook friends, and visualizing them all when sharing would be problematic. Some reduce complexity in privacy decisions by focusing on a subset of friends:

> *… when sharing, I do not think about this friend… I met once… several years ago… I think of… my closest friends… the friends who give me updates on my posts* (#26:Y9F)

Primary audience	*Teens*	*Adults*
Recognize the idea of a primary audience	8/9	7/9
Less than 10% of Facebook friends	5	1
From 10 to 20% of Facebook friends	1	2
From 20 to 30% of Facebook friends	1	1
Consider all Facebook friends as audience when sharing	1	2
Recognize the idea, but find it difficult to quantify	1	3

Table 12: Primary audience

Most participants recognize the idea of a primary audience[71] as a subset of their total collection of Facebook friends (**Table 12**). About 2/3 estimated the size of this subset, and the table presents the results of seeing these estimates[72] as a factor of the total number of friends. As usually sharing their posts with 'friends' (or more), the informants are focusing on a primary audience that is significantly lower than their actual audience when sharing. The primary audience is generally described as the people they interact with the most, online or in the physical

[71] *primary audience* refer to the selection (usually a subset) of Facebook friends envisioned by a user when sharing
[72] most informants estimated the size of the primary audience by a range of numbers. When calculating primary audiences' share of total Facebook friends, the largest number in the range was always used

world. Three informants say they do not find it meaningful to talk about a primary audience, as they focus on their complete network when sharing.

5.4.1.2 Supporting decision-making by trust

Experiences of trust	*Teens*	*Adults*
Likely to accept a third-party app if accepted by friends	*	*
Likely to accept a friend request if accepted by friends	*	*
Trust in friends' confidentiality important for sharing decisions	*	*
Share Facebook password with trusted others	*	*
Likely to take precautions when recommended by friends	*	*
Likely to accept a third-party app from a trusted source	*	*

Table 13: Experiences of trust

Another aspect potentially reducing complexity in privacy decisions is trust. Expressions of trust appeared in a variety of contexts in the interviews. A full-scale analysis of trust in the empirical material is not within scope for the study, but as a recurrently mentioned matter, a very brief presentation of the contexts in which the question of trust most commonly appeared in, is worthwhile. **Table 13** gives an overview of these contexts.

5.4.2 A feeling of invulnerability

Another characteristic feature of the privacy experience is the feeling of *invulnerability* towards privacy risks that color the interaction. Two explicit expressions of this experience are the perception of own insignificance in the perspective of a potential perpetrator and the notion of low sensitivity for own, personal information.

5.4.2.1 Insignificant in the perspective of the perpetrator

Most (15/18) informants found it unlikely to be interesting as a potential target for a perpetrator (**Figure 37**). A general reason is associated to anonymity and to the fact that there are hundreds of millions of user accounts on the Facebook service:

> *... I am not sure if anybody... who would bother to get anything from my account? Well, I don't know, but I think like this. We are anonymous in the crowd in there* (#27:A3M)

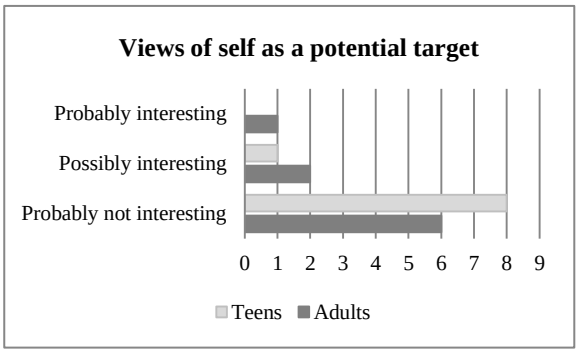


Figure 37: Views of self as a potential target for a perpetrator

Some other reasons were generally made with a touch of humor: 'I am too boring', '…not wealthy enough', '…not famous enough', or 'I am too old'

However, strongly accentuated in both age groups was the conception of own information as of low sensitivity for misuse. The next paragraph reviews some characteristics of this view.

5.4.2.2 Notion of information sensitivity - revisited

Many informants considered their own information as rather invulnerable for misuse. 10 informants rated their own information's sensitivity as *low*, five as *medium*, and three rated this as *high* (**Figure 38**):

> *… I am not that interesting… what I… make available on Facebook is … rather ordinary information of no particular interest… there are photos and situations which may be entertaining… except this, it has… no further potential* (#28:A6M)

Self-censorship was stressed as the major reason for this low sensitivity:

> *… I ask the question 'are there any data at all on Facebook that may be subject to misuse? … it is this matter of staging, again. I do not keep anything on Facebook… that is not in the white pages, or yellow pages, or wherever… and photos that may be compromising, of course, I don't have any of those…* (#29:A8M)

The careful selection of information strengthens a feeling of control, and privacy decisions feel less complex:

> *… I cannot imagine myself as interesting, even if… I have to admit… I have a very open Facebook profile… this is precisely because I think '… nobody… nobody is able to [mis-] use this…'* (#30:A8M)

The informants were asked how they would think and feel if their Facebook password fell into the hands of unauthorized others. Responses strengthened the impression of low sensitivity for own information, as this situation was described as uncomfortable, but harmless. A few concerns for integrity issues related to exposure of personal messages were expressed, yet no concerns for information security were brought up.

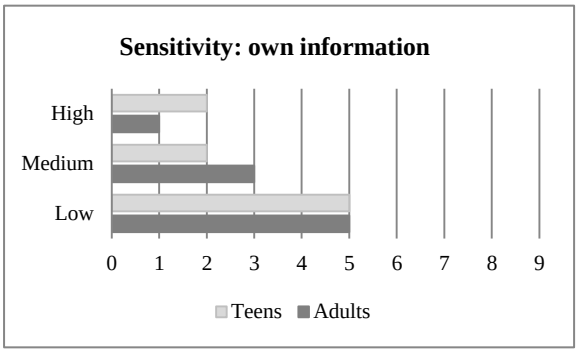


Figure 38: Notion of information sensitivity: own information

Another expression of low sensitivity relates to exposure in Facebook Platform; 1/3 of the participants say they were likely to accept the third-party application asking for extensive rights to access personal information, even if they were aware of the risks associated to this choice.

In sum, various expressions for low sensitivity were expressed in the interviews. Own information was rated lower than any of the specific information categories considered earlier (section 5.2). This was reflected in the model for weak and strong areas of privacy literacy by changing the knowledge

element *Notion of information sensitivity* from *improvable* to *weak*. The updated model is presented in the review at the end of this section (**Figure 39**).

5.4.3 A fragile experience?

The image of security and invulnerability apparent from the previous paragraphs has more colors, though. Expressions of uncertainty and insecurity were observed in the interviews as well. However, these expressions were more toned down, and commonly quite vaguely described. In strength, they were undoubtedly subordinated the expressions of feeling secure and invulnerable. Among others, an abstractly described feeling of possessing insufficient knowledge of privacy came up several times:

> *I would like to think that I am quite skilled, but I am perfectly sure there are a lot of things we quite simply don't know of… things that we don't have enough knowledge of* (#31:A2F)

Contributing in this study turned out as a reality check for many of its participants. Looking this thoroughly towards privacy and security, and reviewing aspects of their own Facebook practice in particular, invited reflections and gave new insights. For the walkthrough of exposure in third-party applications (section 5.3), this was particularly striking. One of the youths describes how this review made her realize a lack of control:

> *… this shows how little control I actually have… I thought I was in control of this… [these settings] are spread out… [Realizing] this was like 'wow!'….* (#32:Y9F)

10 informants expressed emotional reactions to the inconsistencies between anticipations and reality that was uncovered for 14 out of 18 participants. The following transcripts reflect some typical emotions of humor and unpleasant surprise that came up in the review of third-party settings:

> *@@ hahaha @@@... @@@ nohohoho @@ Wow! @@ … @@ I didn't have the vaguest idea that it was this many @@* (#33:Y5F)

> *Wow! I have never used those! I will get rid of the whole lot… None of them… I have never used those!* (#34:A2F)

> *Oh, I use… wow!...how do I delete…? … this must be a joke!... and I thought that I was not a part of this… @@... good grief! @@ Okey… this will be… now I will become much more aware* (#35:A6M)

Many participants said that the study was raising their awareness to the issues involved. At the same time, though, the self-examination implied was adding to the feeling of uncertainty. Participation was described not only as interesting and informative, yet as evoking an uncomfortable feeling of uncertainty and insecurity as well. In transcript #34, the informant expresses how the experience is

likely to change his choices in the future. And another informant describes how she finds herself more aware of privacy issues after the strong focus kept on this topic in the interview:

> *… these things are important, for sure… why haven't I… been more focused [earlier]… I think like this now, when we have gone through it all …* (#36:A9F)

The review showed that no informant had opted to *deactivate platform applications* function (5.3.2). In the review, however, several adult participants wanted to activate this setting immediately.

In sum, the reality check involved in the concrete experiences of the interview situation may influence the participants' general experience of privacy on Facebook in the longer run. The new insights gained might come to 'inspire emotional and behavioral change' in the future.

5.4.4 The user experience – a summary

The participants overall experience of privacy on Facebook is characterized of a *basic sense of security and control***.** This was found a little stronger among the youths than in the group of adults.

Most participants use self-censorship as their main strategy for information protection. Among the young informants it is quite common to use a combined strategy, where they include the use of privacy settings for protection as well. Adults focus their self-censorship primarily on the potential consequences for identity and personal integrity, whereas youths keep a higher focus on security issues and the protection of information against misuse. Adults further envision the possibility of shared information being publicly available in the future, whereas youths potentially aim at the creation of a personal space online. In addition to the focus on a main information protection strategy, trust and a primary audience view potentially strengthen the fundamental sense of security among informants, as well.

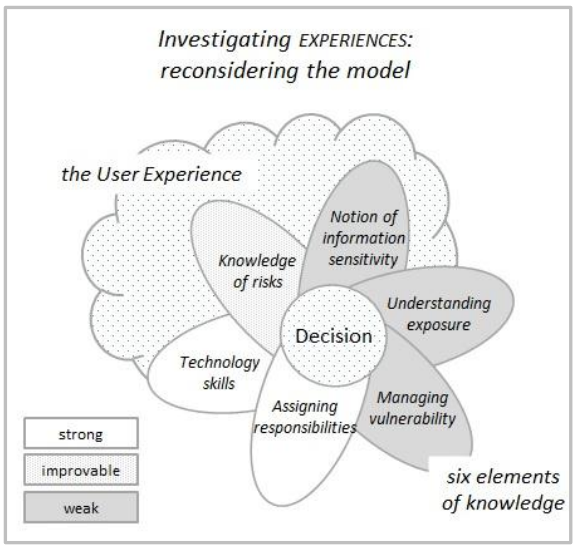


Figure 39: Privacy literacy: Weak and strong areas reconsidered by experiences

Looking into the participants' perceptions of themselves in the perspective of a perpetrator, as well as their notion of information sensitivity for own, personal information, suggested a *low to medium degree of vulnerability* experienced among informants. Their views of their own information called for a downgrade of the knowledge element *Notion of information sensitivity* from *improvable* to weak. This change is reflected in the final version of the model of weak and strong areas of privacy literacy (**Figure 39).**

The informants' secure experience to some extent contrasts their actual privacy situation on Facebook, which is characterized by a high level of exposure to the 'silent listeners' and a medium level of exposure to other users (section 5.3). It also contrasts the general privacy situation for social media use (chapter 2), as well as elements of privacy knowledge revealed in section 5.2, like *Knowledge of risks* and *Notion of information sensitivity*. To the extent that privacy decisions are influenced by their security experience, these decisions may turn out as inadequate to protect privacy.

In order to reflect the knowledge stemming from this EXPERIENCE and the potential influence of this on privacy related BEHAVIOR, a separate knowledge element in the model of privacy literacy is suggested; *Managing vulnerability* (**Figure 39).** This element captures the recognition of vulnerability, choice of an information protection strategy, as well as the goals and time perspective related to the exercise of this strategy. Further investigation will be needed to explore the actual effects of this element on privacy behavior.

Finally, the fragility of the general experience ('experience') was questioned, as the concrete experience ('an experience') of participating in this study seemed to add to the informants' vague and not very pronounced feeling of uncertainty and insecurity. This concrete experience may come to change the general experience of some participants and perhaps their decisions related to privacy on Facebook, in a longer run.

5.5 A review of findings

Based on the preliminary model presented in **Figure 11**, elements of the informants' *privacy literacy* have been investigated from three perspectives in this study; 1) by mapping out the informants' knowledge directly by self-reports and measuring; 2) by comparing and cross-checking some of these findings to informants' behavior in the form of privacy decisions in actual Facebook use; and 3) by investigating the informants' privacy-related user experiences, which frame the practical application of their privacy knowledge.

The first round of analysis focused on measuring of the informants' KNOWLEDGE. Three knowledge elements from the preliminary model, *Knowledge of risks***,** *Notion of information sensitivity***,** and *Understanding exposure,* were found as *improvable* (**Figure 26**). Ambiguous results for *Understanding Exposure* in particular, pointed this out as a potential problem area.

The analysis of knowledge uncovered some valuable details, like the tables *of most focused threats* (**Table 8**) and *least focused threats* (**Table 9**), reflecting a low focus on current threats like social engineering and coupling. And also the notion of *expressive information* as the *least sensitive* information type may increase users' vulnerability to these threats in particular. The views of most and least focused threats were common for the age groups. The two elements *Technology skills* and *Assigning responsibilities* were found *strong* for both groups

In the subsequent look into the informants' BEHAVIOR in some areas of Facebook use, several indications of a potential relationship between knowledge and behavior were observed. The impression of all three aspects of *Understanding exposure* as potential problem areas was confirmed and strengthened in this cross-checking of knowledge to actual behavior. A downgrade of the knowledge element from *improvable* to *weak* (**Figure 33**) resulted from this cross-check.

The actual exposure of personal information to third-parties in *Facebook Platform* was found as *high*. The actual exposure through functions in *Facebook Core* was found s *medium*. In Facebook Platform, the *young* informants had significantly higher exposure than the adults through their *own use* of third party applications (**Figure 29**), whereas both groups had high exposure through *their friends' use* of applications (**Figure 30**). Informants generally *did not use* the *security functions* provided by Facebook to protect their information (**Figure 32**).

Investigating the informants' behavioral choices further *confirmed* the rather *low* focus on expressive information and threats like social engineering and coupling found in the investigation of KNOWLEDGE, previously.

Analyzing the informants' EXPERIENCE of their interaction with Facebook gave further information about their privacy literacy. This analysis uncovered two distinctive features of the informants' general privacy experiences; *a basic sense of security* and *a feeling of invulnerability*. This experience diverge from their actual privacy situation on Facebook and to the extent that it influences their privacy decisions, it may come to influence their privacy decisions negatively.

Analyzing experience uncovered differences between the age groups related to the choice of information protection strategies, goals, and timeframe for the privacy process. Youths tend to focus on security issues and the building of a personal space for communication on Facebook. Most of them point to the use of Facebook's privacy settings as a main strategy for protection of information and one half of them use self-censorship in combination with privacy settings. Adults generally focus on identity and self-presentation online with the purpose of sharing information appropriate for the potential, yet not necessarily intended, public availability of information in the future. Summarized, self-censorship, self-presentation and potential publicity in a long-term perspective commonly characterize the adults' perspectives, whereas privacy settings, data protection, privacy, and immediacy are keywords typical for the youths' privacy process.

As a result of the analysis of EXPERIENCE a sixth knowledge element was added to the model of privacy literacy; *Managing vulnerability.* And as this analysis further found the informants' view of low sensitivity for own information as strengthening and expanding the impression of knowledge from the first round of analysis, the knowledge element *Notion of information sensitivity* was downgraded from *improvable* to *weak* (**Figure 39**).

Highlights from the data analysis are illustrated in **Figure 39** and summarized in **Table 14** on the next page.

	Knowledge element	*Overall impr.*[73]	*Overall age diff.*	*Area*	*Impr.*	*Age diff.*
Knowledge	Technology skills (self-reported)	Strong	Youth +[74]	PC and Internet use	High	-[75]
				Facebook use	High	-
				Facebook settings	High/Med	Youth +
	Assigning responsibilities	Strong	-		High	-
	Knowledge of risks	Improvable	-	Self-reported knowledge	High/Med	Youth +
				Ind risk awareness profiles	High/Med	-
				Risk scenario	Medium[76]	-
	Notion of information sensitivity	Weak	(Youth +)[77]	Self-identifying info.	High/Med	Youth +
				Access-enabling info.	Med/High	Youth +
				Expressive info.	Med/Low	Adults +
	Understanding exposure	Weak	(Adults +)[78]	In general	High/Med	Adults +
				In Facebook Core	Med/High	Youth +
				In Facebook Platform	Low/Med.	-
Behavior	Actual exposure on Facebook	Med/High	Youth +	Exposure FB Core	Medium	-
				Exposure FB Platform	High	Youth +
				Exposure in FB Security	High	-
Experience	A basic sense of security	Weak[79]	n/a[80]	Based on a preferred protection strategy[81]	n/a	n/a
	Low vulnerability			Based on low value for own info		n/a
	A fragile exp.?			Reality check inspires changes in behavior?		n/a

Table 14: Data analysis: a review of findings

[73] impr. = impression
[74] the + sign indicate that the measure observed for this group was in the higher end of the scale
[75] hyphen = no general age difference can be stated
[76] some risks are less focused (among these social engineering, coupling)
[77] youths show a higher focus on SI and AI than adults. For views of sensitivity for own, personal information no significant age differences were observed
[78] adults have a better understanding of exposure in general and give the impression of applying this knowledge in interaction
[79] the experience is not subject to measurement, and in this case, weak reflects that the experiences was diverging from the actual privacy situation of the informants
[80] n/a = not applicable
[81] as opposed to adults, half of the youths depend on a combined data protection strategy

6. DISCUSSION

In this chapter, findings are discussed in light of the four research questions. Section 6.1 looks at the relevance of privacy knowledge for non-secure behavior (Q1). Section 6.2 discusses the interplay between privacy experiences and privacy behavior in explanations of non-secure behavior (Q2). Section 6.3 describes the weak and strong areas of privacy literacy uncovered (Q3), and section 6.4 reviews the differences in privacy literacy observed between the age groups (Q4). Section 6.5 reflects on the importance of the theoretical contributions for the research process, and points out some particularly supportive concepts: *emotions*, *time*, *negotiations*, and *identity*.

Section 6.6 finalizes this chapter by presenting an evaluation of the study; discussing aspects relevant for its scientific quality and the role of theory in the research process.

6.1 The relation between knowledge and non-secure behavior

RQ1: *Can inadequate knowledge of privacy explain why users sometimes show non-secure behavior on Facebook?*

Several findings indicate privacy knowledge as important for behavior. The most significant indication is associated to informants' understanding of their information exposure to third-parties (*exposure in Facebook Platform*), where measures of knowledge indicated a potential problem area (5.2.5.3). The cross-check of knowledge to actual behavior confirmed this impression; actual exposure to third-parties was found as high (5.3.2). Age differences were observed in this area, these are reviewed in the discussion of RQ4.

A similar relationship is suggested for information exposure through the core functionality on Facebook (*exposure in Facebook Core).* This was indicated as a potential problem area by the measures of knowledge (5.2.5.1), and the cross-check to actual behavior (5.3.2) confirmed this impression. A medium level of exposure was observed for Facebook Core.

On the individual level, the relationship between knowledge and behavior was strengthened by the two informants misunderstanding the privacy settings, resulting in a higher level of exposure than intended. This problem was indicated by several knowledge measures for these informants: their understanding of information exposure through Facebook core functionality (*understanding exposure in Facebook Core*) was rated as Low for both; and in their self-reports for *knowledge of Facebook privacy settings*, both rated this knowledge by the medium level value *good*. The latter value is in the lower end of the scale actually applied by informants for self-reports. Another individual level example indicating a relation between knowledge and behavior is the case that only one participant was protecting her personal information against sharing by friends' use of third-party applications. This informant rated her *knowledge of Facebook privacy settings* as *pretty good*, and her

understanding of exposure of information to third parties (*understanding exposure in Facebook Platform*) was measured as *high*.

A relation between knowledge and behavior was indicated in two other knowledge areas, as well, more indirectly than the above. Informants generally expressed a restrictive attitude towards registering *self-identifying* and *access-enabling* information, but similar considerations were not exhibited for *expressive information* (*Notion of information sensitivity*, 5.2.4.3). This pattern was recognized in the review of their actual information sharing on Facebook, and indicates a relation between knowledge and behavior. More indirectly, it can be interpreted as a relationship between actual exposure and the low focus on threats like social engineering and coupling revealed in *Knowledge of risks* (5.2.3.4), as well. Expressive information has the potential of providing extra power to attempts of imposing these threats upon others (2.1.2)

However, finding that informants in general do not employ the security functions provided by Facebook (5.3.3) does not support an explanation of non-secure behavior by level of knowledge, as the focus on security issues was quite pronounced, particularly among youths. This lack of rationality may be interpreted as a result of the informants' experiences of privacy in their Facebook interactions, a matter which is discussed for RQ2, below.

CONCLUSION: Findings suggest that privacy knowledge can explain why users sometimes show non-secure behavior on Facebook. This is indicated by three areas of knowledge identified as weak or improvable in the model of privacy literacy: users' understanding of information exposure (*Understanding exposure*), users' understanding of and awareness to risks (*Knowledge of risks*), and their conceptions of sensitivity for misuse related to different categories of information; expressive information in particular (*Notion of information sensitivity*). The most significant indicator was *Understanding Exposure*.

6.2 The interplay between knowledge and user experiences

RQ2: *Do users' experiences of privacy on Facebook complement the rational, fact-based knowledge aspects of their privacy literacy?*

Findings suggest that privacy experiences can complement the rational fact-based knowledge aspects of users' privacy literacy in two ways; by explaining a lack of rationality in some of their privacy decisions and by improving and strengthening the impressions from knowledge measurements.

The informants' experience of security and low vulnerability may explain the lack of rationality in most users' decisions of not employing *Facebook security functions*, despite the awareness of security risks expressed in the measures for conceptions of information sensitivity for self-identifying and

access-enabling information, among youths in particular (*Notion of information sensitivity,* 5.2.4.1, 5.2.4.2). This assumption of user experiences as influencing actual behavior cannot be confirmed, however, several aspects point in this direction. The question of user experiences influence on actual behavior is further discussed below.

The investigation of users' experiences also improved and strengthened the impression of knowledge found by measuring knowledge in previous analyses. This is indicated in the changed impression of knowledge described in the revisit to their *Notion of information sensitivity* (5.4.2.2), where the experience complemented and strengthened the impression of low sensitivity for expressive information (5.2.4.3), and also revealed that informants generally find their own information as of low vulnerability for misuse. It is further indicated by the emotional reactions and reflections appearing when reviewing their information exposure to third-parties, which strengthened the impression of non-secure behavior as related to a lack of knowledge in this area (*understanding exposure in Facebook Platform,* 5.2.5.3 and 5.3.2.1).

The assumption that user experiences influence actual behavior is based on the interpretation that protection feels less important for informants who are experiencing themselves as rarely exposed to threats (section 5.4). To confirm such assumption, a more thorough investigation of the privacy decision process would be required. However, previous research has found a relation between experiential aspects and privacy behavior (section 2.3). And other findings from this study point to experience as a potentially important factor for privacy behavior, as well. For example, the feeling of uncertainty in the authorization process for third-parties appeared as influencing the informants' privacy decisions (5.3.2.1); trust in others was denoted as simplifying the privacy decisions (5.4.1.2); as was the experience of a primary audience (5.4.1.1). And further, the reactions in[82] and after[83] the review of exposure to third parties demonstrated the potential influence of concrete experiences ('an experience') on behavior and knowledge.

A competing explanation for the problem of most users not employing *Facebook security functions* could be related to Facebook design and users having trouble with recognizing the security settings. Accessing these settings require users to navigate between different web pages (associated to two separate main menus: privacy settings menu vs. account settings menu[84]). The splitting of settings on many pages may make these less apparent to users.

[82] informants wanted to deactivate Facebook Platform functions immediately (5.4.3)
[83] informants expected a change of behavior in the future (5.4.3)
[84] this interface has been changed and looks different today than at the time of data collection

This study has shown that the informants' secure experience of privacy on Facebook contrasts their actual privacy situation, which is characterized by a *medium to high* level of information exposure (section 5.3) in a context of many privacy threats (chapter 2). To the degree that user' privacy decisions are influenced by this secure experience, these may turn out as inadequate to protect their information.

To reflect the findings related to experience, a new knowledge element was introduced to the model of privacy literacy: *Managing vulnerability* (5.4.4). This knowledge element represents the knowledge coming from the vulnerability experience and captures, recognition of vulnerability, chosen information protection strategy, as well as the goals and time perspective related to this strategy.

CONCLUSION: Investigating privacy decisions from several perspectives (KNOWLEDGE, BEHAVIOR, and EXPERIENCE) provided more rich insights into the informants' behavior in privacy related situations. Findings suggest that privacy experiences can complement the rational fact-based knowledge aspects of users' privacy literacy in two ways; by explaining a lack of rationality in some of their privacy decisions, and by improving and strengthening the impressions from knowledge measurements. Further investigations of the decision process are recommended to understand the influence of experience on behavior in detail.

6.3 Weak and strong areas of privacy literacy

RQ3: *Are some areas of the users' privacy literacy identified as weaker than others, in this way as candidates for improvement?*

The findings reflect that informants generally recognize themselves as the main responsible for protecting the information shared online. Their general technology skills were reported as strong; this impression was not weakened in the interviews. As previous research has shown problems in the use of self-reported privacy knowledge (chapter 2), a more thorough investigation of technology skills potentially give other results. Such investigations have not been within the scope of this work, though.

As this study is aimed at explaining non-secure behavior by a low level of privacy knowledge, the most interesting findings for this study are related to the *weak* and *improvable* areas of literacy.

Informants in both age groups are potentially vulnerable for misuse of information due to features of the *experience* that characterize their interactions with Facebook (*Managing vulnerability*, 5.4); by the basic sense of security; by the conception of low sensitivity of own personal information; and by employing a limited number of main strategies for protection of information.

The privacy experience of the young informants was characterized by a relatively short timeframe and an aim at creating a personal space online. These aspects potentially increase vulnerability, as digital information tends to be long-lived and the risks for misuse are numerous, despite the youths' regulation of information control by Facebook privacy settings. Adults expressed a more long-term perspective for their privacy decisions, but base their sharing on a rather public policy. Sharing publicly, combined with a lack of knowledge of certain risks (*Knowledge of risks*, 5.2.3) may put adults at risk, unwittingly.

The informants' risk awareness was observed as relatively strong, but a low focus on current threats like *social engineering* and *coupling* potentially increases their vulnerability (*Knowledge of risks*, 5.2.3.4). This impression is strengthened by the low recognition of the need to protect *expressive information* (e.g. preferences, 'likes', and interests) against misuse. Expressive information was commonly not recognized as valuable in the hands of a perpetrator (*Notion of information sensitivity*, 5.2.4.3).

The extensive sharing of personal information with 'silent listeners' through the use of third-party applications came as a surprise on a significant number of informants (*exposure in Facebook Platform, 5.3.2*). This is intriguing, in light of the excessive use of third-party applications typical for today's technology use (chapter 2). An insufficient recognition of the volume of third-party exposure, problems related to the authorization process for third-parties, as well as a lack of understanding of Facebook's privacy settings for sharing with third-parties (*understanding exposure in Facebook Platform, 5.3.2.1*) was observed. The interviews revealed *weak knowledge* as an important explanation for the extensive sharing in this area (*Understanding exposure in Facebook Platform,* 5.3.2.1), but also the *user experience*, by the trade-off usefulness/pleasure versus protection in the authorization process for third party applications, may be important for this situation. This matter is further discussed for RQ4, below.

The model of privacy literacy illustrates overlap in the different knowledge areas and knowledge elements may have strong internal relations. For strong privacy literacy, these internal relations should be recognized, in addition to knowledge in the separate areas. Assumedly insufficient knowledge about such relations was uncovered in analysis.

An example of these relations is how a user's conception of a particular information element's sensitivity for misuse (*Notion of information sensitivity, 5.2.4*) expectedly is closely related to her understanding of threats *(Knowledge of risks, 5.2.3*): who would find this information valuable and for what purpose? Knowing the information in need of protections requires updated knowledge about the risks relevant for its respective information category. In analysis, several cases of insufficient knowledge about relations between threats and information categories were observed; the relation

from *social engineering* and *coupling* to *expressive information*, as mentioned previously, but also the relation between the risk for *identity thefts* and access to a *complete profile* of personal information about a user. Even if identity thefts was the most focused threat among participants, very few focused that the gathering of a *complete profile* of information of all three categories, like a Facebook profile, can be a highly valuable tool in the hands of a perpetrator.

Another example of internal relations in the model of privacy literacy is the (assumed) relation between a *user's experience* of an interaction (*Managing vulnerability*, 5.4) and her *Knowledge of risks* (5.2.3). To what extent are users' willing to invest in prevention for a risk they experience as not relevant for their own privacy situation? Further research is needed to confirm the influence of a basic sense of security and invulnerability on users' privacy decisions, but as discussed for RQ2 (6.2), previous research, as well as findings of this study, point in this direction.

CONCLUSION: Weak and improvable areas of privacy literacy were identified in the empirical analysis: *aspects of the user experience* like timeframe, goals, and the basic sense of security; *a low focus on current risks* like social engineering and coupling; a *weak notion of sensitivity for* misuse of the users' own, personal information in general, and for expressive information in particular; as well as a significant lack of understanding of the extensive *sharing with third-parties.* Insufficient knowledge about relations between the knowledge elements in the model of privacy literacy was observed, as well, like the relation between *information sensitivity conceptions and risk awareness* and the potential relation between the *user experience and risk awareness*. The weak and strong areas of privacy literacy observed for this study are illustrated in **Figure 39** and summarized in **Table 14.**

6.4 Privacy and age

RQ4: *Does teens' privacy literacy on Facebook differ from adults' privacy literacy? If so, how?*

The most significant age differences observed relates to the user EXPERIENCE (section 5.4) and informants' choice of information protection strategies, goals, and timeframe for the privacy process. Adults generally report self-censorship as their preferred, and only, information protection strategy. They are likely to focus self-presentation and the shaping of an online identity in a long-term perspective, and the potential public availability of information in the future is an important criterion for self-censorship. To a larger extent, youths report the use of several protection strategies; privacy settings are used to complement self-censorship. Youths are likely to focus their privacy process on the immediate need for protecting information against security threats and on preventing information from access outside an audience of their own choice ('the outsider threat', 2.2.1).

As both perspectives have their pros and cons, it is not possible to claim that one is better suited to protect privacy than the other. A restrictive censorship for self-presentation focused on data

preservation in a long-term view is beneficial, as is the short-term view on protection against security threats and outsider's access to personal information, as well. Informants in both age groups would probably benefit from including aspects of the other group's perspective into their own view. And further, the current level of threats on Facebook (chapter 2) proposes an expansion of the repertoire of information protection strategies employed by both age groups. Combining many strategies[85] would strengthen the level of information protection.

As to measurements of rational, fact-based KNOWLEDGE, the most important differences observed relate to *Knowledge of risks*, where adults revealed a better understanding for commercial infringements of personal information (5.2.3.5), as well as of the risks associated to data persistence (*Understanding exposure in general*, 5.2.5.1). Youths appeared with a better understanding than adults of the privacy settings for Facebook core functionality (*Understanding exposure in Facebook Core*, 5.2.5.2), yet no age differences were observed for privacy settings for third-parties (*Understanding exposure in Facebook Platform*, 5.3.2.1).

As to BEHAVIOR, age differences were observed for the informants' actual exposure of personal information on Facebook. Youths' exposure to 'silent listeners' like third-parties, Facebook, and advertisers was significantly higher than for adults *(Exposure in Facebook Platform*, 5.3.2). A similar pattern was not observed for the measures for knowledge of exposure to third-parties (*Understanding exposure in Facebook Platform*, 5.3.2.1). However, this may be explained by other knowledge factors, like the youths' weaker understanding of the problem of data persistence (*Understanding exposure in general*, 5.2.5.1) and their weaker understanding of the problem of commercial infringements of personal information (*Knowledge of risks*, 5.2.3.5). Another possible interpretation is to explain this difference by differences in the user experiences, like the stronger sense of security found for youths (a basic sense of security, 5.4.1) potentially influencing their privacy decisions negatively or by a different balancing of the trade-off usefulness/pleasure versus protection by youths and adults in the authorization process for third party applications. Users' decision process has not been investigated sufficiently in this study to confirm either of these latter explanations related to the user experience, though.

Technology experience was indicated as potentially important for privacy literacy (5.2.1.1 and 5.2.3.1). The two informants with short experience were both adults. Most adult participants in this study were quite experienced technology users, though, and the sample of users with low technology experience is too small to claim any age differences in this respect. To the extent that adults have less

[85] like self-censorship; familiarize with the privacy settings; maintain settings regularly; use security functions whenever available; employing well-considered password policies; and staying updated on relevant risks; etc.

technology experience than young people, this potentially leaves them more vulnerable to privacy issues.

CONCLUSION: The most significant age differences observed for privacy literacy was revealed in the analysis of EXPERIENCE, and is related to the informants' choice of information protection strategies, goals, and timeframe for the privacy process. Self-censorship, self-presentation and potential publicity in a long-term perspective commonly characterize the adults' perspectives, whereas privacy settings, data protection, privacy, and immediacy are keywords typical for the youths' privacy process. Age differences were also observed in KNOWLEDGE, as adults appeared with a better understanding of the risks associated to the long-term preservation of data on the internet (data persistence) and to the commercial infringements of personal information. Youths appeared with a better understanding of the privacy settings for Facebook core functionality. As to BEHAVIOR, age differences were observed for the informants' actual exposure of personal information on Facebook, as youths' exposure to 'silent listeners' (third-parties, Facebook, and indirectly advertisers) was significantly higher than for adults.

6.5 Reflections on the use of theory

Two contributions dominate the theoretical perspective applied in this study; McCarthy and Wright (2004) by the structure provided by their four threads and six processes of the user experience; and Palen and Dourish (2003) by their descriptions of the dialectics and dynamics of the privacy process and the process boundaries of time, identity, and disclosure. Their contributions have supported a research focus on emotional as well as rational aspects of privacy and on the negotiations involved in the privacy process. These perspectives have allowed for nuances and for viewing data from different angles in data analysis.

The main part of the analysis of experience was focused on uncovering the general ideas and mindsets overarching the users' Facebook interactions ('experience'). In this work, the theoretical concepts related to *emotions, time, identity,* and *negotiation* has been very useful and given valuable directions for the process. In the analysis of the concrete, limited experience informants had when reviewing their actual exposure in Facebook Platform ('an experience', section 5.3, 5.4), the six meaning-making processes and the sensual and compositional threads were of great support, as well.

From the starting point described as '… what we would generally think of as cold computational processes – perceiving, thinking, reasoning, decision making, categorizing – are shot through with values, needs, desires, and goals' (McCarthy & Wright, 2004, p. 85), emotions have been a particular focus in this work. McCarthy & Wright's idea of the emotional thread has supported the research process from development of the interview guide through interviewing to data analysis. The data structure built in analysis came to reflect emotional elements as they appeared from the empirical material.

The time aspect is important in both perspectives and has been central in the data analysis. The temporality boundary and the spatio-temporal thread both focus the interplay between the past, the current, and the future in our aims to control the privacy process. This focus helped uncovering differences in youths' and adults' time perspectives; differences potentially relevant for their choices in the privacy context. Adults tend to orientate their decisions to the future to a larger extent than the youth. Basing their decisions of a more immediate time conception, youths' privacy processes are potentially more vulnerable to problems related to data persistence. The spatio-temporal thread further drew attention to the informants' in part diverging goals as to the use of Facebook for publicity versus privacy.

The concept of identity is also captured by both perspectives. Technology use strengthens and shapes our identities; this process is relational and happens in dialogue with others; 'self and other making sense of experience' (John McCarthy & Peter Wright, 2004, p. 107). The identity boundary reflects the purpose of controlling others' interpretations of our selves by displaying and shaping our identity in a continual process. Among adults, the investigation uncovered a tendency of self-representation for the future and for potential publicity. For youths, identity is important as well, yet the goals for self-representation are more immediate and potentially related to an aim of presenting oneself to more limited social contexts. Data persistence and the desituating of information (lose time, place or intention in mediation - section 3.2) can disrupt the regulation of goals by the identity boundary.

The disclosure boundary reflects the core process of controlling the disclosure of personal information, a process where the goals of privacy and publicity are in tension. Information disclosure by friends or third-parties and data persistence both have the potential to disrupt the regulation of this boundary. In this process, the adults expressed a tendency to focus on controlling the content of the information shared, whereas youth were more focused on controlling this boundary from an access/no access perspective.

Through its focus on dialectics, applying the *Privacy For a Networked World* framework (Palen & Dourish, 2003) opened up for richer nuances in the empirical data. By viewing privacy as a continual negotiation process, opposites in the material became more obvious and room was given for the exploration of conflicting perspectives throughout the analysis process. The dichotomies usefulness/pleasure versus protection, and privacy versus publicity, both appeared as recurrent trade-offs of the privacy process. This perspective made other opposites more visible, as well; like the tension between security and uncertainty in the general privacy experience, where security 'wins' the negotiation process assumedly supported by a main protection strategy, trust, a primary audience view, and the informants' conceptions of low vulnerability for themselves and their personal information.

The six sense-making processes of experience was found most helpful in directing the focus of the analysis of the concrete, limited experience ('an experience') informants had when reviewing their actual exposure in Facebook Platform (section 5.3, 5.4). The compositional thread was apparent in the lack of understanding uncovered for transition between different privacy contexts on Facebook. The reactions in the review indicated that the compositional thread was broken, and technology did not support framing the user experience adequately.

The conceptual separation of 'experience' from 'an experience' (Forlizzi & Battarbee, 2004) was useful for the analysis of user experiences, and the study of secure experiences by Mathiasen and Bødker (2008) has been a major inspiration for the approach used in this work.

6.6 Evaluating the study

Qualitative studies can be argued to be subjective by nature. Awareness of the influence of values and biases is appropriate, especially in the processes of problem formulation, data analysis, and in presentation of the results (Walsham, 2006). A common set of criteria for *assessment of scientific quality* in qualitative studies is not yet agreed upon (Bryman, 2008) [86], however, some generally accepted guidelines for assessing quality in research can support the evaluation of studies. In this section I discuss the study in light of its application of theory (6.5.1), and by the concepts of validity, reliability, and reflexivity, as well as by some recommendations for the study of privacy in HCI (6.5.2).

6.4.1 The role of theory

Walsham (1995) separates between three ways of using theory in interpretive studies; as an initial guide to design and data collection; as part of an iterative process of data collection and analysis; as well as a final product of the research. The theoretical perspective chosen for this study (section 3.4) does not provide very thorough instructions for applying these contributions to the research process; however, despite the lack of detailed instructions, the theoretical perspective has been applied actively as a lens to view the world. This lens has provided useful support and directions for numerous thematic and methodological choices made throughout design and implementation of the research process.

De Vaus (2001, ch. 1) describe two different styles of research based on the role of theory in the research process: *theory testing* (moving from the general to the particular by using deductive reasoning to build propositions from the theory and test if these are correct), and *theory building*

[86] checklist for evaluation has been proposed by several researcher, the checklist of Malterud (2002) has been used to guide this study

(making sense of observations, and using inductive reasoning to build a theory from these for later testing). The research process in this study has been data-driven and fits into the latter category. The rather strong empirical focus has made my own judgments important for the final results, and the process has some common features with the Grounded Theory perspective where 'researchers are encouraged to draw on their own theoretical backgrounds to help inform the study' (Sharp, et al., 2007, p. 390). However, the directions extracted from the selected theoretical perspective have been too pronounced to characterize this research process as Grounded Theory.

6.4.2 Validity, reliability, and reflexivity

Validity and reliability are generally accepted concepts in assessing scientific quality (Bryman, 2008; Malterud, 2003; Sharp, et al., 2007). Validity concerns the degree of correspondence between the research questions and the empirical observations used to elucidate these (*internal validity*). Did the researcher collect empirical data relevant for the research questions? *Reliability* is about accuracy in the process of collecting and analyzing data. Would the study, when replicated by other researchers, yield the same results? The idea of *reflexivity* supplements the concepts of validity and reliability. This concept grasps the reflectiveness of social researchers to the potential influences on results from their 'methods, values, biases, decisions, and mere presence in the very situations they investigate' (Bryman, 2008, p. 698). And finally, the concept of validity further includes an evaluation of the study's degree of transferability to others parts of reality (*external validity*). External validity requires internal validity, reliability, as well as reflexivity in the conduct of research. The following paragraphs reviews some aspects related to these concepts.

6.4.2.1 Internal validity

Research design is associated to the logical structure of the inquiry, and the purpose of creating a good research design is to reduce ambiguity of the research evidence. (De Vaus, 2001, ch. 1). The research questions and the analysis approach of this study were refined gradually throughout the research process to increase the quality of this design. The fundamental logical structure was not subject to major changes in these iterations, though.

Several measures were taken throughout the research process, to capture data relevant for the research questions. The data collection arrangements were gradually developed with useful support by the study participants. Several data collection methods were tested and a variety of interviewing techniques were triangulated, tested and applied. The phenomenon in question was studied from several perspectives (knowledge, behavior, and experience) in order to strengthen quality of the final results. In data analysis, qualitative and quantitative analysis approaches were triangulated, and data suitable for comparisons were extracted. These measures assumedly strengthen the validity of the research results.

Some challenges relate to the chosen research strategy. When approaching qualitative data quantitatively, results potentially relocate too far from their originating contexts. In order to prevent this, continual recontextualizations of results to raw data was emphasized in both phases of the data analysis. Another potential challenge relates to the lack of sufficiently rich information provided by the sample in data collection. The iterative sampling and analysis approach chosen for the study usually contribute in preventing this problem of reaching the point of saturation prematurely. In the first, qualitative part of the data analysis common features in the data material were observed, these were interpreted as indicating clear tendencies in the empirical material. This observation encouraged the decision to go on with a second, more quantitative analysis phase. However, an alternative interpretation of this observation might be that the point of saturation was reached prematurely due to insufficient diversity in the research sample. As the sample was varied regarding to age, experiences, gender, as well as occupational backgrounds, and size-wise was not small for a qualitative study, the first interpretation is assumed for the project.

6.4.2.2 Validity in studies of privacy

Potential problems concerning data validity associate to the study of users' attitudes, as these are problematic to get access to and to categorize. In order to transcend the discrepancy between attitudes and behavior commonly experienced within studies of privacy, Iachello and Hong (2007) emphasize the need to balance directly asking about privacy to observations of the users' behavior. They suggest the use of techniques providing sufficient context as well as concrete situations, in order to get closer to the users' experiences: '…personal privacy dynamics should be investigated with studies that closely simulate the experience of the users, rather than on a hypothetical basis' (2007, p. 29). Howe, et al. (2012) also point out this need to check intention versus actual behavior, and recommends accessing the emotional reactions of users through for example the use of simulation based techniques.

This study applied various techniques to prevent the problem of attitudes potentially deviating from behavior: 1) asking directly about the informants' privacy understandings and preferences; 2) asking indirectly by exemplifying other users' understandings and preferences (impersonal scenarios); 3) asking indirectly by asking informants to view themselves through the eyes of others; 4) observing static aspects of behavior (walkthrough of privacy settings), as well as 5) observing immediate behavior by studying the reactions related to the walkthrough of privacy settings and actual exposure. Applying this selection of methodological angles and techniques provided richer data than expected from simply asking directly about privacy, and yielded information of rational, fact-based privacy knowledge, as well as of reflections and emotional reactions of potential importance for this knowledge.

Investigating the phenomenon from three angles of KNOWLEDGE, BEHAVIOR, and EXPERIENCE are expected to strengthen the validity of results. To illustrate benefits of cross-checking the analysis of knowledge against actual behavior, weighted averages was computed for the values in **Figure 15**, **Figure 25** and **Figure 31**. These figures all picture the informants' *understanding exposure in Facebook Platform*[87], yet approach this knowledge from different angles[88]. Weighted averages for each approach reflected a high-medium level of knowledge from **Figure 15**, *medium-high* from **Figure 25**, and *medium-low* from **Figure 31**. This shows how the evaluation of knowledge was gradually developed and strengthened throughout the analysis.

6.4.2.3 Reliability

Due to the nature of the research process and the empirical data, the replicability requirement does not have the same relevance for the qualitative study as for quantitative research. However, it is important that the researcher organize the qualitative research process allowing for a future investigator to understand this process as well as the conclusions drawn for results.

The research process of this study has been systematically documented by use of several tools. This documentation on various formats allows for better traceability in the future, yet has supported quality in the current process, as well. In the presentation of results, it has been an aim to detail aspects of the process properly, from problem description and theoretical frame of reference, to sampling strategy and procedures for analysis of empirical data.

Some comments apply to the measurement of knowledge and behavior in particular. The procedures applied for measuring of knowledge (described in 4.4.2.5) are relatively simple[89]. More advanced methods for measuring would probably be required if the results were to demonstrate a high level of knowledge by informants. Aiming at uncovering lack of knowledge, like here, these procedures are assumed as sufficient. And further, the analysis of exposure (section 5.3) is concentrated on the informants' explicit protection of information, as well as on their authorization of others' access to information. These measures are assumed as relevant indicators of actual exposure in the context of this study, but would probably be insufficient as measures for the informants' actual risk level on Facebook.

---

[87] **Figure 15** includes knowledge from both **Figure 24** and **Figure 25**, which have relatively similar patterns of results

[88] **Figure 15** = self-reports; **Figure 25** = measurements based on examples of other peoples application activity; **Figure 31** = measurements based on the informants' own behavior

[89] for example, **Knowledge of risks** are measured by self-reports adjusted for a qualitative impression of what risks the informants' know of and which seems to concern them the most. More aspects are potentially important when aiming at demonstrating a high level of risk knowledge, like knowledge of safe practice, what actions participants take to address known risks, etc.

6.4.2.4 Reflexivity

A general challenge in interpretive studies is to understand social meanings, the meaning-making processes, and the contexts within witch it all takes place (Walsham, 1995). The process of interpreting the informants' meaning-making is inseparable from the researcher's own interpretations of the world, and also, as even a simple human action like a twitch by the eye can have several interpretations, the final results represent *second- (or even third-) order interpretations* of social phenomena (Geertz, 1973, ch. 1). This has implications for our understanding of the empirical data, as 'what we call our data are really our own constructions of other people's constructions of what they and their compatriots are up to' (1973, p. 9). The role of the qualitative researcher is inherently subjective due to the subjective character of qualitative data collection and analysis, but also due to the researcher's sharing of concepts and interpretations in the interview context which potentially influences the informants' own interpretations (Iachello & Hong, 2007; Malterud, 2002; Walsham, 1995).

The theoretical perspective described in section 3.4 reflects some fundamental premises for this work. In the practical research process, I have been aware of the participants' statements and actions as potentially arising from cultural, social, or linguistic contexts different from my own. The information provided to participants in the interview context was aimed to balance against the ethical requirement of taking care of the participants' interests and integrity. I also tried constantly considering my own role in the interview process. The relation between the empirical material and the interpretations of this material was attended to by thorough transcriptions and by recurrent recontextualizations of findings to the empirical data throughout the process of analysis and presentation of results.

6.4.2.5 External validity

The methodological choices for this study have consequences for its degree of transferability of results to other parts of reality. Qualitative interviews usually do not scale well (Iachello & Hong, 2007). The use of a *strategic sample*[90] introduces a subjective element into the research process, which leave the empirical findings as *not generalizable* to a population. The results potentially have some transferability as to concepts, though (Bryman, 2008; Malterud, 2002; Norwegian Committees for Research Ethics, 2011). To increase the external validity of this work, the sample and the principles for the sampling process are described in the paragraphs 4.1.1 and 4.4.1.2, as well as in section 5.1. A model of privacy literacy is suggested, and this models potential relevance for behavior is indicated by

[90] a purposively selected sample from the phenomenon's sampling frame, as opposed to a *representative sample*, i.e. a sample that reflects the population accurately (Bryman, 2008)

the weak and strong areas of the informants' privacy literacy described. These findings can be useful on a conceptual level, and also their transferability can be increased by further testing in a study of more generalizable character. This study does not claim generalizability as such.

The above evaluation of research quality finalizes the presentation in this chapter. Potential issues related to the research process have been brought forward, as well as some actual measures taken to pursue quality throughout the process. However, as Walsham (2006) point out: a good process is important, yet the most important criterion of quality in all research is its capability to provide interesting research results.

This page is intentionally left blank.

7. CONCLUSIONS

7.1 A model of privacy literacy

Investigating privacy decisions from several perspectives (KNOWLEDGE, BEHAVIOR, and EXPERIENCE) provided more rich insights into the informants' behavior in privacy related situations.

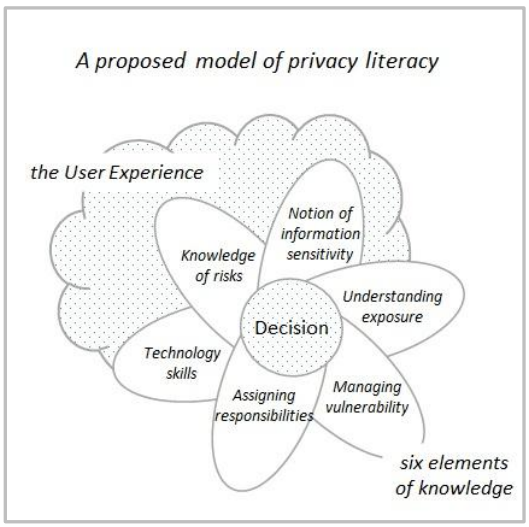


Figure 40: A model of privacy literacy

This work proposes a model for privacy literacy (**Figure 40** and **Figure 41**) reflecting relations between users' rational, fact-based knowledge, features of the user experience, and the privacy decisions they make in interactions with technology.

Application of the model in empirical analysis uncovered areas of privacy knowledge in need for improvement: *aspects of the user experience* like timeframe, goals, and the basic sense of security; *a low focus on current risks* like social engineering and coupling; a significant lack of understanding of the extensive *sharing with third-parties*, as well as a *weak notion of sensitivity* for misuse of the users' own, personal information in general and expressive information, like preferences, 'likes', and interests, in particular.

Knowledge element	*Description*
Technology skills	This element captures general technology skills and technology experience, the knowledge needed to understand designs, interfaces, functions, the exchange of control between different service providers, as well as the politics (driving forces, thinking, principles, and commercial aspects) important for design of different applications
Assigning responsibilites	This element captures the recognition of personal responsibility for protecting own personal information against misuse once shared and the recognition of the responsibility of other parties like the service provider, third parties, and public authorities for privacy and information security
Knowledge of risks	This element captures the understanding and awareness of threats present in an interaction with technology, the understanding of consequences of exposing information to a given threat, and the ability to weigh these consequences against the advantages of sharing, as well as to the costs involved in protecting against the threat
Understanding exposure	This element captures the general understanding of technology interactions as involving a potential for exposure of personal information, understanding concepts like data persistence and data virality and their practical implications for information exposure, understand the mechanisms for information control provided for the service
Notion of information sensitivity	This element captures the understanding of the three main categories of personal information (self-identifying, access-enabling, and expressive information) and why it is important to restrict others' access to this information, understanding sensitivity in general as well as for own, personal information, is closely related to Knowledge of risks
Managing vulnerability	This element captures knowledge related to the user experience, like the general sense of security and control, the recognition of vulnerability for own, personal information, the choice of information protection strategies, as well as the goals and time perspective related to the exercise of these strategies

Figure 41: A model of privacy literacy: description of knowledge elements

The analysis further found features of the users' experiences of privacy in disharmony with their actual privacy situation on Facebook. To the extent that users' sense of security and invulnerability influences their privacy decisions, this may introduce problems for privacy and their aim to behave cautiously. This situation may explain some lack of rationality observed in privacy decisions.

Some think of privacy problems as related to users' recklessness and negligence. This study found users expressing an explicit desire to behave cautiously online and recognizing a responsibility for protecting their personal information against misuse. Still, entertainment, usefulness, and pleasure are primary purposes for technology use and expectedly weighty factors in the balancing act of privacy decisions. Supportive designs and well-informed education of users are both important associates for users aiming to reach their desired level of privacy.

7.2 Recommendations and further research

Findings supports the trend (Howe, et al., 2012), that users have a relatively low focus on typical security terms. In education, avoiding a too strong focus on these can be advantageous. Additionally, findings suggest educators to communicate information about privacy and security to users by focusing concrete examples of incidents to invite closeness and identification, as well as focusing the actual consequences a threat may impose for user's own information and situation.

Based on this analysis, users are recommended to think of data protection in a long-term as well as a short-term time perspective. They are encouraged to combine a number of different information protection strategies (like self-censorship; familiarize with the privacy settings; maintain settings regularly; use security functions whenever available; employing well-considered password policies; etc.), and to continually update their knowledge of current risks and information vulnerabilities. A strengthened knowledge about the actors and driving forces for commercial infringements of personal information would be advantageous, for youths in particular.

Investigations of the details of the privacy decision process will be needed in the future to confirm the influence of user experiences on actual privacy behavior. A useful track would be to test the influence of a basic sense of security and invulnerability on actual privacy decisions. This theme calls for qualitative research in the first place, and the theoretical perspective of this study is expected to be particularly supportive for this purpose. Making use of this perspective has been informative and inspiring. Further elaboration and testing of the model (or elements of the model) for privacy literacy on a wider, representative sample would be an interesting next step, as well.

Another track is investigating the importance of former experiences (concrete experiences in the past) for privacy decisions. This study has indicated an importance of concrete experiences for behavior (5.4).

And further, the strong focus on identity and contextual integrity observed in analysis, among adults in particular, suggests a closer look into the importance of users' recognition of context in interactions. The importance of identity[91] for social interactions and of context[92] for privacy interactions has been described previously, and the tendency observed to focus a mere subset of the actual audience in sharing decisions (chapter 2 and section 5.4) points to users' recognition of context as an aspect relevant for further studies.

The importance of user experiences for privacy decisions calls for inclusion of experiences in usability considerations for technology design. Approaching design from an experiential perspective requires a widening of the design horizon to include aspects like goals, time, place, emotions, social interaction, and dialectics.

Previous research has shown how Facebook design influenced users' privacy negatively by introducing unexpected changes in their privacy settings (e.g.Stutzman & Kramer-Duffield, 2010). This work identified problems associated with the separation of privacy contexts by Facebook's main architectural building blocks. In order to frame users' privacy experiences adequately, it is recommended that architectural features are made visible in the user interface design to the extent that these affects the mechanisms for information control. And further, accentuating and visualizing aspects of users' privacy situation in design would help directing users' focus to the need for information protection, informing their privacy decisions, and supporting the balancing and trade-offs typically characterizing their privacy situations. After all, privacy will always be subordinated the primary purposes of users' interactions, and expectedly; the more support from design for this secondary process, the more pleasure and usefulness for users in their interactions with technology.

> *I am in there because I find its usefulness higher than its problems, you know…Yes, it is a nice thing, Facebook… absolutely* (#37:A3M)

[91] Erving Goffman: *The Presentation of Self in Everyday Life* (1959)
[92] e.g. Helen Nissenbaum: *Privacy in context: Technology, Policy, and the Integrity of Social Life* (2010)

This page is intentionally left blank.

8. BIBLIOGRAPHY

Acquisti, A., & Gross, R. (2009). Predicting Social Security Numbers from Public Data. *Proceedings of the National Academy of Science, 106*(27), 10975-10980. doi: 10.1073/pnas.0904891106

Acquisti, A., Gross, R., & Stutzman, F. (2011). Faces of Facebook: Privacy in the Age of Augmented Reality / Black Hat 2011 Conference Presentation. *Black Hat Webcast Series* Retrieved April 15, 2013, from http://blackhat.com/docs/webcast/acquisti-face-BH-Webinar-2012-out.pdf

Acquisti, A., & Grossklags, J. (2005). Privacy and Rationality in Individual Decision Making. *IEEE Security and Privacy, 3*(1), 26-33. doi: 10.1109/msp.2005.22

Altman, I. (1975). *The Environment and Social Behaviour: Personal space, Privacy, Crowding, and Territory*. Monterey, CA: Brooks/Cole.

Bannon, L. (1991). From Human Factors to Human Actors: The Role of Psychology and Human-Computer Interaction Studies in Systems Design. In J. Greenbaum & M. Kyng (Eds.), *Design at work: Cooperative Design of Computer Systems* (pp. 25-44). Hillsdale: Lawrence Erlbaum Associates.

Bawden, D. (2008). Origins and concepts of digital literacy. In C. Lankshear & M. Knobel (Eds.), (pp. 17-32).

Berendt, B., Günther, O., & Spiekermann, S. (2005). Privacy in E-commerce: Stated Preferences vs. Actual Behavior. *Commun. ACM, 48*(4), 101-106. doi: 10.1145/1053291.1053295

Bernstein, M. S., Bakshy, E., Burke, M., & Karrer, B. (2013). Quantifying the Invisible Audience in Social Networks. (CHI '13 - to appear) Retrieved April 15, 2013, from http://hci.stanford.edu/publications/2013/invisibleaudience/invisibleaudience.pdf

Besmer, A., & Lipford, H. R. (2010). *Users' (Mis)Conceptions of Social Applications*. Paper presented at the Proceedings of Graphics Interface 2010, Ottawa, Ontario, Canada.

Blythe, M., Overbeeke, K., Monk, A., & Wright, P. (Eds.). (2005). *Funology: From Usability to Enjoyment*. Dordrecht, The Netherlands: Kluwer Academic Publishers.

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2012). Misplaced Confidences: Privacy and the Control Paradox. *Social Psychological and Personality Science, (published online before print August 9, 2012)*. doi: 10.1177/1948550612455931

Brandtzæg, P. B., Lûders, M., & Skjetne, J. H. (2010). Too Many Facebook "Friends"? Content Sharing and Sociability Versus the Need for Privacy in Social Network Sites. *International Journal of Human-Computer Interaction, 26*(11-12), 1006-1030. doi: 10.1080/10447318.2010.516719

Brandtzæg, P. B., & Lüders, M. H. (2009). Privat 2.0: Person- og forbrukervern i den nye medievirkeligheten. Oslo, Norway: SINTEF IKT.

Bryman, A. (2008). *Social Research Methods*. Oxford: Oxford University Press.

Bødker, S. (2006). *When Second Wave HCI Meets Third Wave Challenges*. Paper presented at the 4th Nordic Conference on Human-Computer Interaction: Changing Roles, Oslo, Norway.

Curtis, A. (2013). The Brief History of Social Media. Retrieved May, 23, 2013, from http://www.uncp.edu/home/acurtis/NewMedia/SocialMedia/SocialMediaHistory.html

De Vaus, D. A. (2001). *Research Design in Social Research*. London, UK: Sage.

DeCew, J. W. (1997). *In Pursuit of Privacy. Law, Ethics and the Rise of Technology*. London, UK: Cornell University Press.

Facebook. (2013a). Annual Report. Retrieved March, 4, 2013, from http://investor.fb.com/secfiling.cfm?filingid=1326801-13-3

Facebook. (2013b). Facebook Developers: Documentation Retrieved March 7, 2013, from https://developers.facebook.com/socialdesign/

Finch, J. (1987). The Vignette Technique in Survey Research. *Sociology, 21*(1), 105-114. doi: 10.1177/0038038587021001008

Forlizzi, J., & Battarbee, K. (2004). *Understanding Experience In Interactive Systems*. Paper presented at the 5th conference on Designing Interactive Systems: Processes, Practices, Methods, and Techniques, Cambridge, MA, USA.

Geertz, C. (1973). Thick Description: Toward an Interpretive Theory of Culture. In C. Geertz (Ed.), *The Interpretation of Cultures: Selected Essays*. New York: Basic Books.

Grudin, J. (2001). Desituating Action: Digital Representation of Context *Human-Computer Interaction, 16*(2-4), 269 - 286. doi: 10.1207/S15327051HCI16234_10

Hassenzahl, M. (2013). User Experience and Experience Design. In M. Soegaard & R. F. Dam (Eds.), *The Encyclopedia of Human-Computer Interaction* (2 ed.). Aarhus, Denmark: The Interaction Design Foundation.

Hassenzahl, M., Diefenbach, S., & Göritz, A. (2010). Needs, Affect, and Interactive Products - Facets of User Experience. *Interacting with Computers, 22*(5), 353-362. doi: 10.1016/j.intcom.2010.04.002

Howe, A., E. , Ray, I., Roberts, M., Urbanska, M., & Byrne, Z. (2012). *The Psychology of Security for the Home Computer User*. Paper presented at the 2012 IEEE Symposium on Security and Privacy, San Francisco, CA, USA.

Iachello, G., & Hong, J. (2007). End-User Privacy in Human-Computer Interaction. *Foundations and Trends in Human–Computer Interaction, 1*(1), 1-137. doi: 10.1561/1100000004

Johnson, M., Egelman, S., & Bellovin, S. M. (2012). *Facebook and Privacy: It's Complicated*. Paper presented at the SOUPS '12 Symposium on Usable Privacy and Security, Washington, D.C., USA.

Kaptein, M. C., Nass, C., & Markopoulos, P. (2010). *Powerful and Consistent Analysis of Likert-Type Rating Scales*. Paper presented at the CHI '10 ACM SIGCHI Conference on Human Factors in Computing Systems, Atlanta, Georgia, USA.

King, J., Lampinen, A., & Smolen, A. (2011). *Privacy: Is There an App For That?* Paper presented at the SOUPS '11 Symposium on Usable Privacy and Security, Pittsburgh, PA, USA.

Kosinski, M., Stilswell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Science of the United States of America, 110*(15), 5733-5734. doi: 10.1073/iti1513110

Kvale, S. (2001). *Det kvalitative forskningsintervju*. Oslo, Norway: Gyldendal.

Lampinen, A., Stutzman, F., & Bylund, M. (2011). *Privacy for a Networked World: Bridging Theory and Design*. Paper presented at the CHI '11 Extended Abstracts on Human Factors in Computing Systems, Vancouver, BC, Canada.

Löwgren, J. (2013). Interaction Design - Brief intro. In M. Soegaard & R. F. Dam (Eds.), *The Encyclopedia of Human-Computer Interaction* (2 ed.). Aarhus, Denmark: The Interaction Design Foundation.

Malterud, K. (2002). Kvalitative metoder i medisinsk forskning - forutsetninger, muligheter og begrensninger. *Tidsskrift for Den norske legeforening, 122*(25), 2468-2472.

Malterud, K. (2003). *Kvalitative metoder i medisinsk forskning: En innføring*. Oslo, Norway: Universitetsforlaget.

Margulis, S. T. (2003). On the Status and Contribution of Westin's and Altman's Theories of Privacy. *Journal of Social Issues, 59*(2), 411-429. doi: 10.1111/1540-4560.00071

Mathiasen, N. R., & Bødker, S. (2008). *Threats or Threads -from Usable Security to Secure Experience?* Paper presented at the Nordic Conference of Human-Computer Interaction (NordiCHI '08), Lund, Sweden.

McCarthy, J., & Wright, P. (2004). Technology as Experience. *Interactions, 11*(5), 42-43. doi: 10.1145/1015530.1015549

McCarthy, J., & Wright, P. (2004). *Technology as Experience*. Massachusetts, USA: MIT Press.

NESH. (2006). Forskningsetiske retningslinjer for samfunnsvitenskap, humaniora, juss og teologi. Retrieved from http://www.etikkom.no/retningslinjer/NESHretningslinjer/06

Nielsen. (2012). State of The Media: The Social Media Report 2012. Retrieved May, 23, 2013, from http://www.nielsen.com/us/en/reports/2012/state-of-the-media-the-social-media-report-2012.html

Norman, D. A. (2004). *Emotional Design. Why we love (or hate) everyday things*. New York, NY, USA: Basic Books.

Norwegian Committees for Research Ethics. (2011). About qualitative methods. Retrieved March 24, 2011, from http://www.etikkom.no/no/Forskningsetikk/Etiske-retningslinjer/Medisin-og-helse/Kvalitativ-forskning/1-Kvalitative-og-kvantitative-forskningsmetoder--likheter-og-forskjeller/

NSD. (2011). The Privacy Ombudsman for Research. Retrieved February 13, 2011, from http://www.nsd.uib.no/nsd/english/pvo.html

NSM. (2010). Nasjonal Sikkerhetsmyndighet: Rapport om sikkerhetstilstanden 2010 (ugradert versjon) Retrieved November, 4, 2011, from https://www.nsm.stat.no/Documents/Risikovurdering/Ugradert%20rapport%20om%20sikkerhetstilstanden%202010%20.pdf

NSM. (2011). Nasjonal Sikkerhetsmyndighet: Rapport om sikkerhetstilstanden 2011 (ugradert versjon) Retrieved February, 7, 2012, from https://www.nsm.stat.no/Documents/Risikovurdering/Ugradert%20Rapport%20om%20sikkerhetstilstanden%202011.pdf

Palen, L., & Dourish, P. (2003). *Unpacking "Privacy" for a Networked World.* Paper presented at the CHI '03 ACM SIGCHI Conference on Human Factors in Computing Systems, Ft.Lauderdale, Florida, USA.

Personvernkommisjonen. (2009). Individ og integritet. Personvern i det digitale samfunnet. (Norges offentlige utredninger [NOU] 2009:1). Kap 4.1: Nærmere om begrepet personvern Retrieved April 11, 2013, from http://www.regjeringen.no/nb/dep/fad/dok/nouer/2009/nou-2009-1/5.html?id=542073

Privacy International. (2007). A race to the bottom: Privacy rankings of Internet service companies. Retrieved February 23, 2012, from https://www.privacyinternational.org/reports/a-race-to-the-bottom-privacy-rankings-of-internet-service-companies

Qual. Research Guidelines Project. (2011). Sampling. Retrieved March 28, 2011, from http://www.qualres.org/HomeSamp-3702.html

Rachels, J. (1997). Why Privacy Is Important. In J. Rachels (Ed.), *Can Ethics Provide Answers And Other Essays in Moral Philosophy* (pp. 145-153). Lanham, MD, USA: Rowman & Littlefield Publishers Inc.

Rotman, D. (2009). *Are You Looking At Me? Social Media and Privacy Literacy*. Paper presented at the iConference '09, Chapel Hill, NC, USA.

Schartum, D. W., & Bygrave, L. A. (2011). *Personvern i informasjonssamfunnet: en innføring i vern av personopplysninger*. Bergen: Fagbokforl.

Sharp, H., Rogers, Y., & Preece, J. (2007). *Interaction Design: Beyond Human-Computer Interaction (2nd Edition)*. Chichester, England: John Wiley & Sons.

Solove, D. J. (2008). *Understanding Privacy*. Cambridge, MA, USA: Harvard University Press.

Steel, E., & Fowler, G. A. (2010). Facebook in Privacy Breach: Top-Ranked Applications Transmit Personal IDs, a Journal Investigation Finds. Retrieved June 12, 2011, from http://online.wsj.com/article/SB10001424052702304772804575558484075236968.html

Stutzman, F., & Kramer-Duffield, J. (2010). *Friends Only - Examining A Privacy-Enhancing Behavior In Facebook*. Paper presented at the CHI '10 ACM SIGCHI Conference on Human Factors in Computing Systems, Atlanta, Georgia, USA.

Synlighet. (2012). Faktahefte om Facebook Retrieved February 4th, 2013, from http://www.synlighet.no/facebook/statistikk-antall-brukere/

The Norwegian Data Inspectorate. (2013). Personvern 2013: Tilstand og trender. Report from The Norwegian Data Inspectorate and The Norwegian Board of Technology. (Report 1/2013). Retrieved from http://datatilsynet.no/Global/04_veiledere/personvernrapport_tilstand_trender2013.pdf

Walsham, G. (1995). Interpretive Case Studies in IS Research: Nature And Method. *European Journal of Information Systems, 4*(2), 74-81.

Walsham, G. (2006). Doing interpretive research. *European Journal of Information Systems, 15*, 320-330.

Wang, N. (2012). *Third-Party Applications' Data Practices on Facebook*. Paper presented at the CHI '12 Extended Abstracts on Human Factors in Computing Systems, Austin, Texas, USA.

Wang, N., Xu, H., & Grossklags, J. (2011). *Third-Party Apps on Facebook: Privacy and the Illusion of Control*. Paper presented at the ACM Symposium on Computer Human Interaction for Management of Information Technology, Boston, MA, USA.

Wright, P., McCarthy, J., & Meekison, L. (2005). Making Sense of Experience. In M. Blythe, K. Overbeeke, A. Monk & P. Wright (Eds.), *Funology* (Vol. 3, pp. 43-53): Springer Netherlands.

Appendix A: Notes to development of Interview Guide v3.0

Planleggingsfasen:

Hva er det jeg ønsker å få vite noe om?

Hvorfor deler vi store mengder personlig informasjon i sosiale medier til tross for at vi uttrykker bekymring med hensyn til konsekvensene av å dele?

Er det forskjell på unge og eldres opplevelser og beslutninger relatert til privacy på Facebook?

Hovedfokus: Privacy Literacy (inkl. både kunnskap og læring):

Skille mellom ferdighetsaspekter (kompetanse) og læringsaspekter (dannelse):

- Å bruke digitale verktøy er en ferdighet den enkelte må tilegne seg, vedlikeholde og kontinuerlig utvikle, for å bli en digitalt kompetent og kritisk innbygger. Evne til kildekritikk og vurdering av innhold er del av digital kompetanse (eNorge, i Egeberg et al.)
- Vi vet lite om kunnskapens betydning for våre faktiske valg. Blir den omsatt til refleksjon og etisk kompetanse, slik at vi forstår hva vi gjør i den enkelte delingssituasjon?
- *Kunnskap som gjenspeiles i innsikt, erfaring og opplevelser, som påvirker vår tenkemåte og oppfatning av verden* . Almenngyldige kunnskaper som har mulighet for å skape strukturer og prinsipper som har overføringsverdi (Klafki)

Antakelse 1: ***Facebookbrukere med gode kunnskaper om digital informasjon, ansvarsforhold, farer på internett og generell teknologikunnskap, beskytter sin personlige informasjon bedre enn brukere som har mindre gode kunnskaper.***

Antakelse 2: ***Facebookbrukere som har erfaring med uønsket deling av personlig informasjon, beskytter informasjonen sin bedre enn brukere som ikke har slike erfaringer.***

Antakelse 3: ***Facebookbrukere som både har kunnskaper og erfaring beskytter informasjonen sin bedre enn de to førstnevnte gruppene.***

Antakelse 4: ***Unge Facebookbrukere har bedre kunnskap og mer erfaring med uønskete hendelser, og beskytter sin personlige informasjon bedre enn eldre brukere.***

For å ta stilling til disse påstandene må jeg vite noe om:

- brukerens kunnskap om teknologi, informasjon, ansvarsforhold og farer på internett
  - må ha deltakere med ulikt kunnskapsnivå
- brukerens grad av erfaring med negative hendelser som følge av uønsket deling av personlig informasjon på nettet
  - må ha deltakere med ulik grad av erfaring med uønsket deling
- hvor godt brukeren beskytter sin personlige informasjon i sosiale medier
  - vurder om dette er godt nok dekket i intervjuguiden
- brukerens alder

Hvorfor ønsker jeg å studere dette?

Det viktigste formålet med studien er å utforske avviket mellom holdninger og atferd i forbindelse med deling av informasjon i sosiale medier

- bidra til å forklare avviket, med fokus på subjektive komponenter og user experience
- bidra til økt kunnskap om kompetansebyggingsbehov med tanke på tryggere atferd på nett (hva og hvordan)

Forslag til tema i intervjuguiden:

Tema 1: ***Bakgrunnsinformasjon om deltakerens Facebookbruk***

Tema 2: ***Ferdighetsaspektet: Kunnskap & kompetanse***

1. Kunnskap om farer (privacy og security – ikke klar grense mellom disse)
   - deler fordi vi ikke har kunnskap om farer
2. Teknologiforståelse
   - deler fordi vi ikke forstår
     - hvordan personvernmekanismene fungerer (usability)
     - hvordan pc & internett generelt fungerer
     - hvem som har/tar ansvaret for å ivareta vårt personvern
3. Informasjonsforståelse
   - deler fordi vi ikke forstår viralitet og bestandighet
   - deler fordi vi ikke forstår ulike typer av informasjon

Tema 3: ***Dannelsesaspektet: Subjektiv opplevelse, refleksjon, motivasjon***

1. Nærhet til farer /subjektiv opplevelse av farer (user experience)
   - erfaringer, forventninger, følelser, holdninger, verdier, time/place (nåtid, fortid, fremtid)…
   - bekymring: er vi bekymret? i hvilken grad? for hva? når er vi spesielt bekymret? hva gjør vi for å redusere bekymringen? deler vi likevel?
   -'det hender ikke meg'?
2. Motivasjon for å forstå privacy og for å lære om privacy

Tema 4: ***Dannelsesaspektet: Atferd / holdninger i konkrete situasjoner***

1. Holdninger til konkrete situasjoner (scenarier, eksempler)

Appendix B: Invitation to participants v2.1

Invitasjon til deltakelse i forskningsprosjekt

Hei!

Jeg er masterstudent i Informasjonsvitenskap ved Universitetet i Bergen. I forbindelse med min mastergrad gjennomfører jeg en undersøkelse av bruk av sosiale medier hvor jeg ser nærmere på hvordan norske brukere opplever sitt personvern på Facebook. Veileder for studien er professor Victor Kaptelinin ved Institutt for Informasjons- og Medievitenskap, Universitetet i Bergen.

Bruk av sosiale medier har økt kraftig de siste årene. Den største aktøren, Facebook, har i dag ca 800 mill. brukere på verdensbasis. Tidligere undersøkelser har vist at mange Facebookbrukere er bekymret for sitt personvern, og formålet med undersøkelsen er å bidra til en nærmere forståelse av hvordan alder, kunnskap og erfaring påvirker menneskers opplevelse av og holdninger til personvern. Innsikt i brukernes situasjon og ønsker kan bidra til bedre forståelse for hvordan programvare for sosiale medier kan utvikles for å ivareta brukernes ønsker på en god måte. Den kan også komme brukerne selv til gode ved å bidra til å gjøre den enkelte mer bevisst sitt eget privatliv på nett og hva som skal til for å beskytte egen informasjon. Den kan videre være nyttig for de myndigheter som har ansvar for å regulere aktiviteten til aktører innen området, og for å utvikle tiltak for kompetanseheving for brukere av sosiale medier.

Jeg ønsker i forbindelse med studien å komme i kontakt med aktive Facebookbrukere fra aldersgruppene 16-20 år og over 45 år som kunne tenke seg å delta. Deltakerne må være aktive Facebookbrukere, ha over 150 kontakter i sin venneliste, og vanligvis logge inn på Facebook minst 5 ganger pr. uke.

Datainnsamling blir gjennomført ved at deltakerne inviteres til å være med i et intervju av ca 1 times varighet. Det er ønskelig å gjøre lydopptak fra intervjuet. Deltakerens navn, alder og annen direkte identifiserende informasjon vil ikke bli lagret elektronisk, og den enkelte deltaker bestemmer selv hvilke opplysninger han/hun vil dele i intervjuet. All informasjon blir behandlet konfidensielt, og enkeltpersoner vil ikke kunne gjenkjennes i resultatene fra prosjektet. Data fra opptakene vil bli lagret trygt, og intervjuene blir gjennomført med godkjenning fra Personvernombudet for forskning: Norsk Samfunnsvitenskapelig Datatjeneste A/S. Lydopptakene slettes og øvrig materiale anonymiseres når prosjektet er endelig avsluttet, senest innen 30.04.2013. Det er frivillig å delta i prosjektet og om du skulle velge og trekke deg underveis, kan du kreve opplysningene som er gitt slettet, uten å måtte begrunne dette nærmere.

Intervjuer vil bli gjennomført fra ca. 15. november 2011. Hvis du kunne tenke deg å delta, er det fint om du returnerer skjemaet på neste side til meg, enten på e-post eller i vanlig post (eventuelle utlegg til porto vil bli refundert). Jeg vil ta kontakt med deg for nærmere avtale når jeg har mottatt skjemaet. Hvis du har spørsmål om undersøkelsen før du sender inn skjemaet, ta gjerne kontakt. Kontaktopplysninger finner du nederst på neste side.

Deltakerne i studien vil få en liten påskjønnelse i form av en gavebillett på kino som takk for innsatsen. For den som er interessert, vil resultatene fra undersøkelsen bli gjort tilgjengelig elektronisk.

På forhånd takk for hjelpen!

Med vennlig hilsen Heidi Molvik Rundhovde

Appendix B: Invitation to participants v2.1

Jeg har lest invitasjonsbrevet om studien av personvern i sosiale medier, og jeg sier ja til å delta i studien.

Navn (bruk blokkbokstaver): ..... Alder .....

Telefonnr: ..... E-post: .....

Sted/dato: ..... Deltakers signatur: .....

Kontaktopplysninger:

Heidi Molvik Rundhovde
[redacted]

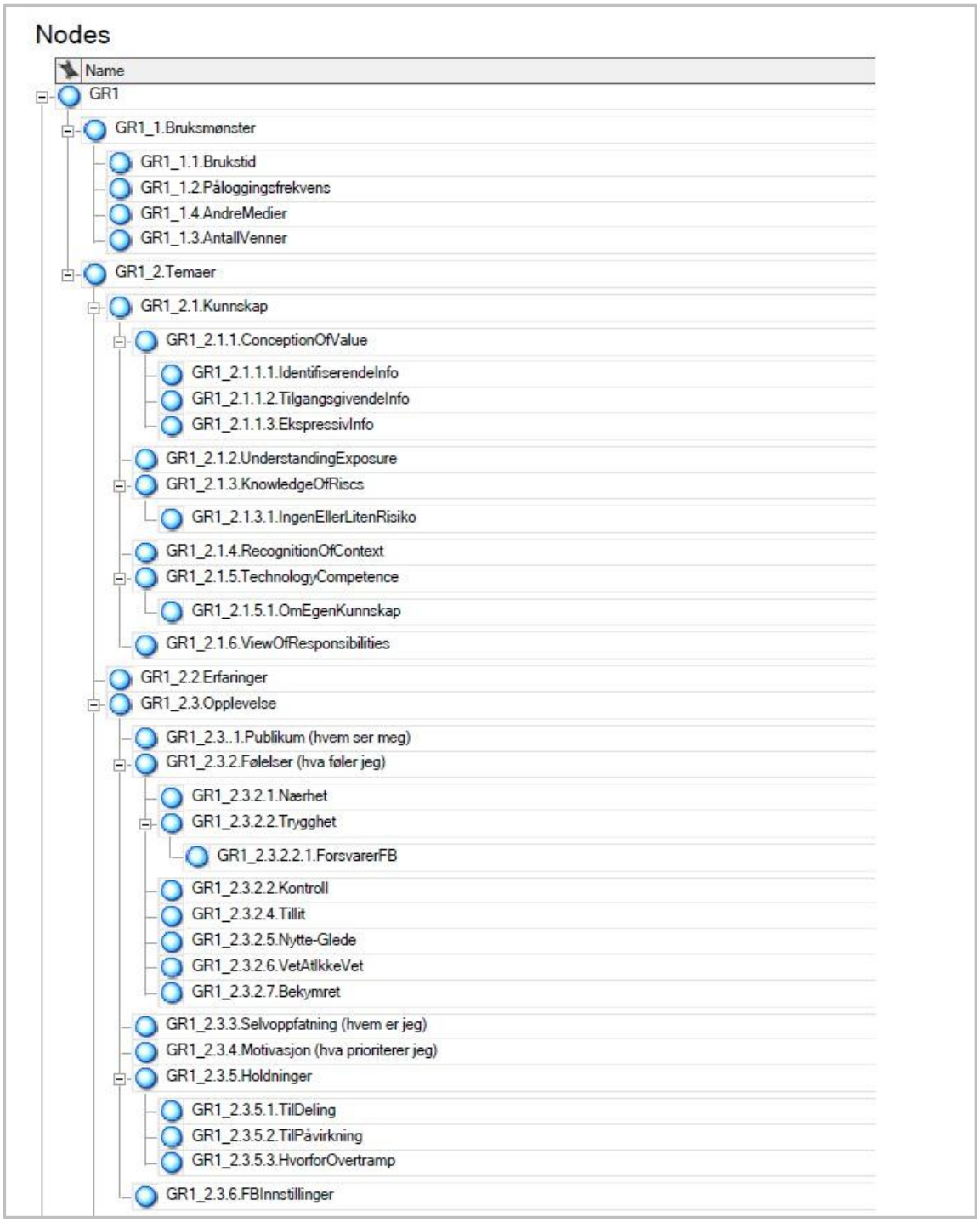
Mobil:
[redacted]

E-post: [redacted]

Veileder: Professor Victor Kaptelinin
Institutt for Informasjons- og Medievitenskap
Universitetet i Bergen

E-post: [redacted]

Appendix C: Example of NVivo data structure



continues next page…

Appendix C: Example of NVivo data structure