Master Thesis in Informatics

A Qualitative Inquiry into Online Privacy and Information Sharing Concerns of Internet Users

Author: Seyedeh Elssa Mojarad Vishkaie
Supervisor: Miranda Kajtazi
Examiner: Jamie Campus and Paivi Jokela
Teacher: Sisse Finken
Date: 2016.23.04
Course Code: 4IK00E, 15 credits
Subject: Degree project at Master Level
Abstract

Information privacy concerns are one of the major causes behind a dramatic decline in the readiness of individuals to share their personal information on the Internet. The aim of this research is to explore the information privacy concerns from the users’ perspective. In the focal point of this qualitative study stands the kryast.se website. The healthcare promotion activities that this website carries out involve the sharing by its users of their personal information on the Internet. For this reason, this study takes recourse to the construct of Internet Users’ Information Privacy Concerns (IUIPC) developed by Malhotra, Kim and Agarwal (2004) as its interpretive framework. It was expected that by using both semi-structured interviews and non-participant observation among the users of the above mentioned website, the concerns of its users can be identified through the interpretative lens of the analytical framework that Malhotra et al. (2004) proposed for privacy concerns of Internet Users. The results of this study indicate that the selected conceptual lens has sufficiently accounted for the concerns that website users may have when sharing their personal information on the Internet, while indicating that internet users tend to be reluctant in sharing their sensitive information.

Keywords: Information sharing, privacy concerns, Internet users privacy concerns.
Acknowledgements

Every dissertation has a journey along with it. It has been a great, challenging, and full of learning experience for me. Along this journey, I was privileged to have supports of many people helping me to finish this academic chapter of my life.

I would like to take this opportunity and thank my compassionate supervisor, Miranda Kajtazi. I am extremely grateful of having her ever-lasting support. I perceive myself a lucky person not only to have her supervision but also to get to know her as a person and spiritual mentor. Miranda has held my hands and encouraged me along the way and shed light to every aspects of this master thesis. I would have never managed to finish my thesis without having her instrumental encouraging comments. I wish to express my sincere thanks to the department of informatics in Linnaeus University, who has been giving me the opportunity to develop my ideas and bring them to fruition by conducting this thesis. Sincere appreciations to Paivi Jokela, Sisse Finken and Jamie Campos for giving me the opportunity to be part of this academicals program and providing me a more professional academicals perspective on my thesis. Furthermore I would like to thank my classmates for their helpful, productive comments which assisted me a lot to make my thesis contribution more valuable.

I would also like to share my gratitude to Gustaf, the owner of the Kryast.se webpage, who believed in me and helped me to conduct this study, introduced me to many wonderful people along this academicals journey.

I am immensely grateful of my beloved parents, Azar and Javad who have always been my inspirations in life. Thanks for encouraging me to follow what my heart says and for your unconditional love.

At the end I would like to thank my dearest friend, my adorable husband, Nersi. I am so grateful to have you in my life, life with you has formed a different meaning for me.
# Table of Contents

1 Introduction.................................................................................................................. 1
1.1 The Area of Investigation............................................................................................ 1
1.2 Research Objective....................................................................................................... 4
1.3 Research Questions ..................................................................................................... 6
1.4 Scope and Limitations ................................................................................................. 6
1.5 Thesis Overview ......................................................................................................... 7
2 Literature Review .......................................................................................................... 9
2.1 The Framework of Internet Users’ Information Privacy Concerns ............................... 9
2.2 The Theory of Internet Users’ Information Privacy Concerns ..................................... 11
2.2.1 The Dimension of Collection ............................................................................... 12
2.2.2 The Dimension of Control ................................................................................... 12
2.2.3 The Dimension of Awareness .............................................................................. 13
2.3 The Role of Internet Users’ Information Privacy Concerns Theory in this Study ........ 14
2.4 Previous Studies Using the Framework of Internet Users’ Information Privacy Concerns .... 15
2.4.1 An Overview of Theoretical Frameworks of Information Privacy Concerns ........ 17
3 Research Methodology .................................................................................................. 19
3.1 Philosophical worldview............................................................................................. 20
3.2 Research Design......................................................................................................... 21
3.3 Data Collection Methods .......................................................................................... 22
3.4 Interview Questions .................................................................................................. 23
3.5 Data Analysis ............................................................................................................ 25
3.6 The Description of the Research Setting ..................................................................... 26
3.6.1 Information Sharing by Internet Users at a Health Promotion Webpage ................ 27
3.6.2 The socio-demographic profile of research participants ........................................ 28
3.7 Validity and Reliability .............................................................................................. 29
3.8 Ethical Consideration ................................................................................................. 30
4 Empirical Findings ......................................................................................................... 32
4.1 The Impact of Risk Awareness on Privacy Concerns in Online Environments ......... 34
4.2 The Impact of Personal Contact on Privacy Concerns ............................................. 36
4.3 The Impact of Control on Privacy Concerns and Information Sharing ..................... 37
4.4 The perceived versus actual Privacy Concerns ......................................................... 38
List of Figures

Figure 1 - The Connection between IUIPC and its components- adapted from Malhotra et al. (2004, p. 341) .................. 14
Figure 2 - Asking Experts on kryast.se (Translated from Swedish to English by Google Translator) .......................... 27

List of Tables

Table 1 - Comparison between GIIPC, CFIP and IUIPC (Inspired by Malhotra et al., 2004, p.340) .............................. 10
Table 2- Template of interview questions .................................................................................................................. 24
Table 3 - The socio-demographic profile of research participants .............................................................................. 28
1 Introduction

You have zero privacy, get over it anyway! (Scott McNeally, the chief executive officer of Sun Microsystems)

How confident should one feel about sharing personal information on websites that can be accessed by millions of people from around the world? According to media reports, the personal information of 33.6 million Americans has been manipulated for fraudulent purposes since 1990 (Son and Kim, 2008, pp.503-504). Thus, it can be reasonably assumed that website users’ information privacy concerns represent one of the obstacles for their willingness to disclose personal information to companies and corporations over the Internet (Son and Kim, 2008, p.504). The lack of confidence in information privacy has been identified as one of the major concerns of Internet users by numerous researchers from different fields of study, such as law and ethics (Caudill and Murphy, 2000), marketing (Dinev et al., 2006), Information System (Smith et al., 1996), and multiple other fields. As early as the 1980s, Mason (1986) proposed that with the increasing speed of information transmission and with the growing sophistication of information technology, individuals will be confronted with numerous challenging issues related to information privacy, accuracy, ownership and accessibility. Mason’s (1986) expectations have been proven to be true by subsequent developments in each of these areas. Especially with respect to information privacy, there have been ongoing scholarly and public debates in recent decades (Bélanger and Crossler, 2011). According to multiple surveys carried out among Internet users around the world, Internet users from different age groups are becoming increasingly aware of the digital footprint that their online activities leave (Youn, 2009, pp.391-392). The survey that was conducted within the framework of Pew Internet and American Life Project has shown that 85% of adult respondents that took part in this survey had significant concerns about their privacy and its possible breach (Madden et al., 2007, p.2). Moreover, in the early 2000s a report prepared by the University of California–Los Angeles Centre for Communication Policy has indicated that 94.5% of American consumers, including both Internet-users and non-Internet users, have concerns about the privacy of their personal information and its security while performing Internet purchases (Malhotra et al., 2004, p.336). This lack of trust may lead individuals to a situation of not trusting online services and websites that they use over the Internet anymore, which can lead to the loss of customers by online businesses (Oberholzer and Oliver, 2005). Perhaps the most important concern for Internet users is that their personal information can be accessed, exchanged and manipulated without their authorization. Therefore, it is highly important that the personal information of Internet users be handled with respect to their privacy. In order to indicate how the privacy for internet users can be defended and the security of their personal information can be improved, it is critical to grasp the concerns of online consumers in relation to their information privacy.

1.1 The Area of Investigation

Malhotra et al. (2004) have indicated that previous studies focused on specific aspects of information privacy within the context of addressing the concerns that Internet users may have about the safety of their personal information (Phelps et al., 2000). Other studies, such as the
research report commissioned by the Federal Trade Commission of the United States, have evaluated the privacy concerns of consumers in relation to online environments while using the theoretical framework of organization studies (Sheehan and Hoy, 2000). However, there have been a few studies that address “the interactive two-way communication and its related privacy threats” (Malhotra et al., 2004, p.337). Thus, privacy concerns can become a hurdle for successful two-way communication between marketers and customers in online environments. As Richards (1997, p.319) indicates, “no other medium has been a catalyst of such a wide range of criticism regarding privacy invasion” than the Internet. Phelps et al. (2000) noted that much of the recent studies have focused on “documenting the general levels of consumer privacy” without making specific inquiries into the privacy concerns of online consumers using their qualitative description. Given that the predominant body of research into these privacy concerns that Internet use raises, it is important to grasp these concerns from a qualitative perspective since there is a lack of more comprehensive studies into the concerns, beliefs, and perceptions that consumers have about online environments and their risks (Phelps et al., 2000, p.40). The need for a qualitative inquiry into privacy concerns stems from previous studies on information privacy being performed within the quantitative paradigm of information System (Bélanger and Crossler, 2011). These information privacy studies are aimed at identifying the various quantifiable aspects of privacy concerns in order to measure the impact of privacy concerns on different dependant variables, such as the willingness to provide personal information online or make transactions over the Internet (Bélanger and Crossler, 2011).

Since this study concentrates upon the customers and support personnel of the website kryast.se in order to gain an understanding of the privacy concerns of Internet users, it is important to elaborate about the notion of information privacy and the concerns that Internet users have in this regard. Additionally, it is worth indicating that in recent years empirical research into the privacy concerns of Internet users has been predominantly quantitative, even though these concerns are individual-level constructs (Hoadley et al., 2010). For this reason, qualitative inquiries into privacy concerns of Internet users are a nascent and important perspective into this topic (Miltgen and Peyrat-Guillard, 2014), especially with regard to identifying additional factors that are likely to affect privacy concerns (Zukowski and Brown, 2007, p.203). At the same time, as the study of Miltgen and Peyrat-Guillard (2014) illustrates, previous research from this perspective into privacy concerns predominantly concentrates on the behavioural, attitudinal and country-specific implications of privacy concerns. This creates a gap between theoretical literature on privacy concerns and empirical studies on their outcomes and antecedents that calls for its interpretative exploration (Smith et al, 2011).

**Information privacy** refers to “the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others” (Westin, 1967, p. 7). Stone et al. (1983, p.2) have referred to information privacy as an individual’s ability to control personal information about oneself. Previous studies have provided support for the conjecture that, in real life, information privacy is divergently influenced by different factors, such as government regulation (Yang and Miao, 2008), industry, technological solutions (Culnan and Bies, 2003), national laws (Milberg et al., 2000), international human rights legislation (Malhotra et al., 2004), and cultural values (Milberg et al., 1995). Thus, the concept of information privacy has multiple facets and indicators.
Information privacy concerns refers to an individual subjective perception of security concerns within the context of information privacy (Campbell 1997 in Malhotra et al., 2004). Information privacy concerns can be influenced by the factors mentioned above (e.g. cultural attitudes, international regulation, national laws, etc.). Furthermore, information privacy concerns “stem from a variety of factors, including an individual’s previous experiences, cultural milieu, and physiological reactivity” (Stone and Stone, 1990, p.386).

For this reason, companies may try to mitigate information privacy concerns of their Internet clients by developing and emphasizing privacy policies concerning the use that they make of the personal information they collect (Hann et al., 2007, p. 13). Given that privacy infringements frequently involve the collection, transmission, storage and manipulation of personal information by organizations, individuals may need to be informed about the implications of such activities for their privacy, even though their personal details may be submitted to corresponding websites voluntarily. Additionally, individual perceptions of what constitutes privacy violation are likely to exhibit significant variation, according to the objective of information disclosure and the purpose of online activity (Dinev et al., 2013, p. 295). Correspondingly, explicit privacy policies, economic incentives or website customization may lower the level of perceived privacy violations (Hann et al., 2007, p. 14). These measures are likely to increase individual willingness to use websites that solicit personal information, despite the risks that might involve (Phelps et al., 2000, p. 27).

There have been numerous studies in information systems literature that evaluate the privacy concerns of individual consumers. Most of this body of academic research has used the following two theoretical frameworks Concerns For Information Privacy (CFIP), and Internet Users’ Information Privacy Concerns (IUIPC) (Bélanger and Crossler, 2011).

The framework of Concern For Information Privacy has been the first theoretical framework for accounting for privacy concerns that have gained wide researcher currency (Smith et al., 2011). On the basis of extensive research of Smith et al. (1996), an empirical quantitative methodology for capturing the privacy concerns of individuals in online environments has been developed. Their methodology has led Smith et al. (1996) to build a multidimensional scale called Concern For Information Privacy. This scale has been extensively used in subsequent research in order to identify individual concerns about organizational information privacy practices (Malhotra et al., 2004). The Concern For Information Privacy scale consists of four dimensions of information privacy concerns. These dimensions are collection, unauthorized secondary use, improper access, and errors. Smith et al. (1996) and other researchers have initially applied these four dimensions of the Concern For Information Privacy scale in the context of offline direct marketing. A few years thereafter, Malhotra et al. (2004) have developed the construct of Internet Users’ Information Privacy Concerns. According to the proposition of Malhotra et al. (2004), this construct consists of three main dimensions of control, awareness, and collection. Malhotra et al. (2004) have developed the framework that specified the dimensions of Internet Users’ Information Privacy Concerns as a scalar variable. Their research results have provided support for the proposition that “IUIPC explains more of the variance in a person's willingness to transact than CFIP” (Malhotra et al, 2004, P.349).

In an attempt to review the information privacy research in the information System domain, Bélanger and Crossler (2011, p.1020) have noted that the theoretical framework of Internet Users’ Information Privacy Concerns has not been used widely by information systems
researchers. According to Bélanger and Crossler (2011, p.1020), the majority of research regarding privacy concerns has tended to utilize the first theoretical framework of Concern For Information Privacy. This tendency derives from the difficulty of empirically measuring privacy as a variable. Moreover, privacy concerns are likely to be more influenced by subjective perceptions and cognitions than by rational evaluations of the risks that Internet use involves, which has led to the conceptualization of privacy concerns in terms of individual attitudes toward privacy practices (Stewart and Segars, 2002). Whereas Malhotra et al. (2004) have adapted the concept of Concern For Information Privacy for the Internet context in the process of developing their multidimensional scale of Internet Users’ Information Privacy Concerns, privacy concerns have been predominantly conceptualized as an individual-level, dependent variable without paying sufficient attention to society- or culture-related independent variables (Smith et al., 2011, pp.997-998). Additionally, previous research into privacy concerns has not arrived yet at robust, replicable findings with respect to both their antecedents and their outcomes. Other studies have suggested that privacy concerns can also be driven by personal characteristics, such as age, and institutional factors, which could enable individuals to make assessments of the possible consequences that information disclosure on the Internet might have (Xu et al., 2008).

However, there still exists a lack of theoretical understanding of the differences that these antecedent factors introduce in the privacy concerns that individuals might have, which has implications for privacy protection and research practice (Li, 2011).

Additionally, most extant research on privacy concerns has almost exclusively concentrated on the United States (Bélanger and Crossler, 2011). Rather than making comparisons between the United States and other countries, it is necessary to focus on privacy concerns, while concentrating upon privacy issues that concern Internet users from countries where cultural, social and demographic factors are likely to impact privacy concerns differently than in the United States (Smith et al., 2011, p.1007). Moreover, Bélanger and Crossler (2011, p.1020) have called for more research evaluating privacy concerns using the Internet Users’ Information Privacy Concerns instrument and to develop its dimensions. Therefore, I will use Internet Users’ Information Privacy Concerns as my theoretical lens in order to consider the privacy concerns of customers in an online website. Furthermore, my analysis will reflect on modification of the so-called model in its blossoming stage to fulfil the cited gap. The dimensions of Internet Users’ Information Privacy Concerns will be explained in the theoretical framework section broadly.

Following in this chapter, the objective of this study, the research question, and the delimitations of this study will be explained.

1.2 Research Objective

The main objective of this study is to understand the privacy concerns of Internet users in relation to situations where they share their information in online environments, such as consumer websites. This research, thus, intends to inquire into the privacy concerns that Internet users may have from a qualitative perspective. Since online users who share their private information over the Internet may be unaware of the threats to their privacy, the aim of this study also include is to find which factors may promote the sensitization of Internet users to possible
violations of their privacy. In order to address this aim, several motivations are presented below, which form the purpose of this study.

Firstly, this study intends to identify the privacy concerns of Internet users’ who share their information on a healthcare promotion website by tackling their information concerns within a quantitatively validated interpretive framework. This objective is likely to make a practical contribution to understanding the manner in which Internet users decide to share their information on websites. The concept of Internet Users’ Privacy Concerns represents the theoretical lens through which the aim of the study will be reached. Thus, this study aims to adapt the framework of Internet Users’ Information Privacy Concerns that were primarily used in quantitative research for the purpose of its application in qualitative studies. These studies address issues related to information systems.

Secondly, this study intends to ascertain if of this theoretical framework can be made interpretive use to identify the privacy concerns of Internet users. In doing so, the theoretical framework of Internet Users’ Privacy Concerns, in general and with respect to its main dimensions, will be approached from the perspective of the qualitative data that this research shall collect. Therefore, the objective of this study is to make a qualitative interpretation of the theoretical framework of Internet Users’ Privacy Concerns. The process of data collection for this research will be focused upon analysing the transcripts of interviews to be conducted with selected online users of the website kryast.se, while also concentrating on the different aspects of their privacy concerns which sharing their personal information on the Internet may involve.

Thirdly, this study intends to contribute to a qualitative interpretation of this theoretical framework in two different ways. This research will adapt the theoretical framework of Internet Users’ Privacy Concerns while seeking to make a practical contribution to the field of information system studies, with respect to the qualitative assessment of the privacy concerns that online environments are likely to raise. By utilising the conceptual framework of Internet Users’ Information Privacy Concerns, this study is likely to contribute to the adaption of this conceptual framework in qualitative research settings that deal with privacy concerns.

Furthermore, given that existing studies have mostly used the concept of Internet Users’ Information Privacy Concerns as a tool for quantitative empirical research, rather than a theoretical construct in its own right, the objective of this study is to investigate if the conceptual framework of the Internet Users’ Information Privacy Concerns can be used interpretively with regard to qualitative data reflecting the privacy concerns of the users of the website kryast.se. Therefore, this study intends to contribute to scholarly literature by utilising the theoretical framework chosen for this study, which is the Internet Users’ Privacy Concerns and explore if its different theoretical dimensions can aid the analysis of users’ privacy concerns.

To summarize, this study is deemed necessary since previous studies in the field of Information Systems have paid less attention to the qualitative aspects of information privacy concerns (Cresswell and Sheikh, 2013, p. 73). The majority of studies on this subject continue to use quantitative survey methodologies that group their research subjects into categories according to their privacy attitudes, rather than providing a qualitative, interpretive perspective on different aspects of privacy concerns (Budak et al., 2013, p. 100). Thus, this study may fill this gap by using
the conceptual framework of Internet Users’ Privacy Concerns for the analysis of qualitative data while providing a qualitative interpretation of this framework.

1.3 Research Questions

The research question of the present study aims to explore the privacy concerns of individual Internet users while making use of the theoretical framework of Internet Users’ Information Privacy Concerns. This question is answered by interpreting the transcripts from the interviews with the users of the health promotion website kryast.se in light of the conceptual framework of Internet Users’ Information Privacy Concerns. This necessitates an in-depth reference, both to the different conceptual dimensions of Internet Users’ Information Privacy Concerns and to related scholarly literature, as a conceptual background for a more profound understanding of privacy concerns that come to the forefront as a result of the interviews of Internet users. This study also aims at investigating whether the usage of Internet Users’ Information Privacy Concerns as a theoretical framework chosen for this investigation can adequately reflect the privacy concerns of Internet users based on the findings to which the qualitative methodology of interviews gives access.

Therefore, the research question of the present study is the following:

What are the Internet users’ information privacy concerns of a health promoting website?

1.4 Scope and Limitations

This study has chosen to collect qualitative data from the users of the health promotion website kryast.se in order to explore the privacy concerns of Internet users. The website whose users were chosen to participate in this research is developed by a private firm and has a relatively small number of customers. Therefore, among the major limitations of this study is that its findings may not necessarily apply to the privacy concerns of Internet users that utilize websites with large-scale user bases.

The present research is also limited in scope since it represents an exploratory interpretation of qualitative data collected from only seven interviewees. As opposed to quantitative research designs, in which the use of representative samples allows for making qualified generalizations about research populations, the present qualitative research design lays an interpretative stress upon the phenomenon of the privacy concerns of Internet users as such. The scope of the present study has been further limited by the theoretical framework of Internet Users’ Information Privacy Concerns that has been chosen for the interpretation of qualitative findings. Using other theoretical approaches to privacy concerns may have led this researcher to different analytic results and research conclusions. In this respect, the choice of the guiding theoretical perspective for this study has narrowed its scope to the tasks of its exploration and validation using the tools of qualitative methodology, such as interviews. Moreover, the secondary literature upon which this study is based has been drawn from the domain of information systems research, and which represents a further limitation of this study. For this reason, the analysis of the qualitative
findings that this study presents does not touch upon other aspects of privacy concerns, such as those related to psychological theories or political aspects.

Given that this study applies the qualitative tools of semi-structured interviews, the scope of this study is limited by the particular questionnaire that was used to elicit the answers from the users of the website kryast.se. While answers to these guiding questions provides qualitative data about the privacy concerns of the users of the specific website selected for this study, using a different questionnaire, a different qualitative research technique or a website from a different domain may have led to other findings. This limits the scope of this research.

Furthermore, the findings of this study may have been significantly affected by the choice of the website whose users and information technology personnel were interviewed. It is possible that the character of this website that promotes physical activity, fitness and psychological matters has affected the kind of privacy concerns that came to expression in these interviews. This represents an important empirical limitation since other websites may give rise to the different privacy concerns of their users due to the characteristics of the domain of activity of these websites and the sector of the consumer market in which they serve. Furthermore, given that the research participants for this study have been recruited in Sweden, the ability to generalize from the findings of this study may be limited, for the concerns of Internet users and information technology specialists in other countries may differ significantly from those in Sweden.

Thus, privacy concerns of users of larger-scale online environments and of users of comparable websites in other countries demand further investigation for their assessment.

1.5 Thesis Overview

The main purpose of this study is to explore the Internet users’ privacy concerns in the context of the specific health promotion website. The structure of this thesis is as follow.

Chapter one, Introduction, introduces the research topic and objective and discusses the knowledge gap in the area of investigation and outlines how this study plans to tackle the research question.

Chapter two, Theory, elaborates on the choice of theoretical framework, which stands at the heart of this study. An extensive literature review about the theoretical lens is provided in this chapter.

Chapter three, Methodology, starts with the implications of qualitative methodology followed by the philosophical worldview that the researcher stands. The data collection methods of Observation and Interview, as well as data analysis approach are discussed. Furthermore, the context of the case of this study, which a health promoting webpage is presented. This chapter ends with indications of particular validation and ethical considerations that this study trails.

Chapter four, Empirical Data, where the Theory meets the empirical data, annotates the story that has emerged from the findings. Hence in this chapter the analysis results are outlined.

In Chapter Five, Discussion, the implications of the study, as well as weakness and strength of the theory are outlined.
Chapter Six, Conclusion, warps up the findings and provides a passage for further researcher who wishes to follow the same path.
2 Literature Review

This chapter begins with a literature overview about the information privacy concerns of users in the context of health care. It then gives a summary of three main interpretive lenses that are used to explore Internet users privacy concerns and introduces the selected theory for this study.

2.1 The Framework of Internet Users’ Information Privacy Concerns

There are several existing studies that one can use to evaluate the Internet User’s Information Privacy Concerns (Malhotra et al., 2004; Smith et al., 1996; Van Slyke et al., 2006; Saeri et al., 2014; Culnan and Armstrong, 1999; Angst and Agarwal, 2009). In reviewing these studies mentioned, three important frameworks are highlighted as the basis of theories in the context of Information privacy concerns developed by IS researchers, and have shown to have an inter-relationship of aspects that could be very useful for the purpose of this thesis as well (Bélanger and Crossler, 2011). By discussing each identified framework, as below, this thesis evaluates the negative and the positive aspects of these three frameworks. As a result of the review, one of these framework is chosen as a theoretical framework in this thesis, which is used to evaluate the Internet user’s privacy concerns when it comes to a health related website. Considering the vulnerability of data that might be present in such websites, where healthcare data are stored for the patients, a rigorous review of these three frameworks have been undertaken.

Smith et al. (1996), Van Slyke et al. (2006) and Malhotra et al. (2004) have examined the interrelations between privacy concerns, individual beliefs and behavioural intentions while coming to varying theoretical conclusions.

Smith et al. (1996) have proposed the theoretical construct of Concern For Information Privacy as a factor that has a direct effect on behavioural intentions. In contrast, Van Slyke et al. (2006) have examined the relationship between the construct of Concern For Information Privacy and the willingness to transact online. Van Slyke et al. (2006) have found that the relationship between these variables is influenced by risk perception (Angst and Agarwal, 2006). As opposed to this conclusion, Malhotra et al. (2004) claim that information privacy concerns are fully mediated by individual beliefs, on the basis of which they have proposed the theoretical construct of Internet Users’ Information Privacy Concerns (Angst and Agarwal, 2006, p.351).

Whereas Smith et al. (1996) and Malhotra et al. (2004) have both focused on devising theoretical frameworks for the information privacy concerns that Internet users have in different contexts, most of empirical studies have followed the approach of Smith et al. (1996) by applying the theoretical framework of Concerns For Information Privacy. As it’s shown in Table 2 which demonstrates the differences between existing constructs for privacy concerns in online environments that Malhotra et al. (2004) have put together, there are three main theories that have been primarily used in scholarly literature to evaluate information privacy concerns across different contexts.
Table 1- Comparison between GIPC, CFIP and IUIPC (Inspired by Malhotra et al., 2004, p.340)

<table>
<thead>
<tr>
<th>Theory Name</th>
<th>GIPC</th>
<th>CFIP</th>
<th>IUIPC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>To examine the privacy concerns on general level</td>
<td>To examine individual’s concerns in organizational context</td>
<td>To examine Internet Users privacy concerns</td>
</tr>
<tr>
<td>Target</td>
<td>No specific target</td>
<td>Mainly organizations to optimize handling customers data</td>
<td>Individuals attitudes towards fairness of sharing private information</td>
</tr>
<tr>
<td>Communication</td>
<td>Both one-way and two-way communication theory</td>
<td>One-way Communication theory</td>
<td>Primarily two-way communication theory</td>
</tr>
<tr>
<td>Factors</td>
<td>One-dimensional Theory</td>
<td>Collection, improper access, unauthorized secondary use and error</td>
<td>Collection, Control and awareness</td>
</tr>
<tr>
<td>Flexibility</td>
<td>First order factors</td>
<td>First order factors, however “Stewart and Segars (2002) argued that CFIP is better represented as second order”(Malhotra et al., 2004, P.340)</td>
<td>Second order factor</td>
</tr>
</tbody>
</table>

As opposed to the one-dimensional scale of Global Information Privacy Concerns that has been devised to measure the general concerns of individuals about information privacy, Smith et al. (1996) have proposed a multidimensional scale of Concern For Information Privacy that was designed to measure individual concerns about organizational information privacy practices.

The present research will apply, for analytic purposes, the scale of Internet Users’ Information Privacy Concerns Upon rather than the scale of Concern For Information Privacy on the following grounds. First, the research objectives of this study relate to online environments as well as two-way communication rather than to direct marketing that the scale of Concern For Information Privacy has been originally devised. Secondly, the theoretical framework of Internet Users’ Information Privacy Concerns has hardly been used for empirical inquiries into individual concerns regarding information privacy. Given that Bélanger and Crossler (2011, p.1020) have indicated that the concept of Internet Users’ Information Privacy Concerns has heuristic research potential in the field of information systems studies, the present researcher intends to make a contribution to the nascent process of adapting this theoretical framework for qualitative research designs. This study will apply the construct of Internet Users’ Information Privacy Concerns to analyse interviews also because this theoretical framework is suited for explaining a person’s willingness to transact online (Malhotra et al., 2004). Thus, the theoretical framework of
Internet Users’ Information Privacy Concerns suits the purpose of this study better than other frameworks.

Furthermore, Malhotra et al. (2004) has furthermore developed a model by merging the Internet Users Information Privacy Concerns (IUIPC) theory as the first order theoretical framework with Trust concept. The arisen model has been evaluated against its interrelationships between IUIPC theory, Trust and Risk and has found out “that trusting beliefs mediated the impact of IUIPC on behavioral intention” (Malhotra et al., 2014, p.349). Individuals behavior tend to be influenced by trust in a risky environment. Trust is believed to justify individuals behavior in sharing their information publicly, when there is a risk of violating their privacy. Malhotra et al. (2004) defined it as “Trusting beliefs are defined as the degree to which people believe a firm is dependable in protecting consumer’s personal information” (p.341). In online context, trust corroborate positive attitudes in that it stimulates disclosure of private information (Saeri et al., 2014).

Also studies suggest that trust stands at the heart of social exchange theory in interpersonal research (Metzger, 2004). Social exchange theory claims that individuals only engage themselves in exchanging data, when the benefits and rewards outweigh the cost and risk associated to this action. Trust plays a critical role in that exchange process, as it’s believed to be the crucial motive of individuals to reveal their personal data, even though the perceived risk and costs might outweigh the benefits gained through the exchange deal. In other words, Trust helps to reduce the perceived costs versus benefits.

2.2 The Theory of Internet Users’ Information Privacy Concerns

Malhotra et al. (2004) have based their studies on the fact that “individuals’ concerns about information privacy cannot be fully understood without investigating how individuals define justice in this long term exchange of information” (p.337). Thus, the Internet Users’ Information Privacy Concerns model was built based on a social contract theory that has been considered effective for studying the perception of fairness and justice (Donaldson and Dunfee, 1994). These two theories postulate that users’ concerns regarding information privacy cannot be grasped unless the way “individuals define justice in this long term exchange of personal information be investigated” (Malhotra et al., 2004, p.338). Thus, the theoretical framework of Internet Users’ Information Privacy Concerns was mostly reformed by the social contract theory that is considered useful for studying the perception of fairness and justice (Donaldson and Dunfee, 1994). When it comes to information privacy, the social contract theory indicates that “a firm’s collection of personally identifiable data is perceived to be fair only when the consumer is granted control over the information and the consumer is informed about the firm’s intended use of the information” (Malhotra et al., 2004, p.338). Numerous other studies on information privacy have also used the same basic theory. For instance, Milne et al. (1993) has used the social contract theory as a tool to capture customers’ behaviour with marketers dealing with particular privacy concerns. Thus, Internet Users’ Information Privacy Concerns was conducted consisting three dimensions of collection, control, and awareness of privacy practices that will be explained respectively.

Information systems researchers have paid extensive attention to information privacy concerns in their effort to explain the variation of privacy concerns or to test the influence of users’ privacy
concerns on various factors, such as a user’s willingness to share their personal information or to transact online. Basically, the concept of information privacy concerns is used in order to account for users’ attitudes and reactions to requests to provide their personal information through the Internet. Most studies around this topic have found that various perceptions of individuals can be influenced by information privacy concerns, such as users’ technology acceptance (Malhotra et al., 2004; Smith et al., 1996). Studies that follow the theoretical framework of Concern For Information Privacy proposed by Smith et al. (1996) have been focusing on the privacy concerns that individuals have with regard to organizational practices. The studies that have used the theoretical framework of Internet Users’ Information Privacy Concerns devised by Malhotra et al. (2004) have concentrated upon individual privacy concerns and personal perceptions of fairness in the context of information privacy. Although the Concern For Information Privacy scale has become a de facto standard for the measurement of information privacy concerns, Malhotra et al. (2004) have demonstrated that the concept of Internet Users’ Information Privacy Concerns can explicate a users’ willingness to share their information online better than the construct of Concern For Information Privacy.

2.2.1 The Dimension of Collection

Collection, as the first conceptual dimension of Internet Users’ Information Privacy Concerns “is the act of gathering data whether it is legal or not” (Zukowski and Brown, 2007, p.198). The dimension of Collection has been defined as “the degree to which a person is concerned about the amount of individual-specific data possessed by others relative to the value of benefits received” (Malhotra et al., 2004, p.338). In direct marketing environments, customers are more willing to share less information about themselves and expect something valuable in return, which is based on the social contract theory's principle of distributive justice. The theory of distributive justice indicates “the perceived fairness of outcomes that one receives” (Culnan and Bies, 2003, p.328). At the same time, in relation to e-commerce contexts, individuals can be expected to be reluctant to share their personal information if they perceive their privacy concerns about sharing their personal information to outweigh the beneficial outcomes of doing so (Culnan and Bies, 2003; Malhotra et al., 2004). In fact, prior research has also indicated that the dimension of information collection is one of the main factors that leads to privacy concerns. For instance, collection is one of the main four dimensions of Concern For Information Privacy. Collection can, thus, be considered as one of the main factors that “captures the central theme of equitable information exchange based on the agreed social contract”, hence expected to be treated as a critical factor of privacy concerns among users (Malhotra et al., 2004, p.338).

Considering collection as one of the main factors that determines the privacy concerns of internet users, the research questionnaire of the present study contains three questions which explore the importance of this factor for research participants. This will be discussed further in Chapter three.

2.2.2 The Dimension of Control

The second dimension of Internet Users’ Information Privacy Concerns is grounded in the social contract theory principle of procedural justice which indicates that “individuals view procedures as fair when they are vested with control of the procedures” (Thibaut and Walker, 1975 in Malhotra et al., 2004). The dimension of control refers to the freedom of voice, or having the choice to exit a situation. Control is rooted in the procedural justice principle in the social contract theory (Tyler, 1994). According to this principle of procedural justice, individuals perceive the
procedures fair when they are empowered by having control of the procedure (Tyler, 1994). Thus, consumers should have the freedom to either accept or reject within the procedure of the decision’s outcome (Malhotra et al., 2004).

The principle of procedural justice also implies that moral contractors acquire control over their personal information by having the freedom to either accept or reject the process or decision outcomes (Malhotra et al., 2004). Since sharing personal information on a website is believed to be a risk that a user should decide to take, Malhotra et al. (2004) have developed a second hypothesis that is based on the fact that if internet users are given control over their personal information that they share on a website, then they feel more confident. According to Internet Users’ Information Privacy Concerns theory, users are believed to have control by the freedom of the choice of approval, modification, or opt-out (exit).

Other studies also suggest that in order to address the information privacy concerns, consumers should have the option to approve, exit or ask for modification when sharing their personal information. (Caudill and Murphy, 2000). For instance, in a study conducted by Phelps et al. (2000), the majority of people (84%) were more willing to have control over their personal data in order to receive fewer unwanted emails, and 62.4% were concerned that they had no control over their information and felt that most companies know too much about consumers (p.35). Thus, with the widespread use of Internet technologies of social media, Internet users increasingly lose control over their private information. This critical issue of lacking control over personal information is likely to cause information privacy concerns among Internet users.

2.2.3 The Dimension of Awareness

A literature review of information privacy concerns suggests that a person is given information privacy when he/she has a) control over their information b) is informed about the kind of practices that are performed by their personal information (Foxman and Kilcoyne, 1993).

Collection and control are the active factors when determining one’s privacy concerns. On the other hand, awareness is a passive component of privacy concerns. Awareness is defined as the degree to which a consumer has concerns and is generally aware about information privacy practices at organizations that he or she deals with (Malhotra et al., 2004, p.339).

Awareness as a component of the Internet Users’ Information Privacy Concerns is separate but as depicted in Figure 1 interrelated with the control factor. Therefore, meaning that when an individual is believed to have control over his/her personal data, then they are aware of the actions being practiced on his/her data. Awareness is also used indirectly in other studies as a crucial factor to determine an individual’s privacy concerns.

Awareness of privacy practices: As opposed to the control dimension that is a direct characteristic of information privacy and should be practiced by either the approval, exit or modification, awareness of privacy is a passive dimension of Internet Users’ Information Privacy Concerns. Awareness is referred to as “an extent to which a consumer is concerned about his/her awareness of organizational information privacy practices” (Malhotra et al., 2004. p.339; Foxman and Kilcoyne, 1993). However, consumers are most likely not aware that the information that they provide for marketers is perceived as “marketer’s property” (Foxman and Kilcoyne, 1993). This issue is believed to invade an individual’s privacy. The awareness factor is interrelated with two kinds of justices, interactional and informational justices. Interactional justice is an “issue of
transparency and propriety of information made during the enactment of procedures”, and informational justice is “the disclosure of specific information” (Malhotra et al., 2004, p.339). In a survey conducted by Phelps et al. (2000), nearly 50% of the people in the study were willing to be aware of the transparency of their personal information with regard to how organizations use their information. Thus, awareness is believed to be another central factor that is used to evaluate an individual’s concerns about their information privacy.

![Figure 1- The Connection between IUIPC and its components- adapted from Malhotra et al. (2004, p. 341).](image)

2.3 **The Role of Internet Users’ Information Privacy Concerns Theory in this Study**

In this study, the concept of the Internet Users’ Information Privacy Concerns works as an interpretative framework for its qualitative research results. Additionally, this conceptual framework has served as a frame of reference for data collection, such as for the construction of the questionnaire, due to its prominence in quantitative studies on the subject of information privacy concerns. In this manner, the present study intends to explore the heuristic potential of the theoretical framework of Internet Users’ Information Privacy Concerns for qualitative research. The conceptual framework of Internet Users’ Information Privacy Concerns has been considered to be well-suited for the purpose of this study since it proposes a unified theoretical construct for the exploration of privacy concerns (Malhotra et al., 2004, p. 340). Also as challenged by Bélanger and Crossler (2011, p.1020), when it comes to explorations of privacy concerns in the field of Information Systems, the concept of Internet Users’ Information Privacy Concerns has experiential research potential in comparison to other theories. Especially given the objective of this study relates to the Online and two way communication environment, rather than direct marketing that the scale of Concern For Information Privacy has been originally devise. Hence as a researcher I choose to set the ground on the theory that is proven to be well suited for the purpose of my study. Naturally using different theory for the same study might render different perspective of seeking the same objective. Since its different dimensions outlined above do not represent separate variables, but subscales within this construct of Internet Users’ Information Privacy Concerns, this qualitative study further explores possible causal links between privacy concerns and risk perceptions, trust beliefs and online use intentions (Malhotra et al., 2004, p. 341). In doing this, the present study takes departure from a quantitative treatment of both Internet Users’ Information Privacy Concerns and these behavioural and attitudinal aspects of Internet use, which disaggregates these scale based on first-order qualitative data into their
constitutive elements. In this regard, the role that the theoretical framework of Internet Users’ Information Privacy Concerns plays in this study is primarily analytical, since it enables deriving second-order analytical conclusions from first-order interview data. While this study does not follow the proposition of Malhotra et al. (2004, p. 340) to treat Internet Users’ Information Privacy Concerns as a second-order quantitative construct, it seeks to arrive at qualitative generalizations from empirical material that represents privacy concerns of Internet users in a particular online setting.

2.4 Previous Studies Using the Framework of Internet Users’ Information Privacy Concerns

According to Bélanger and Crossler (2011), whose research made an attempt to review the scholarly literature on the topic of information privacy concerns, there have been relatively few studies which have used the Internet Users’ Information Privacy Concerns as their theoretical framework in order to explore the privacy concerns of Internet users in different contexts. Besides, all of these studies have used this theoretical approach as part of quantitative methodology that has applied the construct of Internet Users’ Information Privacy Concerns for measuring the privacy concerns of individuals with an aim of providing further validation for this conceptual framework. Whereas Malhotra et al. (2004) have sought to examine the theoretical assumptions behind this conceptual framework, subsequent studies have mostly concentrated on applying the concept of Internet Users’ Information Privacy Concerns as a variable within different quantitative research designs.

The first study that has used the framework of Internet Users’ Information Privacy Concerns as its theoretical lens is Zukowski and Brown’s (2007) research that has examined the influence of demographic factors on the information privacy concerns of Internet users. The factors that compose the internet users concerns for information privacy are the dimensions of Collection, Control, and Awareness as they are defined within the framework of Internet Users’ Information Privacy Concerns that Zukowski and Brown have applied (2007, p.197). In order to examine the influence of demographic factors on these dimensions of privacy concerns, Zukowski and Brown (2007) have distributed corresponding questionnaires to 199 respondents. The hypothesis that these authors have tested pertained to the question concerning demographic factors shaping antecedents of the primary dimensions of the Internet Users’ Information Privacy Concerns construct. In order to examine their theoretical assumptions about the interrelations between the concept of Internet Users’ Information Privacy Concerns and the demographic factors, Zukowski and Brown (2007) have relied upon the analysis of correlations between their research variables. In this study, thus, the significance of correlation coefficients was taken as an indicator for the interrelationships between these factors. Also being based on the methodology of quantitative research, this study has confirmed the hypothesis that it has derived from existing literature. The results of Zukowski and Brown’s (2007) study suggest that demographic factors, such as age, education and income level, have a significant impact on the information privacy concerns of Internet users. More specifically, Zukowski and Brown (2007) have found that these demographic factors moderately determine the privacy concerns that sharing information in the Internet may give rise toward. Based on the correlations between the dimensions of Internet Users’ Information Privacy Concerns and the demographic factors, Zukowski and Brown (2007) have indicated that Control and Awareness are the components of the privacy concerns concept that are most closely
interrelated, apart from being influenced by the demographic characteristics of Internet users. The results of this study, thus, demonstrate that individual awareness about risks to privacy in which Internet use involves has a significant impact on their concerns about not having control over their personal information.

In the empirical study carried out by Yang and Miao (2008), the determinants of Internet Users’ Information Privacy Concerns have been examined based on a sample drawn from the community of Chinese Internet users. This research has explored the interrelations between the information privacy concerns of Internet users (IUIPC) and their intention to make online transactions (Yang and Miao, 2008). Since the main purpose of this study is to examine the relationship between these two variables among Chinese Internet users, this research has adopted quantitative methodology. Questionnaire responses about their intention to make online transactions, to have trust in websites, and their privacy concerns were all collected from a representative sample of 759 Chinese respondents recruited from the student population. Since at the time of Yang and Miao’s (2008) study no legal frameworks for the protection of the privacy of Internet users were established in China, these researchers have applied the internationally validated construct of the Internet Users’ Information Privacy Concerns as a theoretical lens for their inquiry. The results of this study indicate that Internet Users’ Information Privacy Concerns is a valid instrument for the measurement of the information privacy concerns of Internet users in China. This research, thus, “offers support for the measurement model’s uses in many fields” (Yang and Miao, 2008, p.3).

Also, the study suggests that, compared to other dimensions (e.g., control) of the theoretical construct in which these researchers have utilized, the awareness dimension of Internet Users’ Information Privacy Concerns has been found to have the highest and most significant impact on the readiness of Chinese Internet users to make online transactions. The findings of this research suggest that, in order to establish the reputation of online commerce in China, the Internet privacy concerns of individuals should be addressed and their trust should be earned by the websites oriented to the consumer market. Yang and Miao’s (2008) study also indicates that the construct of Internet Users’ Information Privacy Concerns in and of itself does not have a direct impact on the willingness of a surveyed individual to carry out transactions online. Yang and Miao's (2008) research findings show that the variable of trust is critical for the motivation of individuals to engage in online transactions, since the respondents were found to have given their preference to those online companies in the privacy protection policies of which they could have a greater reliance.

Last study is contributed by Nov and Wattal (2009) and has been used in prior literature on trust, privacy concerns (IUIPC), and social norms in order to hypothesize the additional determinants that may influence users’ privacy in online communities. Since this study merged three theories to evaluate users’ concerns in a social network context, the significance of the study is based on validating the merged scale that it has proposed. Consequently, in this study exploration of the antecedents and effects of privacy concerns has adopted quantitative methodology (Nov and Wattal, 2009). Nov and Wattal's (2009) study seeks to understand how privacy concerns influence the readiness of individuals to share their personal information at social networking websites, such as Facebook or Flickr. As an inquiry into users’ privacy concerns in social media environments, Nov and Wattal's (2009) research has hypothesised that the role of social norms and trust in other members of the same community can determine the level of a user’s privacy concerns. In this research, trust plays a key role as a factor that influences the motivation of individuals to share their personal information. Using quantitative methodology to examine their
hypothesis, Nov and Wattal (2009) have measured additional factors that impact users’ privacy concerns in social networks. Consequently, the study of Nov and Wattal (2009) makes a partial use of the theory of Internet Users’ Information Privacy Concerns as a tool for testing their hypothesis that Internet privacy concerns are positively related to social networking community-specific privacy concerns. The results of Nov and Wattal’s (2009) research indicate that the level of trust toward other members of social networks and the corresponding online community information sharing norms and culture have a negative impact on the privacy concerns of social networks users and their willingness to share their personal information publicly.

2.4.1 An Overview of Theoretical Frameworks of Information Privacy Concerns

Information privacy has been studied through various lenses with consideration for different perceptions. In an attempt to review the studies regarding information privacy concerns in all sectors, specifically the information system section, most of the studies have used two theories to explore individuals’ concerns regarding their privacy. They have used mostly Concerns For Information Privacy (CFIP) or Internet User’s Information Privacy Concerns (IUIPC).

According to research conducted by Bélanger and Crossler (2011), the former studies in this scope of topics were more focused on trust, culture, security, economics of information privacy, surveillance, personalization, risk, marketing, and control. However, this study aims to explore the concerns of patients regarding their informational privacy on a healthcare promotion website through the qualitative-interview approach. Thus, this study aims to discover patients’ perceptions of what happens with the information that they share on the website (Dinev et al., 2006). As it was aforementioned, the theoretical framework chosen for this study is Internet Users’ Information Privacy Concerns which outlines users’ privacy concerns based on the “subjective views of fairness within the context of information privacy” (Malhotra et al., 2004, p.337).

Before developing the scale of IUIPC, most studies used the scale of Concern For Information Privacy that has been proven and used in various studies. However, studies in this regard suggest that Concern For Information Privacy is suitable for the offline marketing context (Stewart and Segars, 2002). As internet users’ concerns regarding their information privacy may differ from offline consumers, Malhotra et al. (2004) developed a model for Internet Users’ Information Privacy Concerns (IUIPC) and validate it through a study which is believed to be better suited for the context of online privacy (Yang and Miao, 2008).

Despite all the aforementioned factors that influence an individual’s intention to share their personal information on the Internet, certain studies about consumer attitudes in e-business and e-commerce environments indicate that there is a single dimension that plays an important role in affecting the intention of individual users to divulge their personal information. This additional dimension as discussed earlier is trust (Malhotra et al., 2004, Vail et al., 2008). Exploring the effect of trust on information privacy concerns, some studies have shown that trust crucially affects the relationship between users’ privacy concerns and their intentions to transact online (Bélanger et al., 2002; Van Slyke et al., 2006). Furthermore, recent quantitative studies suggest that violating information privacy concerns is likely to lead to the loss of trust among the customers of commercial websites, especially when their private information is shared without their authorization (Bansal and Zahedi, 2015, p. 62).
As former studies have suggested, information privacy concerns can inspire Internet user's attitudes toward decision-making. For instance, this can be exemplified by their willingness to be profiled or their acceptance of using the internet for promoting their health. Through this study, users of health promotion websites have concerns regarding their information privacy that will be identified by using IUIPC theoretical framework. As previously discussed in Introduction chapter, researcher have studied the information privacy concerns through other perspectives, such as personal characteristics, namely age and institutional factors (Xu et al., 2008). However this study has deeply rooted its theoretical framework in the theory of Internet users Information Privacy Concerns (IUIPC), which has been developed and verified by Malhotra et al. (2004). The IUIPC theory conceptualizes itself based on three factors which are Collection, Control and Awareness. Therefore the theoretical framework of this study has mainly positioned itself on those three main factors, which in this particular model they don’t represent any interrelations with personal characteristics. While there are other conceptual theories in the context of information privacy concerns that have paid attentions to others aspects of privacy concerns, the current study is meant to be solely focused on the theory of IUIPC. Combining it with other aspects might divert the focus of three aspects, as well as result in failing to follow the passage of the work as presented by Malhotra et al. (2004). In essence, Malhotra et al. (2004) proposed a model in the second part of their study to find the interrelationship between the second order IUIPC model and behavioural intentions. The proposed model, consists of IUIPC theory, Trust/Risk Beliefs, behavioural intentions and covariate variables, namely age, education and Gender. The casual model has then been evaluated in a quantitative study against its hypotheses to identify and introduce a model which its factors could justify one's behaviour in regards to information privacy-related issues in an online environment. The results of the study indicate that Age had negative interrelationship with individuals intentions to share personal information, as well as “no effect of gender and experience as victims were found on the context-contingent factors” (P.348). Hence it is possible to indicate that Malhotra et al. (2004) did not ascertain any interrelationship between Internet Users Information Privacy Concerns theory and demographic factors, namely Age, previous experience as victims and Gender. Accordingly, this study follows the same lead and does not treat demographic factors as fundamental aspects in conjunction to individuals reactions to the privacy-related issues.

The possible implications of personal factors are shortly discussed in the empirical findings but are not treated with high priority in this study. Naturally, prioritizing other theories for the same study might result into new interesting requirements, which due to time constraint this study is excused to fulfil.
3 Research Methodology

In this chapter the characteristics of a qualitative research methodology laid out for this study will be discussed and the possibility of the integration between empirical data and the theoretical framework will be explored.

The lack of trust in online environments has led many Internet users to consider sharing their personal information over the Internet as involving risks to their privacy. In particular, Internet users perceive their health information as sensitive information from the privacy perspective. Based on their attitudes and perceptions about risks to their privacy, Internet users might be unwilling to share their information online. Identifying users’ concerns regarding their privacy can help to explore particular dimensions of users’ expectations from websites in terms of protecting their privacy.

In order to achieve the desired purpose of this study that is aimed at exploring users’ concerns about a health promotion website, the process of collecting research materials has followed a theoretically oriented approach. As part of this approach, scholarly literature on the topic of information privacy concerns has been reviewed. For the purpose of exploring users’ privacy concerns, the scholarly publications in the field of information systems studies have focused on different aspects of information privacy and its technical aspects. Of relevance to this study the scholarly sources that have mainly focused on the formulation and validation of theories concerning information privacy and user concerns in online environments.

In this regard, the most well-known theoretical approach in the online environment is the theoretical framework of Internet Users’ Information Privacy Concerns that was proposed by Malhotra e al. (2004). This theoretical framework consists of three different dimensions named Collection, Control, and Awareness. This theoretical framework has primarily been used by information systems researchers in order to conduct quantitative inquiries that have been aimed at identifying the privacy concerns of online users in relation to different quantitatively-defined variables. Nevertheless, to date there have been no studies that would validate this theoretical framework using a qualitative methodological approach. Therefore, one of the purposes of this study is to contribute to a further development of this theoretical framework and to facilitate its wider application by other information systems researchers by proposing a qualitative validation of this framework theory that proposes an analytical frame of reference for inquiries into the privacy concerns of Internet users.

Since qualitative methodology is used for the purpose of this study, the involvement of actual Internet users as research participants for the qualitative assessment of the selected conceptual framework is essential. Therefore, another complementary approach of this study is empirically-oriented that requires the involvement of users of the health promotion website. For this qualitative research, having in-depth communication with the users of the chosen website is crucial. Qualitative researchers use different methods for the data collection from their research participants. For the sake of this study, I have chosen observations and interviews as methods of empirical data collection. In this chapter, the interview questions and their connection to a theoretical lens will be elaborated. Observation is the other method of data collection that makes it possible for the researcher to analyse users’ behaviour, resulting in a more accurate qualitative
analysis. More importantly, observation facilitates and compliments the process of collecting interviews. Therefore, observations and interviews mutually facilitate the analysis of researcher results.

In the following chapter, the main characteristics of a qualitative study established for this study is fully discussed.

3.1 **Philosophical worldview**

The philosophical worldview for this study is an interpretive one. This study seeks to assess the privacy concerns of Internet users while making use of the qualitative methodology. Consequently, the interpretive worldview can particularly suit the objectives of the present research since it can accommodate both qualitative research methods and a critical perspective on empirical findings (Myers and Klein, 2011, p.18). This philosophical worldview allows the possibility of reaching the aims of this study because it agrees with an approach of the privacy concerns of Internet users while using a particular guiding theoretical framework (Myers and Klein, 2011, p.19). As opposed to the positivist research paradigm (Lincoln and Guba, 1985), the interpretive worldview will allow making a contribution to information systems’ scholarly literature by proposing a qualitative perspective on privacy concerns. Therefore, a standpoint that this study assumes is an interpretive approach that can deepen the qualitative understanding of a subject matter. This helps the researcher to understand how individuals experience their world where their particular concerns are situated. As Angen (2000) states: “Interpretive researchers assume that reality as we can know it is constructed intrasubjectively through the meanings and understandings garnered from our social world” (p.385).

An interpretive researcher is engaged in the process of understanding the phenomena from the user's perspective. Myers (2008, p.38) indicates that “interpretive researchers assume that access to reality (given or socially constructed) is only through social constructions such as language, consciousness, shared meanings, and instruments”. The interpretive researcher has the characteristic of being interactive and participative in the environment where the actors of research exist. In such environment the researcher seeks to identify the concerns and issues with which people are coping, and how they deal with such situations. It attempts to understand various phenomena from the perspective that people assign to them (Klein and Myers, 1999). Although we can never be confident of anything related to human beings and their behaviour, we can at least “legitimate the ground for believing that some things are clearly better than others” (Madison, 1988, p.35).

Also, interviews and observations are well known data collection methods that can be readily utilized for interpretive studies and research designs. The interpretive approach conceives of individuals and reality as inseparable and builds up knowledge based on what the researcher perceives. The researcher is, therefore, engaged in the interpretation of the world through the eyes of research participants. As a researcher engaged to achieve my academicals goal, I believe the world we live in is only well understood once we endeavour to produce an interpretation of it. From the scholarly point of view, this is well matched with what interpretive researchers aim for. In line with Myers and Klein (2011, p.20), this study also aims at creating bridges between qualitative and quantitative studies of the phenomenon of privacy concerns of Internet users.
3.2 Research Design

In order to achieve the goals of the study, the in-depth analysis of the real users of a health promotion website on the Internet is required. In the first step of qualitatively exploring the privacy concerns of Internet users, research participants have been chosen. Through this phase, three groups of people were interviewed. These groups included the online users of the website, the IT specialist and the coach team.

Qualitative research design has the potential to consider an issue not only from a researcher perspective, but also from the perspective of his/her research participants too. In this regard, Lincoln and Guba (1985) state that “[I]f you want people to understand better than they otherwise might, provide them information in the form in which they usually experience it” (p.120). Whereas, Cronbach (1969) believes that the statistical research cannot consider all the effects that occur in the natural setting. Lincoln and Guba (1985) state that “the time has come to exorcise the null hypothesis,”(P.124) and use the qualitative research approach that is more frequently adapted for the volatile world of today.

According to Tracy (2010), there are basic characteristics that define qualitative research designs, such as conducting research in natural settings, with the researcher being the primary instrument of research, using a particular theoretical lens, using multiple sources of data, inductive data analysis, and paying attention to participants’ meanings.

The argumentation for this thesis concerning the choice of qualitative research methodology is discussed below. However, as Patton (1990) states, “these are not absolute characteristics of qualitative inquiry, but rather strategic ideals that provide a direction and a framework for developing specific designs and concrete data collection tactics” (p. 59).

Natural setting: Qualitative researchers attempt to understand their subjects in their natural settings. Thereby, researchers attempt to interpret the phenomena that they make their inquiry in terms of the meanings that research participants give to them (Denzin and Lincoln, 2000). In order to achieve this goal, the website http://kryast.se/ has been chosen as a context for the present research. In the process of this study, the concerns of its participants about information privacy were observed in their real-life setting. This has helped me to evaluate and explore the concerns about information privacy that are held by the users of that website.

Researcher as the key instrument: According to Tracy (2010), qualitative researchers collect their data from various sources. Which includes documents, observations, interviews, etc., rather than relying only on secondary sources, such as studies by other researchers or closed questionnaires. In this respect, a series of face-to-face interviews are conducted with the consumers of the chosen website in order to collect information about privacy concerns from the perspective of individuals using a particular website.

Theoretical lens: Qualitative researchers regularly use a theoretical lens to have a more focused insight into the subject of their study (Tracy, 2010). As it was mentioned in the theoretical framework section, Internet Users’ Information Privacy Concerns is a theoretical approach to investigating antecedents and outcomes of privacy concerns that the website use can potentially involve. Due to its complexity, this theoretical framework for accounting for privacy concerns has not been broadly used by information System researchers. Therefore, it has been chosen for this
study as a lens for gaining a deeper understanding of the privacy concerns that can be a result of the sharing of personal information on the Internet. This thesis will, thus, use different dimensions of Internet Users’ Information Privacy Concerns as analytical tools for reflecting upon its empirical results.

3.3 Data Collection Methods

In this thesis, two methods for data collection are used: interviews and observations. A more detailed description on the process of involving each method is given below.

Interview: For this study, semi-structured interviews will be conducted in connection to the chosen website (kryast.se) among its users and support personnel. The target group are the users or patients who use this website for health promotion purposes. The main purpose of conducting semi-structured interviews with users of this fitness promotion website is to capture their concerns regarding their information privacy on the website. All the respondents for this qualitative research will be recruited among the users of the selected website who have an active account at the website and are consulting it in regard to health-related issues and fitness activities. However, no specific determinants for choosing the participants and users have been selected other than their willingness to participate in the interviews. The voice recorder is used during the interviews with the pre-acknowledgements. The interview guides will be used to ask the same prepared questions from different consumers and to make the interactions more focused (Hoepfl, 1997). However, questions may be modified through the research to be more concentrated on the areas of particular importance (Hoepfl, 1997).

The key points that this study is aiming to explore are answered through face-to-face interviews, as well as telephone interviews. Sometimes, an opportunity was provided to interview the users of this website several times. Additionally email interviews were used throughout the whole data collection process in this research. The online users group which are the main focus of this study have been recruited from the moderately active users of the website. Seven users were interviewed and their concerns for their privacy matters were identified. In addition to the users, one of the main developer as well as one of the main couch/adviser of the website were interviewed.

After conducting the interviews, the recordings were transcribed verbatim. The qualitative data collected through semi-structured interviews are presented in transcribed form in the Appendix II.

Observation: Since the website users should pay a monthly fee for using the services provided for them, the owner of the website who also provides the users of the website with different kinds of fitness-related guidelines has provided the present researcher with an account that enables a passive observation of the website. This opportunity has facilitated this research in reaching deeper understandings than through interviews alone because it has equipped the primary researcher with the knowledge of the context of this investigation, a possibility to explore the research problem, and an opportunity to see things that participants themselves are not aware of (Patton, 1990). Moreover, field notes will be used during each observation to provide descriptions about the users’ health related and other activities.

In the process of collecting data for this study, the users’ behaviours in terms of sharing their information publicly has been observed, since social networks at a health promoting website have
their own characteristics. This practice of observation upon collecting the data for this study involved inspecting a selected group of users of this website, who are more actively using the website over several weeks. Their behaviours have been mostly monitored at specific time of weeks, i.e. weekends, by when participants have more spare time to engage themselves in sharing information. One useful insight the observer could retrieve from this aspect of qualitative research is to analyse the behaviour of the users of this website to get a better understanding of the selected users before the in-depth analysis. This could better prepare the researcher for more constructive interviews, resulting in arriving with more specific questions to the situation of interviews with research participants.

3.4 Interview Questions

Before collecting empirical data by means of semi-structured interviews, it was essential to construct the interview questions based on the dimensions of the theoretical framework of Internet Users’ Information Privacy Concerns since it is the theoretical lens chosen for this study. Based on the literature review, previous studies have also used the framework of Internet Users’ Information Privacy Concerns in order to explore information systems users’ concerns in different environment. This has helped me to have a frame of reference for the composition of the interview questions. At least nine questions were asked from the users of the health promotion website chosen for this study. In some cases during the interviews, research participants were questioned about their practices of sharing sensitive information on the website in which they actively use. Moreover, I have interviewed one of the main information technology specialists who have designed the website and have access to the information of its users. While the users of the healthcare promoting website are the highest focus of the empirical data collection, a separate interview with one of the main developer of the homepage shed lights on some technical aspects that users of the website were unaware of, where the conflict in responses between users expectations and real practices of users data is realized. A separate interview is also conducted with one of the main coaches of the website who provides public and private healthcare advices and guidelines, which is also insightful on the real practices being performed on users personal information.

For the interviews conducted with the users of the website and a representative of its information technology specialists and health coach, the questions that have been used were based on the three main components of the theoretical framework of Internet Users’ Information Privacy Concerns. Consequently, in this research, over three questions were formulated to reflect the collection component of the chosen theoretical framework, three to reflect the control component, and two to investigate the awareness component. Furthermore an additional question was raised to rationalize users behaviour, when the Internet Users Information Privacy Concerns theoretical framework fails to justify individuals decision to share their private information. This question was rather unplanned and was arisen throughout the interviews as necessitated. The template for the interview questionnaire is represented in Table 2.
**Table 2- Template of interview questions**

<table>
<thead>
<tr>
<th>Dimension</th>
<th>Number of question related</th>
<th>The questions</th>
</tr>
</thead>
</table>
| **Collection** | 3                          | What sort of information have you been asked to share by the website?  
What sort of activities do you usually share on the website, and what are your expectations from your coach on the website in return?  
Have you ever been concerned or felt doubtful to share your personal information or an activity because you felt that doing so may threaten your privacy, or the requested information is too personal?(collection)  
A-Yes, could you please share your experience.  
B-No, what do you think has protected you from these threats? |
| **Control** | 3                          | How easily do you have access to any information related to you on the website?  
Do you have an option to opt-out (exit) or delete your written activities in case if you want to unregister yourself from the website? When registering on the website, have you been informed about your options to unregister or remove all your personal information from the website?  
Do you use your real name as your real ID on the website? If not, can you explain your reasons? |
| **Awareness** | 2                          | Are you aware of the possible threats that may violate your privacy by misusing your personal information? How likely do you think these sort of incidents may happen in kryast.se? Do you think you have sufficient knowledge about the risk of sharing personal information and the privacy issues it can cause?  
How much have you heard or read during the last year about the use and potential misuse of the information collected from the internet? Do you use any sort of particular software to ensure your privacy protection? |
3.5 Data Analysis

Succeeding the verbatim transcription of collected data through interviews and Observation, within the next step, the text needs to be analysed through interpretations. The method chosen for analysis of the empirical data of this study is stirred by “directed content analysis” (Hsieh and Shannon, 2005, P.1284). According to Hsieh and Shannon (2005) the directed content analysis is well suited for a qualitative study that seeks to start with an existing theory. “Using an existing theory or prior research, the researcher starts immediately coding by identifying the key concepts or variables as initial coding categories [hence,] “codes are derived from theory or relevant research findings” (Hsieh and Shannon, 2005, P.1286).

The binding between data collection and the analysis of empirical data for this study rests upon a pattern that is rooted deeply in the theoretical framework that was chosen for this study. The IUIPC theory consists of three main factors of Collection, Control and Awareness. Thereby prior to data analysis, after grasping the theory and literature related, codes such as collecting sensitive information, expectations, awareness, fairness, etc. have been generated in conjunction to the research question and theoretical framework of this study. As the goal of this study is primarily to identify the internet users concerns in regards to sharing their personal information, whilst reading through the text, all the passage that appear to be connected to privacy concerns have been highlighted. Within the next step, after reading through the highlighted texts several times all the underlined sections have been given a code using the predetermined coding categories. Subsequently, all codes are reviewed carefully for refinement and infiltrate into final main categories. The categories are based on the theoretical framework factors, which are: impact of control on privacy concerns, impact of awareness on privacy concerns, as well as the motives of users in sharing their private information (Collection).

Subsequently, any text that does not fall into the pre-determine categories is distinguished to be analysed further, as if they should serve as a new category or a subcategory under an existing one. These newly labelled categories merged from data analysis shed light on the aspects that were scattered from the Internet Users Information Privacy Concerns theory and could help to enrich the theoretical framework for this study and ultimately help to tackle the research question (Hsieh and Shannon, 2005). The new category derived from the content data analysis has been connected to the concept of trust, which justifies the behaviours of users upon sharing their personal information. Consequently new concepts have been identified through the directed content analysis and united from three pre-determined categories and the new category to answer the research question and implicate to both practice and theory.

The interpretations of these findings will be fully discussed in chapter four.
3.6 The Description of the Research Setting

Kryast.se is a newly-created health promotion website that is open for use, both by individual persons and through company memberships. The website was constructed with the main purpose of making health activities more attractive for its users and for motivating them to engage in physical and health-promoting activities. As part of its services, this website also offers company memberships for employees that are willing to undertake fitness-related activities in order to promote their health. Furthermore, this website offers information about healthcare activities that helps its users to approach issues related to their health, physical activity patterns, and lifestyle from different perspectives. As indicated by its owner, this website tailors its products, services, and information materials that it offers in accordance with what its users want while also assisting them with their health problems and needs. In the case of when companies hire the services of this website with the aim of promoting a healthy lifestyle among their employees, this website makes available tools for the analysis of the company culture that workers are exposed to, while assisting the employees with dealing with their health issues. Therefore, depending on the kind of assistance its online users request, the team of personnel, experts and coaches who are working for this website looks for the solutions that are most likely to provide answers to the particular problems its users need addressing. The variety of ways in which online users of this website can find solutions to their health problems includes expert-written tips, video-recorded lectures and informative articles on topics covering general health and nutrition issues. Users of this website can also send private messages to its health-promotion experts in order to receive advice about their nutrition habits, fitness training, health promotion, and stress management. Other fields of expertise are being added to this website as it expands its pool of experts and therapists to whom it gives access.

Therefore, the website http://kryast.se/ offers to its customers a wide range of services related to health promotion. The website was developed by BeneVita, a wellness company that was founded in collaboration with Linnaeus University. Given that the services in which this website offers primarily focus on the promotion of health and wellness, this site offers not only freely accessible tools for raising health awareness among individuals, but also offers subscriptions to both corporate clients and individual employees through paid access to proprietary content in different health-related areas, such as stress reduction, healthy diets, and physical exercises. In order to motivate its users to adapt a healthy lifestyle, this website makes available links to fitness journals, weight-tracking applications, well-being indicators, and fitness blogs. Under the supervision of fitness coaches and nutritionists, the users of this website find assistance that helps them stay motivated. This website, thus, creates a health-promoting online environment as a basis, not only for individual wellness activities but also for promoting a better physical and psychosocial workplace climate. Since the success and the quality of customer service at websites highly depends on their ability to collect and analyse the personal information of their users (Son and Kim, 2008), it is critical for online service providers to earn the trust of their customers and to increase the attractiveness of the websites to more users. Thus, the present research hopes to make a valuable contribution to the ability of the BeneVita Company that has developed the website Kryast.se to address the needs and concerns of its users.
Information Sharing by Internet Users at a Health Promotion Webpage

The information shared by the users of the website that serves as the context for this study is primarily disclosed at their profile web pages. This profile information is relatively limited in its scope since it predominantly includes the full name, birth date, and website activities of the users. This basic personal information is accessible and can be easily shared with other users of this website. However, sensitive information from the privacy standpoint, such as the four last digits of the Swedish social security number, is never asked from the users of this website for security reasons. Furthermore, as it is illustrated in Figure 2, the users of this website can send private messages to its experts and coaches, and ask for their advice. The information that these messages contains can be accessed by the health- and fitness-related personnel of the website as addressees, as well as by the information technology staff members involved in the maintenance of the website. It should be noted that the aspects of managing this website, which are related to information technology, are taken care of by an external company. While the users of this website can share their health information either publicly or only with the website experts, such as nutritionists or psychologists or other experts, their sensitive information, such as social security
numbers, can be accessed independently by the information technology company which maintains and develops this website, as well by the company which owns and manages the servers where the website is hosted.

3.6.2 **The socio-demographic profile of research participants**

The following table presents the social, demographic and Internet use characteristics of research participants.

**Table 3 - The socio-demographic profile of research participants**

<table>
<thead>
<tr>
<th>No.</th>
<th>Age</th>
<th>Gender</th>
<th>Origin</th>
<th>Occupation</th>
<th>IT Background</th>
<th>Social Media Use</th>
<th>Internet Browsing</th>
<th>Website Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>27</td>
<td>Female</td>
<td>Foreign</td>
<td>A video editor</td>
<td>Considerable</td>
<td>Active User</td>
<td>Around the clock</td>
<td>3 times a weeks for about 1.5 hour per session</td>
</tr>
<tr>
<td>2</td>
<td>67</td>
<td>Male</td>
<td>Sweden</td>
<td>A self-employed businessman</td>
<td>No</td>
<td>Active user (Facebook or LinkedIn)</td>
<td>To a limited extent</td>
<td>30 minutes a week</td>
</tr>
<tr>
<td>3</td>
<td>45</td>
<td>Female</td>
<td>Sweden</td>
<td>A real estate consultant</td>
<td>No</td>
<td>Active user (Facebook or LinkedIn)</td>
<td>2 hours per week</td>
<td>30 minutes a week</td>
</tr>
<tr>
<td>4</td>
<td>28</td>
<td>Male</td>
<td>Sweden</td>
<td>A self-employed businessman</td>
<td>No</td>
<td>Active User (Facebook and LinkedIn)</td>
<td>8 hours a day</td>
<td>3 hours a week</td>
</tr>
<tr>
<td>5</td>
<td>33</td>
<td>Female</td>
<td>Sweden</td>
<td>A business Project Manager</td>
<td>No</td>
<td>Some Use (Facebook), active on occupation related websites</td>
<td>10 hours per week</td>
<td>2 hours per week</td>
</tr>
<tr>
<td>6</td>
<td>35</td>
<td>Male</td>
<td>Sweden</td>
<td>A computer software engineer</td>
<td>Considerable</td>
<td>Some use (Facebook and LinkedIn)</td>
<td>2 hours a day</td>
<td>1 hour per week</td>
</tr>
<tr>
<td>7</td>
<td>22</td>
<td>Male</td>
<td>Foreign</td>
<td>A refugee and a student of information</td>
<td>Considerable</td>
<td>active use of social media, such as Facebook and university-related</td>
<td>To a large extent, check emails</td>
<td>2 hours per week</td>
</tr>
</tbody>
</table>
3.7 Validity and Reliability

The Validity and reliability of a qualitative study ascertains the quality of a qualitative study. While the qualitative researchers, as opposed to quantitative researchers, are eager to embrace their involvement and are always present in the research setting to record an event before and after the changes (Golafshani, 2003), the results of both qualitative and quantitative researchers need to be tested to confirm its credibility. Although the credibility of a quantitative study relies on instrument construction, in qualitative study "the researcher is the instrument" (Patton, 2002, P.14), hence the validity and reliability of a qualitative study relies upon the effort of the researcher (Golafshani, 2003).

The result of a qualitative study is perceived as reliable, when the outcomes can endorse the concepts of Consistency, Dependability or Neutrality (Hoepfl, 1997; Golafshani, 2003). Similarly, in this study to the extent that the selection of research participants has not been biased with regard to their social and demographic characteristics, such as age or gender, the outcomes of this study can be considered reliable, as it is expected that this research setup can both be replicated in a different research setting and lead to consistent empirical findings regarding the selected research topic. In this respect, the detailed description of the website whose users have been interviewed is called to increase the reliability of the research results, since it makes a precise replication of this study possible with a different fitness- and health-related website.

In order to examine the validity of a qualitative study, the researcher seeks to establish confidence in the findings and how trustful these results are. For a qualitative researcher, it is essential to be able to generalize the results of the study to increase the validity or trustworthiness of his/her findings. Since this study will be making use of the qualitative tools of research, such as semi-structured interviews, the validity of the outcomes of this study will primarily rest upon a detailed description of the research procedures, the disclosure of full interview transcripts and an awareness of the primary researcher of the limitations that this research method puts on the possibility of making generalisations based on qualitative data. Given that the responses of research participants can be influenced by the nature of the website they make use of in the context of the research question that is being investigated, a discussion of this website as a research setting also supports the validity of the present study since it explains the responses that have been obtained during semi-structured interviews.
3.8 Ethical Consideration

The ethical issues that may arise during qualitative research can relate to the dimensions of scientific merit, participant protection and research integrity (Parse, 2001). During this study these dimensions of research ethics will be addressed in the following manner.

Scientific merit: In order to ensure the scientific merit of the study, the primary research will ensure that all the information collected in the process of this qualitative research will be properly cited and truthfully reflected, both in the form of interview transcripts that shall present the research data to the fullest extent possible and in the analytic elaborations on these data as a basis for the scholarly conclusions in which this study shall arrive.

Participant protection: In order to ensure the protection of the participants' identity and the informed participation of the interviewees in this study, the following precautions will be taken:

- The purpose of the present study is explained to all the participants before the start of their interviews, in order to prevent the disinformation of research participants and to ensure that informed consent for their participation in this study is obtained.
- All of the identifying and/or personal information gained from research participants in the course of their interviews are kept confidential, in order to ensure their anonymity. In the event that a research participant shall be willing to retain his or her identifying information in the interview transcripts, the interviewees are adequately informed of the possible risks of doing so for his or her privacy. Otherwise, I will act to the best of my ability to preserve the confidentiality of the research participants.
- The research participants are voluntarily participating in the collection of qualitative data via semi-structured interviews. As part of this process, research participants are informed that they can withdraw from this study at any point in the process of the interview. They are invited to give or avoid answering some questions at their will.
- Since the website kryast.se forms the context for this study, the owner of this website has provided me a user account in order to enable the observation of this website, as well as to provide a possibility for making a preliminary investigation. To make sure that the owner of this website is adequately informed of the purposes and instruments of the present research, I have explicated my research objectives, the contents of the research questionnaire, the rationale for the timeline and scope of this research, and what additional documents may be needed for the collection of qualitative data. Since this study seeks to explore the information privacy concerns from the perspective of consumers that make use of a website, the present research hopes to contribute to a more optimal management of privacy concerns that sharing personal information or giving public access to it can give rise to. Consequently, the expected outcomes of this study are translated into suggestions for the modification of the information systems management at this website so as to enable the alleviation of the possible privacy concerns that its users may have.
- The research questions that are used for the collection of qualitative data are carefully formulated in order to avoid offending research participants and to ensure that they do not lead to stressful situations at the time of the interviews.
- One of the data collection tools that is being used during the interview process is a voice recorder. However, to ensure that the data collection process takes place within the framework of informed consent, the decision over whether to make use of the
recording device is made in individual agreement with each research participant before the interview takes place.

- Integrity: The integrity of this study shall be ensured by means of clear, accurate, and truthful documentation of the results of the present research. Thus, throughout the research process, special attention is paid to maintaining the integrity of this study.
4 Empirical Findings

In this chapter, the major themes that emerge from the interview transcripts are presented. Among the themes that are determined through directed content analysis of the interview transcripts, the privacy concerns about personal information, the impact of trust, and interpersonal contact on these concerns, the importance of control over personal information and the perception of users versus the actual usage of their personal information can be identified. Furthermore, the qualitative data of this study indicates that the awareness of risks that Internet use involves has a relatively high impact on privacy concerns. At the same time, this study confirms that privacy concerns have a significant influence on information systems management, especially the limits of privacy protection on the Internet and the importance of trust for website management.

In order to answer its research question, this study has employed a qualitative research methodology and a research plan that earlier chapters of this study have elaborated upon. As specified in the main purpose of this study, the research approach that best suits the nature of this research subject is qualitative one. In addition, this study can be characterized as having a qualitative nature due to its being connected to human subjects and their personal opinions on a face-to-face discussion driven by an interview, about the information privacy concerns, and the impact of having personal information disclosed on the Internet.

Internet users share their personal information at commercial websites in order to receive specialist advice from coaches, doctors or therapists in return. This is also true in the case of this study. At their profile pages, the users the website kryast.se publicly share their personal information, such as their name, birth date, fitness activities, weight, email and training diaries. Out of the seven research participants that were interviewed, three of the website users have sent some private messages to their coaches. When it comes to the less sensitive information, the users seem to not have any serious privacy concerns about sharing it with others. However, except for one of the active users of the website, research participants who use this website generally refuse to share their psychological issues with the therapist. Excluding one participant who used a non-genuine name for the registration at this website, other users have provided their real names.

More specifically, this study has set as its aim to explore the privacy concerns of Internet users in respect to their decisions to share their personal information in a health promoting website. In order to explore that, I have used the website Kryast.se to figure out the privacy concerns of its users and the reasons for the emergence of these concerns in the context of the health promotion website. Using the website kryast.se as its empirical context, the present study has explored the privacy concerns that Internet users have, while using qualitative methodology for the collection of information on the subject of the present research. According to the strategy of data analysis that was selected for this study (Dye et al., 2000; Tracy, 2010), after the stage of the identification of general themes that emerge from the interviews conducted in the process of this research, this empirical data is then further analysed in this section.

All of the research participants claim that they have easy access to their personal information through their online account and can change it easily. One of the main criteria for identifying the dimension of the control over private information is previously knowing or being informed as a user of how to unregister from the website. All of the research participants did not have any idea
of how to unregister themselves from the website. They assumed that opting out of their subscription first or asking the company to remove their account information should be enough to keep it private. As the present researcher interviewed the information technology specialist, it was, however, revealed that the only way to opt-out from the website is to ask its administrator to do that.

During the interviews, users of the website sensed a threat to their private information and their control over it. It is possible to indicate the contradiction between the users' sense of control over the data, and what the technical and practical limitations to control over data that the IT staff members have highlighted. The findings show that users are unaware that they cannot unregister from the website by themselves. In one way or another, the participants decided to divulge their information because they trusted the experts and personnel who were working for the company behind the website.

Nevertheless, while the users of this website have assumed that they can opt-out from their subscription to this webpage with ease and no implications for their privacy, the interpretation of the qualitative findings of this study also indicates that the research participants were unsure with regard to the extent to which their information is kept confidential at this website. For this reason, a significant part of the interviewed users of this website have been found to not be willing to disclose information that they considered sensitive and private.

This apparent contradiction can be explained with reference to the effect that trust has on privacy concerns, as the empirical findings of this qualitative study show. While the majority of research participants have claimed that they are highly sensitive to the privacy of their personal information, they simultaneously had relatively little reservations about sharing their information on this website. The qualitative data of this research demonstrates that it is trust towards the managers, developers or experts of this website that have significantly reduced their privacy concerns. Lacking knowledge in the field of information technology, the users of the website selected as a context for this study have consistently cited trust as the main reason that they did not feel concerned about the privacy of their information. More specifically, trust, both to the website and to the commercial company that stands behind it, could be one of the reasons because of which the users of this website have underestimated the risks to the privacy of their personal information.

For Internet users, having control over their personal information that is shared in online environments lies at the heart of their privacy concerns and data security. With regard to sharing basic information such as name, email and birth date, all of the participants claim that they have an option to share it in public, or to restrict the access of others to only some of their personal information. However, the majority of participants were not sure if the information that they share on the website was only kept between themselves and their coach. Therefore, they chose not to share sensitive information, either privately or publicly, on the website. Only one of the research participants had full confidence that the information that was shared with the website experts was held in private.
4.1 The Impact of Risk Awareness on Privacy Concerns in Online Environments

A low level of privacy concerns about personal information: According to Participant 1, sharing her eating habits on the health promotion website does not raise privacy concerns, since they are perceived as distinct from medical information: “I think I’d rather be uncomfortable to share my psychological issue on the internet, but I don’t mind sharing my eating diaries and habits on the webpage.” There seems to be consensus among the users of this website that fitness-related information does not involve as many privacy concerns as would be for the sharing of information about one’s mental status. During the interview, Participant 2 has indicated that “as it comes to my mental status I would be more careful to write it down if not sure that it was only between me and my coach.” Similarly, Participant 4 considers the information about his fitness training as raising much less privacy concerns than would be for sharing information about any psychological problems he may have: “I have high expectations that [the information about psychological issues] is kept very confidential.” Similarly, Participant 5 did not perceive the sharing of her personal and fitness-related information, such as weight, as raising privacy concerns. It is possible that this attitude connects to the control that she has over the access to her personal information, since she did indicate that she does not share all of her sports training information. Her ability to choose what to share apparently adds to her sense of privacy, as Participant 5 explains: “Some of that information is not for everyone to see, and I can choose if I want to share it or not.” In other words, as the responses of Participant 7 exemplify, the privacy concerns that the use of the researched website may raise are balanced by the utility that making personal information accessible by other users of the website can bring: “I found the website interesting, as it allows you to get in touch with others with the same goals.” Moreover, as also follows from the interview with Participant 7, sharing basic demographic or social information appears to involve significantly less privacy concerns than sharing more psychological information would: “. From the beginning I was confident to share my information, such as age and sport goals, in the website, but when it comes to private matter such as psychological issues, I was a bit doubtful about sharing such information.”

A relatively high level of privacy concerns due to general risks of Internet use: These concerns have lead Participant 2 to install privacy-protecting software. Moreover, these privacy concerns have also lead Participant 2 to refrain from using his real name at the health promotion website kryast.se, in order to prevent intrusions into his private sphere, even though he has not personally been a victim of privacy infringements on the Internet. Likewise, Participant 3 not only takes precautions about what kind of information she shares on the internet, but also makes use of software programs that protect her privacy during Internet use. Participant 3 has reported that, when using social media websites, she “think[s] twice about what [she is] writing.” Nevertheless, in contrast to Participant 2, these general privacy concerns that social networking websites may raise have not led Participant 3 to abstain from using her real name at kryast.se. However, as emerges from the interviews with Participant 4, Participant 5 and Participant 6, these privacy-protecting software packages are likely to represent Internet firewall and virus protection software, as a standard practice among Internet users. With regard to the protection of his privacy, Participant 4 has stated that he takes standard precautions while using the Internet: “[A]s a user, I do not use particular software for protecting my privacy, but I do use the virus protection software as do most other internet users.” As Participant 5 has indicated, over the recent decades, regular Internet users have become relatively more exposed to risks to their privacy with the proliferation of social networking websites: "Now that there are lots of these websites in which
you can share information, I think it is more important to have more knowledge [about privacy risks] in comparison to 10 years ago." In other words, this study shows that privacy concerns and risks actively shape the manner in which Internet users approach websites, where they may be requested to share their personal information, as Participant 7 has indicated: “I always read through the privacy policies [of the websites I use] and check how secure [they are].” Furthermore, from the interview with Participant 7, it emerges that through their personal experience Internet users are highly aware of the risks they can be exposed on the Internet: “I am hoping the website is being monitored quite well-enough to spot those threats [to the privacy of its users that viruses or hackers pose].”

A low level of concerns about the website use, despite risk awareness: This willingness to share a real name may be due to the perceptions that Internet users may have about what kind of information they share and how it can be considered public enough so as not to lead to concerns about privacy infringement. Thus, Participant 4, did not see sharing his first and family names as a threat to his privacy. Similarly, Participant 5 had not made any inquiries about the privacy policies of the website kryast.se before her registration and did not have a sense of risk to her privacy while using this website. For this reason, Participant 6 has shared on this website, not only his name and fitness habits, but also information related to his medical problems and expecting that the website takes all of the necessary precautions to keep this information private: “My expectation [from the website] is of course to have all my personal information as confidential as possible.” At the same time, this attitude toward privacy is combined with a judgement that Participant 6 exercises about what information to share, which can be a consequence of general awareness about privacy risks that Internet use involves: “The online world nowadays is exposed to many risks which [one] cannot [easily] anticipate.” For this reason, for the relatively limited time that Participant 6 spends at this website has apparently led him to have a low level of privacy concerns: “[Out of] 10 hours a week [that I spend using the Internet], on this particular website, I spend half an hour weekly.” In other words, risk awareness that is acquired though the habitual use of the Internet equally affects the usage of the researched website that is deemed generally safe, as Participant 7 has indicated by voicing his indirect privacy concerns about the information that he shares with a psychologist that he contacts though the website: “I would like to keep such information private.”

A limited impact of privacy concerns about Internet use on the utilisation of the website: At the same time, it appears that, while registering on the health promotion website whose users are the subjects of this study, the consumers of its services do not inquire about the privacy policy of the website. Similarly, interviews indicate that the users of this website do not inquire about the control over their personal information that they may transfer to it, as the interview with Participant 1 indicates. In other words, despite the awareness of the privacy risks that website use can involve, research participants have not exhibited a pro-active attitude toward defending their privacy by asking for relevant information from the website, as Participant 2 has indicated. However, as the responses of Participant 3 clarify, there is a relatively limited impact of privacy concerns connected to Internet-usage, in general, on the patterns of information sharing and access at the health promotion website. Due to the nature of the information that the website collects from and makes available to its users, this is not perceived as a source of risk to privacy. Participant 3 has indicated that she does not think that “any harm [to her privacy] may happen on the website.” Similarly, Participant 6 did not recall having any specific privacy concerns connected to sharing his personal information, while registering for this website. In other words, as the
interview with Participant 7 shows, the users of the researched website have largely not checked its privacy policies during their registration.

4.2 The Impact of Personal Contact on Privacy Concerns

A high level of interpersonal contacts leading to a low level of privacy concerns during the website use: At the same time, this attitude towards fitness-related information is not shared among all research participants. Participant 3 has not disclosed her weight-related information at the health promotion website since she has a low level of trust in the future privacy of the information that she shares at this website: “I did not want to share my weight on the website, because I think it’s my private information.” Nevertheless, Participant 3, similar to the other research participants, also considers her physical training information as less private than other kinds of health-related information, such as information about psychological conditions. Participant 3 has clearly expressed that she has limited privacy concerns about the specific information that she shares at the website kryast.se: “I share training activities [...] and my expectations from my coach.” Likewise, Participant 4 perceives the website kryast.se as an internet resource where health and fitness information can be shared without a significant risk to his privacy: “Normally, I am using the [website to share my] training diaries, while putting [for public view the information about] my exercise [routines] with [an addition of] a few comments.” Since Participant 4 also engages in reading blogs by other users of this website, it is possible that the interpersonal dimension of this website diminishes privacy concerns in relation to its services and generates a sense of trust toward this website. Similarly, Participant 5 has cited that the social networking aspects of this website have affected her privacy concerns: “I think you can make some small groups and invite people to your group in activities, but I think other users can see it still.” In contrast to more general, fitness-related information, such as weight-loss activities or fitness goals, Participant 5 has cited a direct interpersonal contact as a precondition for sharing medical information, such as mental health-related information: “I am very comfortable to share activities and my goals in life, but I don’t think I will ever use the internet to share psychological issues and will leave it for face-to-face, or at least for the telephone.”

A high level of social contacts leading to a low level of privacy concerns: Additionally from the interviews, it has emerged that the trust in which the kryast.se website generates plays a crucial role in allaying privacy concerns that more impersonal information sharing websites are likely to lead toward. Participant 1 indicates that “I met the people working in the company and they are really kind and good people, and I don’t really think that they will misuse the personal information of users.” Similar to Participant 1, the willingness to share personal information at the health promotion website kryast.se seems to depend for Participant 3 on the interpersonal dimension of the context to which this information relates. As the reason for sharing the information related to her fitness activities at the website, Participant 3 has cited the presence of her friends during these training activities. Likewise, Participant 4 has stated in his interview that having an acquaintance with individuals that are involved with managing the health promotion website generates trust and the expectation that his personal information that is shared on the website is kept private. However, this effect of trust on privacy concerns can be broader, since, as the interview with Participant 7 shows, communicating with coaches and advisors on the research website can decrease privacy concerns, as the professional nature of the communication that takes place on the website seems to allay the initial fears about possible risks to privacy: “[A]s the
communication went by and turned out to be very helpful for me, I gained more trust to share more private matters with the specialists [at this website]."

A **significant impact of personal contacts on privacy concerns**: In a similar manner, Participant 5 has indicated that she has a relatively high level of privacy concerns vis-à-vis the website, since she does not have direct contact with either its managers or the coaches that she communicates with through this website: "[Even] if [my private information] were disclosed, I won't care that much. [In case] the information was so private for me, I would have never shared it on the Internet in the first place. And I am a bit conservative to share my private information on the Internet." Due to these generally significant levels of privacy concerns that Participant 5 has, she exercises judgement about what information she considers is safe to share on this website: "I choose what I share, even though I trust the system." In contrast, Participant 6 has indicated that personal acquaintances with the developers of this website has led him to have a high level of trust that his privacy will not be infringed upon: "I know the owner of the website and I trust him, but on other websites like Facebook, which are globally used, I provide a fake ID, as I don't trust these websites."

### 4.3 The Impact of Control on Privacy Concerns and Information Sharing

A **high level of control over personal information and its sharing leading to a low level of privacy concerns**: Furthermore, the website whose users were investigated was found to raise less privacy concerns than Facebook since it did not involve sharing personal sensitive information. In the words of Participant 1: ‘I heard that if you apply for a job, the company may look for you on Facebook […] and I have concerns about Facebook, [since] there are lots of news about it that it’s not secure.” However, this differentiated perception of the website kryast.se in comparison to other websites with a larger share of media exposure may not necessarily lead to a lower level of privacy concerns since Internet use, in general, is understood by the research participants as involving privacy risks. Accordingly, Participant 2 has said that "[a] use[s] of Internet […] [seem to involve] a possible risk of violating my privacy.” It can be inferred that this general awareness about privacy risks that Internet use is fraught with can also lead to broad privacy concerns, especially with respect to Facebook use and the risks of accessing banking services over the Internet. As the interview with Participant 7 perceived control over the access to personal information may assist with decreasing these privacy concerns, since he assumes that he can remove his sensitive information from the researched website if he chooses to: “Probably there should be a way to opt-out independently, isn't there?”

A **high level of perceived control over personal information leading to a low level of privacy concerns of website users**: Additionally, this low level of concerns about the privacy protection mechanisms of the website may derive from the access to and control over the information that the users of the website share. As the reason for a relative lack of privacy concerns that the health promotion website could raise, Participant 4 has indicated the manner in which information is managed at this website, which gives its users a sense of control over their shared personal information: “I can see all the information written and shared by me easily.” The ability to put in a request to the management of the website that it remove all personal information from its web pages and databases has given Participant 4 an assurance that his personal information is not at risk. Moreover, Participant 4 largely considers these measures as sufficient for the protection of his
privacy, and as a consequence of utilizing that website since at his request the data containing his personal information and a record of his online activities can be removed: "I think they will be removed." Likewise, Participant 6 has expressed his trust in the website in connection to the access to the coach that he has over the website, which has reduced his privacy concerns: "I think my coach will [help] me [deal] with my [privacy] concerns." Similarly, Participant 7 expressed the direct impact of his perceived control over the privacy of the personal information that coaches at this website obtain access to on the level of his privacy concerns: "I would have never shared my private information with my couch if it was not held private. I expect from my couch to not share this information with anyone else."

A significant impact of privacy concerns on online communication at the researched website: From the perspective of those who provide services through this website, such as fitness coaching, the issue of information privacy concerns clearly affects the manner in which the communication with the users of the health promotion website is handled. Participant 5, who is also a coach at kryast.se, has exhibited a clear concern about the privacy of the users of this website: "I make sure to log out from the website when I am done with messaging to ensure that their privacy is protected." In other words, despite the perceptions of the users of kryast.se, the information that they share with their coach, and possibly with other users, may be considered confidential. In this respect, Participant 5 has provided additional information on the precautions that he takes to protect the privacy of the users of this website and to prevent its infringement as a coach: "I never leave my computers without first logging out, and I have a long and secure password to my account." The actual experience of privacy infringement that some Internet users have, as did Participant 6 at another website, may also affect the general level of privacy concerns that particular websites raise, especially due to technical expertise that this involves. Participant 6 explicitly connects his privacy concerns, technical expertise, and Internet use: "[Since] my knowledge in [the sphere of] IT is limited, […] I do not generally trust the Internet.

4.4 The perceived versus actual Privacy Concerns

Furthermore, a comparison between the interview responses of the users of the website that served as the context for this qualitative study, and the information that the interviews with the members of the information technology support team of this website, brings to light the contrast between perceived privacy concerns and the actual risks of sharing private information. The interviewed information technology specialist has indicated that, for certain security reasons, when users cancel their registration at the website, it does not follow from this that their information cannot be shared with others afterwards. On the contrary, this personal information will be retained for an undefined period in the back-up systems or databases of the website. However, as this research indicates, the users of the website are not aware of this technical risk to their information privacy. Based on the responses of research participants, there is a gap between the expectations of the users of the website that their information will be kept confidential and that they will be in control of who, when, and how has access to their private data and what kind of precautions the website has implemented in order to protect these data from hacking or getting exposure.

These findings are corroborated by the perspective of website developers on the privacy concerns of the users of the researched website, since they highlight the objective limits to privacy
protection on the Internet. While the technical personnel and the developer team that operate this website echoed the privacy concerns of its users, they understand that these concerns are largely subjective and are not necessarily related to an objective assessment of the risks that habitual website use involves. Thus, they make efforts to limit the access to the sensitive information from the privacy perspective, such as payment information, by using encryption: “[W]e can [exercise] control [over who has] access [to sensitive information] through our server [that is protected by encryption mechanisms based on] SSH keys, so that [through these means] we can [determine] who can access the information.” At the same time, from the perspective of the developers of the website addressing privacy concerns also involves fraud prevention: “We have a fraud security system, so that when something inappropriate happens in the system, we will get a message that goes directly to developers who may decide [what] solutions [are necessary].” As interviews indicate, in order to protect the website against external threats to the privacy of its users, encryption mechanisms are widely used to manage this website: “[T]he [use of the] SSL encryption means that no one can interfere with the communication [taking place through the website] and read this communication, unless one has access to the system that only we and the administrator of the system [have].” At the same time, these precautions do not guarantee an absolute security of sensitive information: “What we can ensure is that we have taken all of the measures that we should be taking, such as the best [privacy protection] practices to protect our users’ information as much as we can.”

Nevertheless, the system oversight that the developer team has over the website, involves not only using the latest privacy protection software, but also monitoring user activity: “[I]f we need to investigate an account like for malicious activity, we have to go back to the back-ups and restore the account information from there.” However, the developers of this website acknowledge that their efforts to protect the privacy of their users may have a limited effectiveness. Additionally, developers indicate that privacy protection is an expensive undertaking since employing relevant computer experts increases the costs of running the website: “[W]hen managers want to save costs by speeding up the development too quickly or by using cheap development companies, they are not thinking about security first, but they are thinking about functionality first, which then leads to a chance of being more likely to get bugs into the system and getting hacked.” Even the developers of this website have to trust that other businesses which provide Internet hosting services take all the necessary precautions to prevent private information from being stolen: “Talking about the servers and its location, the application [exists in a] cloud environment, so basically we trust another company who hosts the information.”
Discussion: Privacy Concerns in the Context of a Health Promotion Website

This chapter opens the discussions on the finding of his study. Based on the analysis of the empirical data collected through interviews, the present study explores the impact of privacy concerns upon attitudes, perceptions, and practices of Internet users. Furthermore the implications of this study to the theory and practice is briefly discussed.

The aim of the present inquiry has been to explore the following research question:

1. What are the Internet users' information privacy concerns of a health promoting website?

The findings of this study indicate that there is a low level of privacy concerns among the participants of this research. In other words, this study has found a low level of concerns about the use of the researched website, despite a general awareness of the risks that Internet use involves. From the characteristics of the research participants that have explicitly expressed this position, it can be conjectured that a large extent of exposure to the Internet and its heavy use has enabled the predominantly younger respondents to learn how to deal with threats to their privacy on the web, such as through anti-virus programs, while raising their awareness of the threats to their privacy that the Internet poses. The respondents that have expressed this position tend to be a younger group between 22 and 35 years of age, to be heavy users of the Internet and to be spending approximately between 2 to 3 hours at the researched website, with the exception of Respondent 2 aged 67 and using the Internet and website to a limited extent. However further finding of this study shows that the limited impact of privacy concerns about Internet use on the utilisation of the health-promotion website seems to be independent of the age, gender, origin, IT expertise, social media use, Internet browsing habits or the website use patterns. These findings stand in contrast to a relatively high level of privacy concerns that almost all research participants have in relation to Internet use in general, with the exception of Participant 1 who is of foreign origin and has a high level of IT expertise and could be non-representative of the general research population. From the analysis of the empirical data it has become obvious that a general low level of privacy concerns related to the health promoting website is due to the fact that users have mostly decided to share non-sensitive information about themselves.

At the same time, given that this is a qualitative study; different dimensions of the Internet users' information privacy concerns have been identified as general tendencies that can be found in the interview transcripts. More specifically, after the interpretative data analysis of the qualitative data that this study has produced, it has become possible to identify thematic clusters that emerge from different responses of research participants. Nevertheless, the general correspondence of the thematic clusters that this study has found to the different dimensions of the framework of Internet Users' Information Privacy Concerns (Malhotra et al., 2004) provides it with qualitative support and a qualitative interpretation. Among the factors that could shed additional explanatory light on these findings it is possible to include a high level of interpersonal contacts, which leads, according to this study, to a low level of privacy concerns during the website use, despite a relatively high level of general Internet risk awareness. This study indicates that personal or social contacts with the representatives of the website represent a factor that has a significant impact on privacy concerns, disregards of social, demographic or Internet use characteristics of
research participants. Furthermore, the findings of this study indicate that the design of websites, a better support for their users and personalised contact with them can decrease the level of privacy concerns of their users, since it was found that a high level of control over personal information and its sharing leads to a low level of privacy concerns. In sum, this study indicates a significant impact of privacy concerns that users of the researched website have on their patterns of online communication both at kryast.se and more generally.

Furthermore it is worth to mention that, the findings of this study could be restricted to younger internet users, as the demographic profile of the research participants that have articulated this position shows. In mapping the demographic profile of the users of this study with the theoretical framework, the qualitative analysis reveals the fact that different conceptual dimensions of privacy concerns may have more salient expression in some demographic groups than in others. In this, the present research concurs with prior studies that have found that privacy concerns to some extend depend on age, since a greater daily exposure to the Internet that younger respondents tend to have is likely to sensitive them to the possible consequences that information disclosure on the Internet might have (Xu et al., 2008).

The empirical findings of this research provide support for the theoretical expectation that there is a positive connection between the perceived user’s awareness about privacy practices at a particular website, and a specific theoretical dimension of privacy concerns of Internet users, such as perceived control over personal information. Thereby this study interpretatively corroborates via qualitative means the conceptual framework of Malhotra et al. (2004) regarding Internet Users’ Information Privacy Concerns. The generally low level of privacy concerns that research participants have expressed follows from the perception of these Internet users that they can easily remove their personal information from the website. This dimension of awareness is primarily connected to users’ perceptions, rather than to actual practices performed on users personal information, and it is underlined by the interview findings that the information technology specialist of the website has made available. Research participants have indicated that they have the impression that, as users of the website, they had the ability to decide who can have access to their information, and to what extent. Despite this initial impression of these Internet users, the qualitative results of this study indicate that there are aspects of information privacy and limitations to its extent for which they are not aware. As the interview transcript with the information technology specialist shows, all of the technical personnel involved in the technical maintenance and development of this website can have access to the personal information of its users and even after unregistering from the website, users information will remain in the backup system. Thus, the fact that there are limitations to information privacy that the exigencies of information systems management impose is concealed from the users of this website. This qualitative finding indicates that the users’ awareness of privacy risks on the Internet are closely connected to their perceptions, and may be unrelated to the actual risks that sharing personal information on websites can involve for technical or organizational reasons. Therefore, the empirical findings of this study have additionally indicated that the theoretical framework of Internet Users’ Information Privacy Concerns can be used as a basis framework within qualitative studies aimed at identifying the privacy concerns of Internet users, however the application of this theory has not differentiated between the perceive privacy risks of users and the actual risks that users might be exposed to.
This study furthermore indicates that Internet users are likely to believe that they have control over their information, in that they have the choice to opt in/out whenever they want. However it is possible to infer from the findings of this qualitative study that its participants are unaware that only the manager of the website can register/unregister a user from the website. Hence, it is possible to indicate that users’ conviction in having control over their personal information is rather connected to their perception and far from the actual control performed over their users accounts.

Furthermore, given the gap between theoretical literature on privacy concerns and empirical studies that Smith et al. (2011) have described, this empirical study represents a qualitative exploration of the outcomes as a result of privacy concerns. Moreover, this research contributes to the exploration of privacy concerns from the perspective of other countries that have not been extensively studied so far, such as Sweden, the importance of which Bélanger and Crossler (2011) have stressed. Nevertheless, this study does not intend to bring comparative analyses with other countries that previous studies have conducted, however, the results of this study can be used to compare the results of the previous studies and witness any potential differences as a result of the cultural differences.

The empirical results of the present research clearly corroborate the study of Son and Kim (2008, p.504) that has indicated that information privacy concerns of website users represent one of the obstacles for their willingness to disclose rather sensitive information. Furthermore the qualitative findings of this study clearly support the study of Youn (2009, pp.391-392), according to which Internet users from different age groups can be expected to be widely aware of the digital footprint, such as on Facebook, that their online activities leave. In this respect this Swedish convenience sample have chosen not to share their sensitive information, such as psychological matters or credit card information due to high level of privacy concerns they discern in online environment. These findings corroborates the survey results of Madden et al. (2007, p.2) that, referring to American population, indicated wide-spread concerns about privacy and its possible breach.

The highly significant impact of trust on interpersonal contacts, privacy concerns and personal communication that this study has found corroborates the research of Oberholzer and Oliver (2005) that has indicated that the lack of trust may lead individuals to not use online services. Similarly, this research provides a qualitative validation of Nov and Wattal's (2009) study, according to which privacy concerns influence the readiness of individuals to share their personal information on the Internet. Thereby, this study has highlighted an additional factor that is highly likely to affect privacy concerns, in correspondence to the necessity of qualitative inquiries into privacy concerns of Internet users that Zukowski and Brown have highlighted (2007, p.203). Similarly, the findings of the present research indicating that a lacking direct contact with the managers or the coaches of the researched website has an impact on the privacy concerns of its users supports the study of Culnan and Bies (2003) according to which information privacy and related concerns are influenced by external factors, such as technological solutions to fill this gap.

Additionally, by showing that there is a limited impact of privacy concerns on Internet use, this research underpins the study of Stewart and Segars (2002) that has indicated that rational evaluations of the risks that Internet use involves are influenced by subjective perceptions and cognitions. Likewise, this research supports the studies of Van Slyke et al. (2006) and Angst and Agarwal (2006) that have shown that the relationship between privacy concerns and the
willingness to transact online is influenced by individual’s perception. Similarly, by demonstrating that the website users have a low level of trust in the future privacy of the sensitive information that they share, the present study indicates the interrelationship between collection of information from internet users and the concept of trust.

Also, by clearly showing the importance of control over personal information and its sharing, the present qualitative study has supported the conclusion of Caudill and Murphy (2000) that information privacy concerns are significantly affected by the ability of Internet users to approve, exit or ask for modification when sharing their personal information. Likewise, by clearly showing the impact of privacy risk awareness and Internet use patterns, this study supports the proposition of Phelps et al. (2000) that awareness affects individual concerns about information privacy.

As it was discussed by Malhotra et al. (2004), the collection component has two sides that must be taken into consideration. On the one hand, it is important to acknowledge the kind of information that is asked from users to share. On the other hand, what users expect to achieve in return for taking a risk by sharing their personal information. In the case of this study, the participants expect to receive prompt feedback responses from their coaches. However except one participant, other users have chosen to only share their non-sensitive information. Hence the findings of this study supports the notion of Control discussed by Malhotra et al. (2004) in that, Control is highly dependent on kind of information an individual is asked to divulge. For the case of health promoting website, the users are not yet convinced that they have sufficient control over sharing their sensitive personal information.

As opposed to the dimension of control, which is an important component of the theoretical framework of Internet Users’ Information Privacy Concerns, awareness is a less salient dimension of information privacy concerns (Malhotra et al., 2004). However, these two dimensions are interrelated. The more that an online user is unaware regarding the privacy practices that the website he or she makes use of applies, the less control the user has over his or her personal data and over the privacy of the information that the website accumulates (Malhotra et al., 2004). As was indicated above, during the interviews, the users of the website kryast.se have expressed their concerns about the degree to which they have control over their personal data. These privacy concerns could be the consequence of the lacking awareness that the research participants have about how their sensitive information can be accessed at, transferred from, and erased by the website.

The implications of the findings of this study to the theoretical frame work as well as to the practice is further discussed in this chapter.

5.1 Implications to Theory

In an attempt of literature review to find the most suitable theoretical framework that could match and satisfy the objective of this study, Internet Users’ Information Privacy Concerns appeared to be a convincible sound theoretical framework in online environments. The analysis results of this study proves the fact that the theory was the main lead to give shape to this study and tackle the objective. However new characteristics, uniqueness, findings could possibly arise from the results of one study, which may possibly help the future users of IUIPC theory in terms of what the current study has gained from this theory.
The interesting point about the Internet Users’ Information Privacy Concerns (IUIPC) theory is the fact that users of this application are free to use the theory as a first or second order concept. In other words the theory can be merged with other proof of concepts that could pursue the objective of one study. As a matter of fact, the result of this study indicates that a merged model of IUIPC with the concept of Trust could possibly better reflect the health Internet users privacy concerns, rather than solely relying on the theory’s main factors. Hence it’s recommended to future users of this application to study the IUIPC theory in general and compliment it with other aspects that are on the high focus of their studies. One point of view in favour of IUIPC theory and its dimensions of Collection, Control and Awareness is the perception of importance on each dimension. For instance Malhotra et al. (2004, P.339) suggested that dimension of awareness is not as salient as other two dimensions, and it’s perceived as a passive dimension than an active one. However as the results of this study suggests, awareness has played important role in determining individuals privacy concerns, in that high level of awareness of internet possible threads among participants of this particular website was a great motive to reveal their personal information.

In order to study the benefits and drawbacks of IUIPC model, its three main factors are worth to be further reviewed; Collection as first dimension of IUIPC model is highly rooted in disruptive justice of Social Contract theory, in the context of this study this means one decides to reveal his/her information if only the costs and benefits of such transaction outweighs the risks of the data getting exposed to internet violations. However the users of the health promoting websites have decided to share their personal information, even though they were not totally convinced if the benefits gained could offset the risk of personal information breach. The analysis result indicates that having trust to the website and its personnel could justify the website user’s behaviour. Hence it’s possible to indicate that trust has interrelationship with Collection dimension, which hasn’t been previously discussed by Malhotra et al. (2004) who have developed the IUIPC theory. In other words, trust could possibly explain why individuals share their personal information, even though they are not sure if such transaction is beneficial for them. On the hand, the users of krayt.se have chosen to not share sensitive information, such as their psychological issues. However the results of this study reveals the fact that users might engage to share their psychological matters, only if their trust is gained by assurance that collection of their private sensitive information is only beneficial for them and any malicious intentions to violate their private data is prohibited.

Control, as a second dimension of IUIPC theory, is rooted in procedural justice of Social Contact theory, meaning one views the sharing of personal information in online context as a fair process, if he/she is granted control over the data that is being shared. Yet the results of this study reveals the fact that there is a gap between perceived control and the actual control that one has over his/her personal data. While users of health promoting website believe that they have their own voice to opt in or out from the website, the actual practice to their data reveals the fact that they actually don't have the control to the manifested data, i.e. exit from the website. Hence it is possible to indicate that the theory of IUIPC has not differentiated between the perceived control and the actual control that individuals have over their personal data.

Awareness, as the third dimension of IUIPC theory is a passive and interrelated to Control dimension. Awareness is referred to a degree that individuals are aware of the possible threads that could happen to the data they share. Yet the outcome of this study implies that there is a difference between the perceived awareness among users of health promoting websites and the
actual awareness. As a result, the users awareness on the storage of their data was rather false and far from the actual exercise that is being done to their personal data. Nevertheless IUIPC theory has not marked the difference between actual awareness and perceived awareness. Furthermore as abovementioned, the results of this study debates if Awareness could possibly have its own voice as an important factors and is worth to be considered as an active dimension. However this would call for further research to highly focus on the importance of awareness in identifying the internet users privacy concerns.

Given the empirical and analytical course this study has taken, it is possible to indicate that the theoretical framework of Internet Users’ Information Privacy Concerns can produce worthwhile results also within the methodological design of qualitative research. Furthermore, it appears that the conceptual frame of reference that Internet Users’ Information Privacy Concerns represents has enabled this study to have theoretical rigour and consistency that it would have lacked otherwise. If another theoretical framework had been chosen, this study would have concentrated on different qualitative aspects of privacy concerns or Internet use. While this study could have approximated the validity standards of quantitative research methods, such as by increasing its sample size or by combining closed and open questions, this would also involve using a different theoretical paradigm, which would not necessarily be comparable to the design of the present study. The results of the study indicates the primary weakness of the selected theoretical framework which is devised to produce estimation of privacy concerns as a factor that representatively describes what holds true for a large number of individuals. This makes IUIPC into a macro-level framework of reference. What this research also highlights is that this approach has an inherent weakness in that it glosses over the fact that different factors of IUIPC do not necessarily cohere on the micro level of a single respondent. Closed questionnaires cannot assess these internal contradictions in privacy concerns because no place for unstructured responses is left. Additionally, as this qualitative study has highlighted, in different contexts internet users are likely to have different privacy concerns. A standardized questionnaire may not necessarily be able to capture that. From the qualitative perspective of this research, Internet Users’ Information Privacy Concerns can aggregate privacy concerns from large quantitative data samples, which enables examining the interrelationships of this variable with other factors, as a major strength of this quantitative approach. At the same time, as this study indicates, internal contradictions between different aspects of Internet Users’ Information Privacy Concerns become obviated, especially when unstructured verbal input, sensitivity to research context and inconsistencies in privacy and risk perceptions become deemphasized.

**5.2 Implications to Practice**

To warp up briefly, the findings of this study from practical level indicate that there is a low level of privacy concerns among the users of kryast.se. This could be explained based on the nature of the information that users share in this website. In essence, the users were quite confident to share the personal information that are perceived rather less sensitive, such as their name, sport habits, etc. However, when it comes to information that is perceived as more sensitive, such as psychological information or mental status, users are reluctant to participate in online communication. Naturally the users perceive releasing more sensitive information riskier than less sensitive information. This is in accordance with the study of Milne and Gordon (1993) in indicating that financial data and medical information are discerned as more sensitive
information than other information, i.e. age, sport habits, etc. Therefore this study fails to identify the privacy concerns of its users related to sensitive information, as only one user among the participants was convinced to share his mental concern with the coach. Accordingly it is possible to imply from users responses that there is generally high level of privacy concerns among internet users in sharing sensitive information. The reluctance among users to share sensitive information could be rectified by gaining individuals trust. Ultimately trust in an environment can mitigate the perceived risk among the individuals. Hence in order for kryast.se or any other health promoting website to expand its services and be able to obtain more sensitive information such as credit card data or providing psychological favour for its users, it is crucial to invest on techniques that could invite users to share sensitive information in such way that individual does not necessarily feel that his/her private information is being infringed. Exploration of such techniques that could possibly gain users trust require for researchers to study carefully users behaviour towards privacy violation topics, which is rather a sophisticated phenomenon that obviously based on the findings of this study online environment has not fully succeeded yet to achieve.

5.3 Role of Participants

The role of participant involvement in this study was to provide disaggregated, micro-level empirical evidence of privacy concerns that using a representative online services website is likely to raise. In other words, since the responses of the research participants in this study have not represented their degree of agreement with closed statements, but open-ended responses to theoretically targeted questions, interviewees responses have helped to shape the outcomes of this research to a significant extent. In fact participants have shed light to aspects of this study that would remain scattered otherwise. Hence, the objective of this study would fail to be met without the users commitment to express their perceptions upon usage of the website. The relatively small sample of research participants has allowed close attention to their privacy concerns. This study has indicated that, rather than being generalized, their concerns about sharing private information fall into specific thematic areas that have largely corresponded to different conceptual dimensions of Internet Users’ Information Privacy Concerns. By disaggregating this quantitative variable into its qualitative components, this study has indicated that, despite generally low level of privacy concerns about the utilization of the researched website that research participants have, they have a high level of awareness of Internet risks. This contradiction can likely to be explained by social contact with website-related personnel, perceived control over personal information and Internet safety precautions that they take, while using this website.
6 Conclusion

Based on the findings of this study, it is possible to answer the main question of this research in the following manner:

- **What are the Internet users’ information privacy concerns of a health promoting website?**

  This study has found a low level of privacy concerns about personal information among its research participants. This research has also found a relatively high level of privacy concerns, due to general risks of Internet use, a low level of concerns about the website use, despite risk awareness, and a limited impact of privacy concerns about Internet use on the utilisation of the website. This cluster of the Internet users’ information privacy concerns corresponds to the dimension of awareness (Malhotra et al., 2004, pp. 339-340). Furthermore, this study has found that a high level of interpersonal and social contacts leads to a low level of privacy concerns during the website use, which indicates a significant impact of personal contacts on easing the process of collection of users information. As well, this study has found that a high level of perceived control over personal information and its sharing leads to a low level of privacy concerns of website users. This indicates a significant impact of privacy concerns on online communication at the researched website. This cluster of the Internet users’ information privacy concerns corresponds to the dimension of control (Malhotra et al., 2004, p. 339).

Based on the present study it is possible to indicate that, despite to a relatively high level of privacy concerns that research participants have in relation to general Internet use, the researched website has involved a low level of privacy concerns that its research participants have evinced. This could only be explained by the type of information that users have decided to share, which are non-sensitive information. This research, however, also shows that the awareness about the privacy risks, that Internet users are exposed to, has allowed the interviewees to recognize that their privacy has not been at risk during their use of the researched health-promotion website. Given that a significant part of participants in this study are younger individuals who spend a significant part of their time on the Internet, the dimension of awareness that the theoretical construct of privacy concerns has apparently involves the ability of Internet users to differentiate between those online environments that are likely to put their personal information at risk and those that are not likely to lead to privacy concerns. Since wide Internet use is prevalent across all demographic groups, this study has, thus, found a low level of privacy concerns in relation to the kryast.se website. This corresponds to the awareness dimension of Internet Users’ Information Privacy Concerns as a conceptual framework that Malhotra et al. (2004) have proposed.

Among the antecedent factors having a significant impact on privacy concerns during the website use, it is possible to include interpersonal contacts, website-related social contacts and personalised contact with website representatives as variables that have led to a low level of privacy concerns among research participants. These findings correspond to the second order conceptual framework of Malhotra et al. (2004) for the measurement of Internet Users’ Information Privacy Concerns in that they indicate that receiving additional information about individuals behind the website that collects the personal information of research participants can
significantly reduce the level of privacy concerns they have. Familiarizing with the individuals behind the website, getting prompt feedback from the website authorities or having exposure to the privacy policies of the website that details actual practices being performed on users personal data would help to gain users’ trust. Trust has been also highlighted by Malhotra et al. (2004)’s second order model. Hence it is highly recommended to the health website owners to base the design of the website on transparency and trust and inform users about the actual practices acted on their personal data through means, such as publishing privacy policies. As a matter of fact, the results of this study proves the fact that gaining users trust would certainly engage them to share confidently their personal information. Furthermore, such privacy policies could also help to raise awareness among users, which could work as inspiration for users to share their personal information.

This study has also found a significant negative impact of control over personal information and its sharing on the level of privacy concerns that the website users have. All in all, this study offers qualitative support for the salience of different dimensions that the conceptual framework of Internet Users’ Information Privacy Concerns has (Malhotra et al., 2004).

Additionally, this study indicates that different conceptual dimensions of privacy concerns may be significantly connected to particular age. While a general level of privacy concerns among the users of the researched website does not seem to be significantly related to socio-demographic characteristics of research participants, a high level of Internet risk awareness has been found among younger interviewees. In contrast, this study tentatively shows that Internet users with a low level of information technology expertise are likely to have lower levels of privacy concerns about websites collecting their personal information, if they have higher levels of interpersonal contacts with their representatives. Furthermore, this research tentatively suggests that the negative impact of control over personal information on privacy concerns can be stronger among active Internet and social media users.

Thus, on the basis of this qualitative research it is possible to confirm that the concept of Internet Users’ Information Privacy Concerns can be applied as a interpretative research framework in the field of information systems studies, as Bélanger and Crossler (2011, p.1020) have indicated. In line with the construct of Internet Users’ Information Privacy Concerns that Malhotra et al. (2004) have developed, this study has analysed interviews with its research participants, in an effort to show that this theoretical framework, despite that it is deeply rooted in quantitative studies, is also suited for exploring why a person would decide to share one’s personal information online, by using a qualitative approach.

Besides, from the theoretical point of view, this study has generated some unexpected results. Malhotra et al. (2004) developed the Internet Users’ Information Privacy Concerns as a first order model and merged it furthermore with other aspects, as such trust to evaluate the casual model against the study objective. Hence it was expected theoretically to get exposure of trust as a separate dimension. Indeed the users have chosen to share their personal information, even though they were not totally convinced if this data exchange has any benefits for them, which stands in the heart of collection dimension. According to data analysis, the high level of personal contact, consequently high level of trust to the website and its personnel was a substantial motive for the users to share their information on the website. The unexpected result from the course of this qualitative data analysis yields that trust has interrelationship with dimension of collection specifically. Therefore it is possible to indicate that online users decision in sharing their personal
information can be influenced by how fair they perceive this data exchange and/or level of trust they have to the other party. Furthermore as discussed in section 5.1, the qualitative results of this study implies that there is a difference between the perceived Control or perceived Awareness and actual Control or actual Awareness individuals have towards the usage of their personal data. As the data analysis suggests that the users perceptions toward the control they have over their data is different from the actual exercise on their data. As such, the users believe they can exit and remove their personal data in their convenience time, however in reality opting out and removing the data from the website is controlled by the owner of the website. Also the users perception of being highly aware of the exercises on their data does not fully comply with the actual exercises that could perform on their data. On the basis of the results of this study, the Internet Users’ Information Privacy Concerns theory has not differentiated between the perceived and actual Control and awareness, which calls for further research to investigate.

6.1 Further Research and Practical Implications

The analysis conducted in this study calls for further research into information privacy concerns from a qualitative perspective. Despite a significant number of quantitative studies on the subject of the privacy concerns of Internet users, a qualitative grasp of how trust vis-à-vis social networks is established, how general awareness about risks inherent in Internet use and the control that web interfaces give to their users affects privacy concerns each remains under-researched areas. Therefore, the following suggestions for further research can be made:

Since the theoretical lens for this study was the concept of Internet Users’ Information Privacy Concerns, it can be suggested for further application used as a second-order theoretical framework for other studies. While the findings of this study suggest that the framework of Internet Users’ Information Privacy Concerns can be used to capture the privacy concerns of Internet users in the case of the website Kryast.se, it is highly suggested to future researcher of this theory to consider combining this theory with other theories or concepts that could meet the objective of their study, since this framework provides a structured conceptual framework for exploring the privacy concerns of Internet users. Hence, I suggest for future studies to explore users’ privacy concerns based on the second-order factor theory of Internet Users’ Information Privacy Concerns.

Given that the main purpose of this study was to explore the privacy concerns of Internet users in the context of health promotion websites, it could be highly insightful to conduct a research into the privacy concerns that individuals may have when using websites on which their users publicly share information related to their mental health and psychological problems.

The findings of this study suggest that explicit privacy policies, which address Internet user concerns, are necessary for websites to decrease the level of privacy concerns that they may raise and help to raise awareness among users. However, the impact of privacy policies that different websites implement upon the attitude of their users, in general, and on their privacy concerns, in particular, has not received sufficient research attention as of yet. Therefore, it can be recommended that more studies into the IS management aspects of privacy concerns on the
Internet be carried out in order to explore the manner in which these policies can be developed to protect the privacy of Internet users.

Even though this discrepancy might cause Internet users' to have privacy concerns, these concerns can be effectively addressed by informing users about the manner in which their sensitive data are handled through relevant confidentiality policies. At the same time, since it is only the information technology personnel who have full control over the information disclosed by the users of the website, the lacking awareness of these users of the risks to their privacy and their limited control over their personal information indicates that they underestimate the actual privacy risks that Internet use involves.

As a result of this study, it is possible to make the following practical recommendations based on the literature review and the analysis presented in this study.

IT specialists can integrate into their websites a wider range of user-friendly tools that can gain users trust and ensure them that their privacy is protected, or to determine how the privacy issues are handled by websites. Given that Bélanger and Crossler (2011) have claimed that the theoretical lens of Internet Users' Information Privacy Concerns could be used to reflect the privacy attitudes of website users, as well. Therefore, taking a qualitative approach with the adapted theoretical framework, I found that companies can affect the security perceptions of the users on their websites by integrating the dimensions of Internet Users' Information Privacy Concerns into their information systems design. This in order to decrease privacy concerns about online transactions of their users.

As this study demonstrates, through the use of qualitative data that I have collected using interviews, I also propose that commercial websites should include privacy policies in their information materials, which is the simplest way to share with their users how their information is being collected from them, and how they can have control over their information and be more aware of the actions that can be done to their private information. Software engineers should probably pay more attention to the actions that cause the privacy of their users' information to be jeopardized. Also, project managers should adjust their business objectives according to the concerns of website users, which in this case is to protect the privacy of their information. Privacy policies should be managed through the direction of users' expectations and how the company is putting a premium on what users expect from them. By making user's expectations one of their priorities, companies and their websites can diminish the privacy concerns of their websites' users.
References


Appendix I: Interview Questions

Guiding Questions for Semi-Structured Interviews

1. What sort of information does the website collect from its users?

2. Do you have access to all of the information that users share on the website? Do you have access to those pieces of information that users share privately with the psychologist or the nutritionist?

3. How do you monitor the information flow on the website?

4. Since your department is dealing with sensitive data, such as credit card information, what sort of software do you use to ensure that your users’ security and privacy are protected? How do you protect users’ information privacy, such as their credit card information? Does the software guarantee protection of users’ information and their privacy? Can you ensure that their personal information is protected?

5. Do you think that there may be any sort of potential for attacks that may violate the privacy of users’ information? If yes, what do you suggest to prevent those incidents?

6. In the event one of the users wants to remove his or her information from the website upon registration, does this scenario really delete this information from the website’s database?

7. How much have you heard or read during the last year about the use and potential misuse of the information collected over the internet?

8. Do you perceive this exchange of information a fair deal? If yes, how would you justify that? If No, why would you still share your personal information, despite the risks associated to exchange of information?
Appendix II: Interview Transcripts

Participant 1

This research participant is 27, female, comes from Poland, works as a video editor, has considerable background in information technologies, actively uses social media, such as Facebook and LinkedIn, browses the Internet around the clock, and uses the website kryast.se on average 3 times a week for about 1.5 hour per session.

1. What sort of information have you been asked from the website to share?

It's been a while that I have been registered on the webpage. I was asked for my name, birth date, if I would like to have my status visible, statistics of my training, weight, or to have my diary visible for others. They asked me if I want to share my content on my webpage with my coach or exerciser; however, I don't have a coach, actually. (She works with the website to make the announcement (coaching videos). She was picked for this job. The videos were about stress, motivation, diet, and exercise. She can see that the website works and the manager gives her access. And she uses it. She has an option to share her statistics with others or not.)

2. What sort of activities do you usually share on the website and what are your expectations from your coach on the website in return?

I share my gym activities, my diary, and eating diaries and if I have completed my goals and my plans.

They have this good service on the website to give you statistics or motivational bars that says, for instance, you have finished 80% of your goals, and many other activities such as how many calories I have burned, how many kilometers I have run, etc. and I expect it to give me physical charts and diagrams. I don't really expect much more than this. I think it's fun to be a user to see how much I have progressed on my activities. Generally the page gives you BMI (Body Mass Index).

Me: Will you share nutrition or psychological information with the nutritionist or the psychologist?

I think I’d be rather uncomfortable to share my psychological issues on the internet, but I don't mind to share my eating diaries and habits on the webpage.

3. Have you ever been concerned or felt doubtful to put your personal information or share an activity because you felt it may threaten your privacy or the requested information is too personal?

No, not really. Not on the webpage. I had concerns on other webpages. The sort of information that I share on the webpage is not too personal, and I don’t mind sharing it.

Why were you concerned on other webpages?

I think you won't be surprised if say that the other webpage is Facebook. I heard that if you apply for a job, the company may look for you on Facebook. That’s why I don’t share too much
information, and I have concerns about Facebook and there are lots of news about it, that it’s not secured and they have too many users.

Me: So, are you saying that one of the main reasons for a webpage to be unsecured is that the page has too many users? So, if in 5 years kryast.se has 5000 users, you will trust the webpage less?

No, I don’t think so.

4. How easily do you have access to any information related to you on the website?

I think I have easy access, and I think I can click on my profile and change my name, last name and password and if I want my activities be visible on my profile. I have never had any problem with accessing and have control over my information.

5) Are you aware of the possible threats that may violate your privacy by misusing your personal information?

I think I am aware, and I can understand if someone can misuse my information for other purposes.

How likely do you think these sorts of incidents may happen in kryast.se?

Given the fact that the webpage is not really famous yet, I have pretty good confidence that it’s not going to happen. And I met the people working in the company, and they are really kind and good people and I don’t really think that they will misuse the personal information of users. I think the reason mainly is that I trust the people who work in the company.

Do you think that you have sufficient knowledge about the risks of sharing personal information and the privacy issues that it causes?

I like to think so, but I have to say no, because I am not using it every day, I have sufficient knowledge about that but you will never know.

6) Do you have an option to opt-out (exit) or delete your written activities in case if you want to unregister yourself from the website?

Actually, I haven’t checked that (she checked while speaking). I am not quite sure. Now as I can tell, I cannot.

Me: So, what would you do if you want to remove your information from the website?

Well, I will probably start by deleting my written activities on the website. As for unregistering from the website, I will call the company and ask them how to unregister myself. Because, after all, my account was made for me by the manager and I didn’t make my account and he made it for me.

When registering on the website, have you been informed about your options as to unregister or remove all of your personal information on the website?

I don’t think so. No, I was not. Since this account was made for me.

Me: When you were registering on the website, did you happen to read any sort of privacy policies?
No, I did not. And I cannot see any privacy policy now.

Me: Do you think that when you want to remove all of your information from the webpage, just by simply unregistering yourself, that it will be removed?

Yes, I hope so.

7) How much have you heard or read during the last year about the use and potential misuse of the information collected from the internet?

I have heard quite a lot and read news about that from Facebook and the WikiLeaks situation.

Do you use any sort of particular software to ensure your privacy protection?

I don’t think I use any external software in privacy protection. I have passwords for everything, but I don’t think that will be counted under software. So I don’t.

8) How many hours in a week do you spend on the internet?

I am online 24/7, unless I am on vacation, otherwise I work by computers all of the time.

And how active are you when you use kryast.se?

Three times a week.

9) Do you use your real name as your real ID on the website? If not, can you explain your reasons?

Yes, I do.

10) Have you ever experienced any sort of improper invasion to your privacy on other websites?

I mean, if you leave your account open, others may come and change your password or name or birthdate. It happens on Facebook to me. It’s scary that someone can do that.

If I were the manager of the company, what would you recommend to protect your private information?

I would recommend that they would make sure that all of my personal information is always visible to me, and that I am the person in control of my personal information, so I won’t feel unsafe. Also, to make notes on the page about how their policy works, and that’s all.

11) Do you perceive this exchange of information a fair deal? If yes, how would you justify that?

If No, why would you still share your personal information, despite the risks associated to exchange of information?

Yes, I think so, but having faith in the future of this website and the whole concept behind it is a great motive to be part of it.

Participant 2
This research participant is 67, male, comes from Sweden, works as a self-employed businessman, has no background in information technologies, does not actively use social media, such as Facebook and LinkedIn, browses the Internet to a limited extent, and uses the website kryast.se on average 30 minutes a week.

1. What sort of information have you been asked from the website to share?

I am not sure if what I write on the website is shared with others!? But I volunteer to write down my weight and my goals with my training. I also write how many hours I spend with each activity. I never opt to share information that is too detailed on the webpage. I would rather keep it as high level as I can.

2. What sort of activities do you usually share on the website, and what are your expectations from your coach on the website in return?

See above.

I did actually expect some sort of feedback more than the monthly report.

3. Have you ever been concerned or felt doubtful to put your personal information, or share an activity, because you felt that it may threaten your privacy, or that the requested information was too personal?

Not really for the sort of information I share today on the website.

But of course, as it comes to my mental status I would be more careful to write it down if I was not sure that it was only between me and my coach.

4. How easily do you have access to any information related to you on the website?

I easily get access to statistics about my activities as far as training is concerned. I have not tried to use information regarding my mental status.

5. Are you aware of the possible threats that may violate your privacy by misusing your personal information? How likely do you think these sorts of incidents may happen in kryast.se? Do you think that you have sufficient knowledge about the risk of sharing personal information and the privacy issues it can cause?

I am aware of that, and it could be the reason for my reluctance to share information as far as my mental status. It’s not that I mistrust Kryast.se, but just have the feeling that this type of information is not anything that I want to share.

All use of the internet and other forms of information seems to have a possible risk of violating my privacy. I guess one has got to trust some channels and keep to them.

6. Do you have an option to opt-out (exit) or delete your written activities in case if you want to unregister yourself from the website? When registering on the website, have you been informed about your options to unregister or remove all of your personal information on the website?

Good question! I have not asked or been informed of that.
7. How much have you heard or read during the last year about the use and potential misuse of the information collected from the internet? Do you use any sort of particular software to ensure your privacy protection?

I have heard quite a lot about it and am now more careful as far as it goes for using i.e. Facebook or my internet bank. I have also installed software.

8. How many hours each week do you spend on the internet? And how active are you when you use krayste.se?

Not very much these days. Maybe a couple of hours? And then I include krayast.se!

9. Do you use your real name as your real ID on the website? If not, can you explain your reasons?

No, and the reason is to avoid anyone "looking over my shoulder."

10. Have you ever experienced any sort of improper invasion to your privacy on other websites?

No, not as far as I know.

11) Do you perceive this exchange of information a fair deal? If yes, how would you justify that?

If No, why would you still share your personal information, despite the risks associated to exchange of information?

Well, it’s a good question. Depends on the future of the website. I do believe in the moto of the website and I hope the owners can follow what they promised. I do also trust the owners, as I know one of them personally.

Participant 3

This research participant is 45, female, comes from Sweden, works as a real estate consultant, has no background in information technologies, makes active use of social media, such as Facebook and LinkedIn, browse the Internet for about 2 hours per week, and uses the website kryast.se on average 30 minutes a week.

1) What sort of information have you been asked from the website to share?

I have chosen not to share all of the information.

Me: What sort of information do you not want to share on the website?

My goals, my weight, and things like that.

Why?

Because these are private, and I do not want to share them.

Me: So, are you saying that when it comes to the Internet that you are more conservative to share your information because you do not trust the Internet to share your information?

Yes!
2) What sort of activities do you usually share on the website, and what are your expectations from your coach on the website in return?

I share training activities, goals with my training. My expectation from my coach is that I do that.

Do you know that in the near future there will be psychologist or more active psychologist on the website? Do you think that by that time you will share some sort of psychological issues with the psychologist through the internet?

If it will be very private information, I do not think I want to share it.

3) Have you ever been concerned or felt doubtful to put your personal information or share an activity because you felt that it may threaten your privacy or the requested information is too personal?

Yes, because I did not want to share my weight on the website, because I think it's my private information. I think that's my privacy.

Me: So, you didn’t share your weight because it’s your private information?

Yes.

Me: For sharing sports activities, why do you think you share those activities? Do you think your privacy is violated when sharing other activities, such as sport or training activities?

Because I train with some of my friends here, this is not so private.

Me: What about me, as a member of a website that often comes to the website and checks your activities, I mean an anonymous person can also see your activities, are you concerned about this?

Maybe I don’t want to share my goals with you.

4) How easily do you have access to any information related to you on the website?

Me: Adding to the question: For instance, you have shared an activity a few weeks ago, can you have access to that information?

Yes.

Me: Other information, when you sign-in to the website, do you have access to those, as well?

Yes.

5) Are you aware of the possible threats that may violate your privacy by misusing your personal information?

I don't have/know, but I don't think any harm may happen on the website.

Me: So you are saying that you have general knowledge about possible threats that can violate privacy?

Yes.
How likely do you think these sorts of incidents may happen in kryast.se?

I don't know. General information cannot harm me; if it would have harmed me, I wouldn't put them on the internet.

Do you think you have sufficient knowledge about the risk of sharing personal information and the privacy issues it can cause?

Yes, I think I have.

Can I ask if your occupation is related to informatics or any related area?

No, I work with economy.

6) Do you have an option to opt-out (exit) or delete your written activities in case if you want to unregister yourself from the website?

I haven't tried that. I know I can delete the exercises.

But let's say that today you decided that all of the information about you wanted to remove all of the information about you on the Internet, and remove all of your footprints?

I would call Gustaf. I will call him, and ask him to do it for me.

Do you think that when he deletes all the information from the website, that all of information will be deleted, generally?

I hope so, I trust Gustaf.

When registering on the website, have you been informed about your options to unregister or remove all of your personal information on the website? Like some notices or privacy policies?

I don't remember if I read something about it.

7) How much have you heard or read during the last year about the use and potential misuse of the information collected from the internet?

I have read a lot about it. And I use all the privacy protection that I can. I share my information only with my friends. When I write on the Internet, I think twice what I am writing. And she has a Facebook account

Do you use any sort of particular software to ensure your privacy protection?

Yes, the regular ones that can be found on the web.

8) How many hours each week do you spend on the Internet? And how active are you when you use krayst.se?

Maybe one hour a day. Not too much, and on krayst.se I log in once or twice a week.

If I were the manager of the company, what would you suggest for privacy protection? If you think the privacy protection is sufficient then you don't need to answer this question.
I don’t know if I have any. Maybe if there was an option as if I want to share with others or not, on registering on the webpage, I could choose if I want to share my training or things like that. It will be better if in the future, for all activities, there will be an option to share it with others or not. If I could make a choice to share with others for each activity, that would be good.

9) Do you use your real name as your real ID on the website?

Yes.

10) Have you ever experienced any sort of improper invasion to your privacy on other websites?

No, I haven’t.

Thanks for your time and answers, which will be helpful for my research. If you would like to add anything, mail me and I will be glad to have it in my mind. I will send you a draft soon.

11) Do you perceive this exchange of information a fair deal? If yes, how would you justify that?

If No, why would you still share your personal information, despite the risks associated to exchange of information?

It depends on how they provide the services they promised. At this point, in conjunction to the data I have been sharing, I can say I am happy with my decision upon sharing the information that I shared. I also trust the website and think they have “good will”. But I am still not quite confident with sharing psychological matters.

Participant 4

This research participant is 28, male, comes from Sweden, works as a self-employed businessman, has no background in information technologies, makes active use of social media, such as Facebook and LinkedIn, browses the Internet for about 8 hours a day, and uses the website kryast.se on average 3 hours a week.

1 and 2) What sort of information have you been asked from the website to share? What sort of activities do you usually share on the website and what are your expectations from your coach on the website in return?

Only name, family name, and email address.

As a manager, in the long-term, we may ask for credit card information as well, but for now the credit card information has not been requested.

Normally, I use the training diaries to put in my exercise with a few comments, and sometimes I read blogs.

My expectations: To be honest with you, right now I don’t have many expectations because I use the coach section.

Me: In the future you are going to present a psychologist on the website as well, and you are going to share psychological issues, what are your expectations from him?

I am expecting to keep it very confidential; I have high expectations on that.
Me: Since you know that the developer of the Stand AB Company and the people who are in charge of the IT section of the company can have access to all of the information of users, how do you feel about it? Eg. They have access through the private messages between users and their physicians or coach.

They have access, and I am expecting to keep the confidentiality of my information.

3) Have you ever been concerned or felt doubtful to put your personal information or share an activity because you felt that it may threaten your privacy, or that the requested information is too personal?

No, because of faith, trusting the people working with the website, the IT section, and manager.

4) How easily do you have access to any information related to you on the website?

Well, it is easy to have access through the information I shared, but if in case I want to print it, I have to copy-paste it, thus if I want to print the statistics related to my daily activities, I cannot easily print it, but access is ok. I can see all the information written and shared by me easily.

5) Are you aware of the possible threats that may violate your privacy by misusing your personal information?

I haven’t thought about threats.

How do you think these sorts of incidents may happen on the website?

I don’t think it will ever happen.

Do you think you have sufficient knowledge about the risk of sharing personal information and the privacy issues it can cause?

No, I don’t think I have sufficient knowledge about that.

So, for example, if you put your personal information on the website and then you want to remove it, yet the people working in the company still have access through this information since they have back-ups? If in case you want to remove all of your information from the website, and you will unregister yourself from there, do you think that will be sufficient?

Yes.

6) Do you have an option to opt-out(exit) or delete your written activities in the event that you want to unregister yourself from the website?

The only way to unregister yourself from the website is to ask the admin, and he will delete it. So I can’t delete my account by myself and I need to contact the manager, and then he will do it for me.

Me: So by only removing the account, do you think all the activities are being removed from the website?

I am not 100% sure, to be honest (I think they will be removed).
7) How much have you heard or read during the last year about the use and potential misuse of the information collected from the Internet?

I heard quite a lot, especially on FB.

No, as a user I do not use particular software for protecting my privacy, but I do use the virus protection software as most of other internet users.

9) Do you use your real name as your real ID on the website?

Yes.

10) Have you ever experienced any sort of improper invasion to your privacy on other websites?

I had an incident on FB yesterday. A girl accepted me as her friend on my FB page, but I did not add her.

11) Do you perceive this exchange of information a fair deal? If yes, how would you justify that?

If No, why would you still share your personal information, despite the risks associated to exchange of information? I do think it's fair and as I said before I trust the people who work behind this webpage, as I know the manager and I am sure they will do their best to put my interest before theirs.

As a coach:

1) What do you think in the near future that the patients or users will share with you?

At the moment, I coach things like eating habits, working out, sleeping well, not stressing, and how to calm down and find mindfulness.

Me: In the near future, will your users have an option to share private messages with you in order to get consultations, etc?

We already have it, and users have been sending me information. I make sure to log out from the website when I am done with messaging to ensure that their privacy is protected.

Me: What do you do as a coach to guarantee your trainees/adopters privacy?

I am very careful when I am reading the messages, so that no one can be in the room and I never leave my computer without logging out. I have a long and secure password to my account.

Me: Do you think as a coach that, in the future, any sort of privacy violations may happen on the website?

Well, I don't think so, and I will do anything I can to prevent it.
Participant 5

This research participant is 33, female, comes from Sweden, works as a business project manager, has no background in information technologies, makes use of social media, such as Facebook, and is active on occupation-related websites, browses the Internet for about 10 hours per week, and uses the website kryast.se on average 2 hours per week.

1) What sort of information have you been asked from the website to share?

Personal information such as name, age, and email address, but also there is some information that you have to put there, and there are some to choose by yourself to share, like weight or height, and things like that.

Me: Is there any information that you share privately with your coach and in which no one else has access?

Some of that information is not for everyone to see that I can choose if I want to share it or not. And also, there are some activities that I can share, like sports activities that I can choose-everyone else can see it or not. For example, I am going for 30 minutes of running, and so it’s somehow like Facebook that you can update your status about your activities.

Me: And do you have this option to limit the audience of your shared information?

I don't know, really. Because when I got my account I was pregnant and didn’t have time, but I just recently began using the website. I think you can make some small groups and invite people to your group in activities, but I think other users can see it still.

2) What sort of activities do you usually share on the website, and what are your expectations from your coach on the website, in return?

Running, activities, also I have some goals like my weight to get back to before pregnancy weight-which I chose to see it myself and also my coach, that is information that I do not share with other people.

Me: Expectations?

I expect for my coach to see if I am reaching my goals, and that I am doing exercises and to give me feedback and responses. Or, if I am not active for a period of time, the coach sends me a message to check on me.

Me: But how about privacy concerns? For instance, if you share some psychological matters with the therapist, what do you expect?

I don't know if I will be comfortable to share this sort of information. I am very comfortable to share activities and my goals in life, but I don’t think I will ever use the Internet to share psychological issues and will leave it for face-to-face, or at least for the telephone.

3) Have you ever been concerned or felt doubtful to put your personal information or share an activity because you felt that it may threaten your privacy, or the requested information is too personal?
Not at this website, and not yet, but maybe if it will be more developed and psychological questions are asked, then I will be. And the reason that I think this has not happened until now is because the website is more concerned with healthy activities. I have no problem with that.

Me: But as you mentioned, you have also shared information, like your measurements, privately, so maybe you do not want me to have access to this information?

I trust the system and the manager, but also I would never write and share anything that I would never in my life want others to know. You know that on the Internet things can always happen. Even if the information that I share privately with my coach were to be disclosed, then I won’t care too much. Even if the information was so private for me, then I would have never shared it on the Internet in the first place. And I am a bit conservative to share my private information on the Internet.

4) How easily do you have access to any information related to you on the website?

I don’t know, because I became recently an active user on the website. When I log in, I can see activities that I did, but I cannot answer this question for sure.

5) Are you aware of the possible threats that may violate your privacy by misusing your personal information?

I think I have some knowledge I know it may be threatened, but I don’t know much about it. I think that’s why I share information on the internet, like kryast or Facebook on a low level, but I choose what I share. For instance, I would never put a naked picture of myself or my baby because I would never know who may see that picture. So I choose what I share, even though I trust the system.

How likely do you think these sorts of incidents may happen in kryast.se?

I don’t think these sorts of incidents can happen now, but in the future maybe when it grows bigger.

Do you think you have sufficient knowledge about the risk of sharing personal information and the privacy issues it can cause?

I have some general knowledge. Now that there are lots of these websites where you share information, I think now it is more important to have even more knowledge in comparison to 10 years ago.

Me: And if I was your coach, what would you suggest to me in terms of protecting your information?

I think that when you get to log in some security regulations would be good to guarantee that the information will be kept only in this company’s database. I think they are doing the security part of the website as much as they can. But if they can get help from people who are educated in these matters (privacy policies).

6) Do you have an option to opt-out(exit) or delete your written activities in the event that you want to unregister yourself from the website?
The day that I want to remove all my information from the website, I will log-in and try to remove most of my information by myself as much as I can, and if there are things that I cannot remove, then I will ask the company. I am not concerned about that, though.

Me: Do you think that by unregistering yourself from the website that your information will be deleted?

Yes, I think, hmmm, I don't know. But maybe it's still somewhere there, I can never know. But I know that on Facebook they own your information even after unregistering.

When registering on the website, have you been informed about your options to unregister or remove all of your personal information on the website?

No.

7) How much have you heard or read during the last year about the use and potential misuse of the information collected from the Internet?

I have not thought about it much, but you hear about it every now and then. I cannot say that I heard it very much. But I don't think about it much, and if I hear about it then it's from the news and they have made some research about it.

Do you use any sort of particular software to ensure your privacy protection?

I use F-secure software.

8) How many hours each week do you spend on the Internet?

Since nowadays we have the Internet on our cell phone, if I collect all of the time that I spend surfing on the Internet, then it is probably two hours.

And how active are you when you use krayst.se?

An hour monthly, because I do not use the website to connect with other people. I use it when I do activities. And if it had more functions, then I would use it more. And it's not like you check every now and then.

Are you a member of Facebook?

Yes.

9) Do you use your real name as your real ID on the website?

Yes.

10) Have you ever experienced any sort of improper invasion to your privacy on other websites?

No, not that I am aware of.

11) Do you perceive this exchange of information a fair deal? If yes, how would you justify that?

If No, why would you still share your personal information, despite the risks associated to exchange of information?
It’s really hard to answer this question. (interviewee answers after few seconds of thinking) I would say it’s a win-win situation. The website helps me to gain my fitness goals and be in touch with society as a mother. In the same time, we are the very first users of the website who can help the owner to get well-known in online environments.

**Participant 6**

This research participant is 35, male, comes from Sweden, works as a computer software engineer, has considerable background in information technologies, makes use of social media, such as Facebook and LinkedIn, browses the Internet for about 2 hours a day, and uses the website kryast.se on average 1 hour per week.

1) What sort of information has the website collected from you?

General information like my contact details and sports habits.

2) What sort of activities do you usually share on the website, and what are your expectations from your coach on the website in return?

My sports habits. I once posted a medical problem that I had on the website. My expectation is, of course, to have all of my personal information as confidential as possible, and to respect my privacy.

How often do you refuse to give out the information requested from you by the website because you think it’s too personal?

20%, but I have the option not to share this information on the website.

3) Have you ever been concerned or felt doubtful to put your personal information, or share an activity because you felt it may threaten your privacy?

I do, and I have chosen not to share this information.

4) How easily do you have access to any information related to you on the website?

I think quite easily, the website is user-friendly and easy to have access to my personal info.

5) Are you aware of the possible threats that may violate your privacy by misusing your personal information? How likely do you think these sorts of incidents may happen in kryast.se?

I am not sure if I am aware of all of the possible threats; the online world nowadays is exposed to so many risks that I cannot anticipate all of them.

6) How do you define the possible practices that your coach might do with your personal information?

I think my coach will mainly support me with my concerns and personal information. He might use that information for my benefit, or at least that is how I would rather think.

7) Do you have an option to opt-out (exit) or delete your written activities in the event that you want to unregister yourself from the website?
I think I do have an option to opt out of the website. I am not that technical, but if you are referring to sign out of the homepage, if this is done through the normal process like other webpages, then I have the option to log out. For deleting my information, I am not sure if it will stay within the system or if it is erasable.

When registering on the website, have you been informed about your options to unregister or remove all of your personal information on the website?

I cannot recall.

8) How much have you heard or read during the last year about the use and potential misuse of the information collected from the Internet?

I have heard a lot about misuse of information on FB and other social media websites.

Do you use any sort of particular software to ensure your privacy protection?

I have normal anti-virus software on my laptop.

9) How many hours a week do you use the Internet? And how active you are with using this website?

Ten hours each week, on this particular website I spend half an hour weekly.

10) Do you use your real name as your real ID on the website? If not, can you explain your reason?

Yes I do. I know the owner of the website and I trust him. But on other websites like Facebook, which are used globally, I provide a fake ID, as I don't trust the websites.

11) Have you ever been the victim of what you felt was an improper invasion of privacy?

My Facebook account was once hacked and used, and it was terrible experience. As I said, my knowledge in IT is limited, therefore I do not generally trust the Internet.

12) Do you perceive this exchange of information a fair deal? If yes, how would you justify that?

If No, why would you still share your personal information, despite the risks associated to exchange of information?

I think it's fair in a way that we both benefit from this. I benefit the website by growing the webpage. But I must say as this is a newly created website, I am keeping my faith to the owners and their promises.

Participant 7.

This research participant is 22, male, comes from Iraq, is a refugee and a student of information technology, has considerable background in information technologies, makes active use of social media, such as Facebook and university-related social networks.

1) What sort of activities do you usually share on the website and what are your expectations from your coach on the website in return?
My name, age and eating habits, goals within certain period of time.

I found the website interesting, as it allows you to get in touch with others with the same goals.

2) Is there any information that you share privately with your coach and in which no one else has access?

I do actually, I have been in contact with a psychologist of the homepage which are being held privately between me and the specialist. I would like to keep such info private.

3) Any expectations from your advisor?

Of course, as mentioned I would have never shared my private info with my coach if it was not held privately. I expect from my coach to not share these info with anyone else and engage himself to support me with personal advices.

4) How did you decide to share your personal concerns privately with your couch?

When I signed up myself for the website and I read through I found this option to share my private psychological or nutritional habits with experts and then I started the communication with the specialist.

5) Have you ever been concerned or felt doubtful to put your personal information or share an activity because you felt it may threaten your privacy or the requested information is too personal?

In general yes, you hear every day a privacy linkage of users information in internet, so I always read through the privacy policies and check how secure the homepage is.

6) How about kryast.se?

I was also at the beginning doubtful to share my private matters. From the beginning I was confident to share my info such as age and sport goals in the website, but when it comes to private matter such as psychological issues, I was a bit doubtful to share such info. But as the communication went by and turned out to be very helpful for me, I gained more trust to share more private matter with the specialist.

7) Why were you concerned on other webpages?

My personal mailbox was hacked once, as I opened an email which contained virus and I was exposed to the virus. But as I have good anti-virus on my laptop I got the alarm and changed the password right after.

8) How easily do you have access to any information related to you on the website?

Quite an easy access, it’s a modern, user-friendly website, enabling users to have easy access to their info, like many other social pages.

9) Are you aware of the possible threats that may violate your privacy by misusing your personal information?
I am aware of those threats that we hear in the news happening, as I am also student in IT, I know a bit about security and how to protect myself against those threats. However everyday there is a new hacking tricks which we are not much aware of. So it's really hard to say if I am totally aware of all possibilities.

10) How likely do you think these sorts of incidents may happen in kryast.se?

Well at the moment kryiast.se has not become much worldwide, but I believe as soon as the webpage is more well-known, it's more exposed to danger. Also I am hoping the website is being monitored quite well-enough to spot those threats.

11) Do you think that you have sufficient knowledge about the risks of sharing personal information and the privacy issues that it causes?

I think I do have the sufficient knowledge.

12) Do you have an option to opt-out (exit) or delete your written activities in case if you want to unregister yourself from the website?

Hmmm, good question. I am not sure. Probably there should be a way to opt-out independently, isn't there?

13) So, what would you do if you want to remove your information from the website?

I would start with looking into the homepage, and checking the help in the website. If nothing ofund I will write an email to the support team.

14) When registering on the website, have you been informed about your options as to unregister or remove all of your personal information on the website?

No I was not.

15) When you were registering on the website, did you happen to read any sort of privacy policies?

No, I did not. I don’t think I have seen one, good point! All social pages should have one.

15) Do you think that when you want to remove all of your information from the webpage, just by simply unregistering yourself, that it will be removed?

Yes. I hope so, but not sure if that’s the case.

16) How much have you heard or read during the last year about the use and potential misuse of the information collected from the internet?

Yes, I have done a paper on that actually for university last semester.

17) Do you use any sort of particular software to ensure your privacy protection?

I use pro-avast anti-virus which has been good to my laptop till now!

18) How many hours in a week do you spend on the internet?
I would say quite a lot, my studies are all with computer and I check my emails and student account at least twice a day.

19) And how active are you when you use kryast.se?

Well depending on the notification emails I receive, I can be more active. Let's say in average 2 hours per week.

20) Do you use your real name as your real ID on the website? If not, can you explain your reasons?

Yes, I do.

21) Have you ever experienced any sort of improper invasion to your privacy on other websites?

Yes, as I mentioned my email was once hacked and since then I am very careful with opening he emails, also I never leave my email signed-in when I’m in public, i.e. University library.

22) If I were the manager of the company, what would you recommend to protect your private information?

I would recommend to invest more on the security of the website. Especially if the plan is to have it more advertised in the internet, it should for sure be more secure for the sake of protecting the users info.

23) Do you perceive this exchange of information a fair deal? If yes, how would you justify that?

If No, why would you still share your personal information, despite the risks associated to exchange of information?

Well, it’s hard to say. I am happy with the results I’ve seen so far. At the beginning I was a bit hesitant to share my psychological issues with psychologist, but I have seen the results and I am quite satisfied. So I am happy now that I chose to share my private information, but I will be disappointed if my private data will be breech out. but I took this risk as I gained trust throughout the online communication I had with my couch.

**Interview with one of the developers of the website**

What sort of information does the website collect from its users?

Basically, we collect basic information like first name, last name, and birth date. Besides that, we collect information about working out. This is the fitness tracking application, so that could be some sensitive data because this can be perceived as personal information to users including weight, current training goals, so these are the main things that we store, we do not store credit card information in the system.

But as far as I heard from the owner of the company, some of the users may now, or in the future, have some sort of transaction each month. In that case, what would you do to protect users’ privacy?
In that case, we would probably offer an external payment system that means that we would only store what kind of payments they have, such as PayPal. So by using an external payment system provider, we never have to store payments, only storing that the payment has been received which in not the credit card information. So, we are really trying to avoid storing credit card data on our site, and would only be storing if the user has been paying or not.

So, the only sensitive data that you think that you are getting from users are about health mentality, and the working out situation?

Yes, and also some private messages between users and their coach, which could be sensitive data (doesn’t have to be).

Does the IT section of your company have access to all of the information that users share on the website?

Yes, we have full access to all information. It’s not easy to get users’ information, but it’s possible. So, if we want to, we can get the information, but not the credit card information, because that won't be stored in our system, all the data and private messages that users share.

So what you are suggesting is that in the future when users need to pay for the services they get from the website that the only source who will have access through the credit card information are PayPal people?

Yes, PayPal or any service provider whom are specialized in credit card data, and we try to avoid it as long as we can.

Do you have access to all of the information that users share on the website?

We have access to every piece of information in the system that resides in our system, so that means everything from the users’messages.

How many people in your company have access to this information?

Basically, it’s the developers; this is about 3-4 people, and we can control the people who have access through our specific server, called SSH key. So, basically we can say who can access this information.

Do you have access to the information that users share privately with their psychologists or the nutritionist?

Yes, we have.

How do you monitor the information flow on the website? Could you explain more about your question?

Yes.

I meant that when users put information on the website, how do you monitor this information technically?

We are not doing any information monitoring in the system.
Basically, now we are in the testing phase. We have some fraud security systems so that when something wrong happens in the system, then we will get an error message that goes directly to developers who may decide the solutions. So each time something goes wrong, they decide about it. Basically, we have set up some kind of rules that these messages can be in this format. So when someone wants to manipulate the system, then we get the messages. So when users do the things in the area of the rules, we don’t do anything, but if they cross this line, we acknowledge this through messages.

Since your department is dealing with sensitive data, such as credit card information, what sort of software do you use to ensure your users’ security and privacy protection?

When we save the data, we encrypt the data. We use the framework which is well-known for its security matters, so it has all of the protection against Internet attacks, like XSS protection. Do you know about that? It’s cross-site encrypting; if someone wants to inject malicious code into the system, then we can protect the system.

So you use encryption software?

Yes, part of the website. But with the things that we want to display and people who are willing to read, we can have one-way encryption, which means that we need to be able to encrypt and decrypt it, so that we need to store the key, and so it’s not totally secured. But the SSL encryption means that no one could interfere with the communication and read the communication unless they have access to the system, such as only us and administrators of the system.

I was given an account by the manager of the company, but my question is can everyone be registered on the website? So someone with malicious intention can register himself on the page?

I may have to ask my colleague this question, but I don’t think there’s a way for that.

So everyone on the website should be registered on the supervision of the manager of the company?

Right now we are not able to make new accounts for new users, but (other colleague says this in Swedish), and he continues: basically, there is no way of creating new accounts by yourself right now. You have to be invited to the page, that’s one way of ensuring a secured information flow.

But as the IT specialist, do you think that there could be a possibility that a person who has the knowledge of hacking or attacking websites can be capable to do so?

No. I don’t see that possibility right now. Every system can be hacked in some ways, but I think we have used all the security applications that we could use in order to secure the system.

Does the software guarantee the protection of users’ information privacy? Can you ensure that their personal information is protected?

Ensuring is such a strong word. What we can ensure is that we have taken all the measures that we should be taking, like the best practices to protect our users’ information as we can. So if someone wants to get the information from the system, they will be forced to hack it very hard! Probably some kind of surrogacy explosion, or like something that could affect a lot of website at the same time, like a big bug in a well-known system. So basically, to have a look at the webpage,
you need to have an account to see what’s behind the walls, and I think it’s really unlikely that a hacker will be invited to the system. But there’s a possibility that someone could get his/her account hacked. So I think that this might be more likely than hacking into the system itself, then there will be a problem.

How likely could it be that a user can hack the system or have access to the private messages?

As a user, it will be easier to hack through the system instead of those who are not. But I still think it would be very hard.

Do you think that there may be any sort of attacks on this website that people’s information could be violated? If yes, what do you suggest to prevent those incidents, even though it has been covered already?

What we do to prevent those kinds of issues is that we keep our systems updated by using the latest security software and patches, and we use the framework called robin rales and they are very good at protecting users. So, every time that there’s a security breach, everyone gets an email and information about how to update the system. That’s very good.

In case one of the users wants to unregister his/her information from the website, does it really delete all of the information from the website’s database?

One way of deleting a user is when they are immediately unregistered, then the whole information about that account is gone immediately. But we have one way of restoring it, that’s because we keep having backups from the system. So if we need to investigate an account, like for malicious activity, we have to go back to the back-ups and restore the account information from there, but within the system it is deleted. But if we want to have access through the unregistered user, we have access to them for up to 40 days.

How much have you heard or read during the last years about the use and potential misuse of the information collected from the Internet?

There have been many large sites having lots of troubles; I see that as really big trouble because the users cannot trust the website entirely. So basically, sometimes we enter all kinds of sensitive information and they are publicly exposed later. For example, a blogging website was hacked and a porn site was hacked, and the chat logs of the website were leaked to others, so then everyone could see what has been said in the chat rooms which were very private information, but they had no security at all. I think the main reason was that someone wants to save money during development, and they hired bad developers who didn’t care about the security, and they forgot the chat password protect the directory where the chat logs were stored, and you don’t need to be a hacker to do that. But what I see is the big problem is when customers or managers want to save costs by speeding up the development too much or using cheap development companies. They are not thinking about security first, but they are thinking about functionality first which leads to a stronger likelihood to get bugs into the system and be hacked.

So, do you think that these sorts of incidents may happen in kryast.se within the next five years?

If the website system is not updated regularly, then it will be hacked someday. But since we always upgrade the system, then I don’t think that it will be an issue in the future because security is one big part of the development.
Are you suggesting that the privacy of the users will be protected in the next five years?

Yes, even more so than now. With companies like Facebook, I don't think that they are taking it really seriously. As you may know every time that you get an update from the Facebook application, it’s something more than you automatically share with your friends and data on your public timeline that is accessible to people that you might have not expected. So I don't see any problem for now, but I think that as people grow more and more aware then we won't have the problem.

What will happen if kryast.se decides to give the responsibility of the IT section of its website to another company?

I really don't know, it's a hard question!

Talking about the servers and its location, the application lives on a cloud environment, and so basically we trust another company who hosts the information with the server facilities, and they have a great deal of security just to enter the building. It would be so unsecured to have the server here in this building because people are coming here every day. So we trust another company.

So the database of the company and the information of the users is stored in another company?

Yes, nowadays the normal way to do it is to have a specialized hosting company, which of course they have a lot of employees that can access through the information potentially. And they have access through the private messages between users and their physicians as well, that can be an interesting touch to your topic.

So do you think the potential misuse possibility of user's information can be done by people from this company and from the server hosting company?

We, in this company and employees who work in the server company, have access through this information, of course we won’t. And if we hire someone and give access to him/her, he/she could do the same thing. For us, we are so accurate to choose our people, but I cannot say exactly about the Server Company. There is one Server Company that works in Växjö, but there is also a company that is hosting krat.se in eastern Sweden.

And do you have to work under specific laws?

No, but the server company probably is and they are responsible for the data that they store in their system for the certain amount of time, but I am not really expert about that.