Miikael Lehto

USER PERCEPTIONS ON THE PRIVACY OF HEALTH INFORMATION

UNIVERSITY OF JYVÄSKYLÄ
DEPARTMENT OF COMPUTER SCIENCE AND INFORMATION SYSTEMS
2016

ABSTRACT

Lehto, Miikael
User perceptions on the privacy of health information
Jyväskylä: University of Jyväskylä, 2016, 96 p.
Cyber Security, Master's Thesis
Supervisor: Salo, Markus

Activity trackers have become more common and they enable the collection of information about an individual's physical activities and health. Traditionally a person's health information was stored in the health care provider's databases, but now health information is being stored in multiple services. This change has brought new ways to utilize technologies in the area of health and wellness, but at the same time questions have surfaced concerning the privacy of an individual's information. This thesis discusses a study regarding the user perception on the privacy and sensitivity of health information collected with wearable devices. The study also explored the user perception on health information sensitivity in general, and their willingness to share such information to other parties. The study used qualitative research approach to collect empirical data and used themed interviews as the tool. Ten individuals who currently use an activity tracker were interviewed for the study. Privacy calculus model was used as a theoretical lens through out the study, which also guided the analysis of findings. The study found that individual's don't perceive the information collected by wearable devices as private or sensitive, but as general information. On the other hand, information in health records is considered to be very private and sensitive and much more specific, as they include additional personal information in written format. The study found that individuals do not share information from their wearable devices on social media. Users are willing to provide their information to doctors if it can be used in their health care. Individuals are also willing to provide their information for medical research and allow the device manufacturer to use the information for improving products and services. Even though the individuals are willing to share their information for different purposes, they had privacy concerns and worried how their information is used. They were concerned how information might spread to other parties and how it might be misused. Privacy concerns did not have a significant impact on the majority of the users as they accepted these risks. This thesis expands the previous research by presenting a new context in which privacy calculus theory can by utilized. Research findings have benefits for practice as the information collected with activity trackers can be utilized in the future for health care and research, since users are willing to share it.

Keywords: privacy, health information, activity trackers

TIIVISTELMÄ

Lehto, Miikael
Käyttäjien kokemus terveystietojen yksityisyydestä
Jyväskylä: Jyväskylän yliopisto, 2016, 96 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaaja: Salo, Markus

Aktiivisuusrannekkeet ovat yleistyneet ja ne mahdollistavat tietojen keräämisen henkilön fyysisestä aktiivisuudesta ja terveydestä. Henkilön terveystiedot ovat perinteisesti olleet vain terveydenhuollon tietokannoissa, mutta nykyään terveystietoja tallennetaan moniin palveluihin. Tämä muutos on tuonut uusia teknologian hyödyntämismahdollisuuksia terveyden ja hyvinvoinnin alueella, mutta samalla on herännyt kysymyksiä henkilöiden yksityisyyteen liittyen. Tämä tutkielma käsittelee tutkimustuloksia, joissa selvitettiin käyttäjien kokemuksia aktiivisuusrannekkeilla kerätyn terveystiedon yksityisyydestä ja arkaluontoisuudesta. Tutkimuksessa selvitettiin myös tutkittavien ajatuksia terveystiedon yksityisyydestä yleisesti ja heidän halukkuudestaan jakaa heistä kerättyjä tietoja eri osapuolille. Tutkimuksen empiirinen aineisto kerättiin käyttämällä laadullista tutkimusmenetelmää ja työkaluna teemahaastatteluita. Privacy calculus -mallia käytettiin tutkimuksen teoreettisena viitekehyksenä, joka myös ohjasi tuloksien analysointia ja luokittelua. Tutkimus on tehty haastattelemalla kymmentä henkilöä, joilla oli aktiivisuusranneke tutkimushetkellä käytössä. Tutkimuksen tuloksena ilmeni, että henkilöt eivät pidä aktiivisuusrannekkeiden tietoja yksityisinä tai arkaluontoisina vaan yleisinä. Toisaalta henkilöiden mielestä heidän lääkäreillä olevat terveystietonsa ovat hyvin yksityisiä ja arkaluontoisia. Lääkäreillä olevat tiedot koettiin yksityiskohtaisiksi, koska ne sisältävät henkilökohtaista tietoa myös kirjallisessa muodossa. Tutkimuksessa selvisi että käyttäjät eivät jaa aktiivisuusrannekkeidensa tietoja sosiaalisessa mediassa. Käyttäjät olivat valmiita antamaan keräämiään tietoja lääkärille, mikäli niistä olisi hyötyä heidän terveydenhoidossaan. Käyttäjät olivat myös valmiita antamaan tietojaan lääketieteelliseen tutkimukseen sekä antamaan laitevalmistajan käyttää tietoja tuotteiden ja palveluiden kehittämiseen. Vaikkakin henkilöillä oli yleisesti valmius jakaa tietoja eri käyttötarkoituksiin, he kuitenkin kantoivat huolta yksityisyydestään ja tietojensa käytöstä. He olivat huolissaan tietojen mahdollisesta leviämisestä toisille osapuolille ja niiden väärinkäyttämisestä. Huoli yksityisyydestä ei kuitenkaan vaikuttanut merkittävästi suurimpaan osaan käyttäjistä, vaan he hyväksyivät nämä riskit. Tämä tutkielmaa laajentaa aiempaa tutkimustietoa esittämällä uuden kontekstin, johon privacy calculus -teoriaa voidaan hyödyntää. Tutkimuksen tuloksista on käytännön hyötyä, koska aktiivisuusrannekkeiden keräämiä tietoja voidaan tulevaisuudessa hyödyntää terveydenhuollossa ja tutkimuksissa, koska käyttäjät ovat valmiita jakamaan niiden tietoja.

Asiasanat: yksityisyys, terveystieto, aktiivisuusrannekkeet

FIGURES

TABLES

TABLE OF CONTENTS

1 INTRODUCTION

The growth of activity trackers, smart watches, and other wearable devices has been robust in the last years (Li, Wu, Gao, & Shi, 2016). These technologies enable the collection of information about a person's physical activities and their health, such as heart rate. These technologies together with mobile applications and cloud services have created a new way to measure and store information about personal health. Prior to these technologies, most health related information was exclusively stored in the hospital or health care provider's system, but now this information can be stored in a variety of services.

This change has brought new problems and questions concerning the privacy of individuals' information (Klasnja, Consolvo, Choudhury, Beckwith, & Hightower, 2009). There is a threat to the privacy of an individual when their health information is accessible by new parties that are not part of the traditional health care value chain. For these reasons it's important to better understand how these new technologies impact privacy and how the technologies can be better utilized in health care.

The goal of this research is to study user perceptions of health information collected with activity trackers and similar technologies. The study explores the privacy and sensitivity of health information and compares them to different categories of information. The purpose is to understand the privacy concerns that individuals have about the collection and storing of their health information in different places. Understanding these perceptions can be helpful when organizations need to determine the type of information they collect and the technologies they develop. It's also valuable for organizations to understand privacy concerns that might limit disclosure of personal information in order to find ways to mitigate these concerns (Gao, Li, & Luo, 2015).

Another area of the study explores the user's willingness to share information that they have collected with their wearable devices. These devices enable individuals to share their information on social media or to friends. Alternatively, the collected information can be used for medical research or product development. The study explores these aspects from the user's perspective to better understand the perceptions of individuals. It's important to learn about the individual's perspective concerning the use of these technologies in order to

have products and services designed with the user in mind (Lee & Kwon, 2015). Adoption of wearable devices in health care requires further understanding of the user perspective.

1.1 Understanding user perspective of privacy

In information systems research there have been several studies on privacy and its different aspects. The central themes found in these studies are the impact of control, trust, and information type to information disclosure. Control deals with the individual's ability to choose how information about them is collected and used. Prior research has found that control has a significant impact on the privacy concerns individual's experience (Patterson, 2013; Xu, Dinev, Smith, & Hart, 2008). These privacy concerns can be at least partially mitigated by giving the individual the perception of control over their information (Dinev & Hart, 2003).

In connection with control, another way to impact privacy concerns is through trust. Individuals are more willing to provide their information to an organization that they trust (Culnan & Armstrong, 1999). Prior research also shows that trust can be developed by organizations being transparent about their information practices and providing users with control (Sheehan & Hoy, 2000). The type of information that is requested also impacts privacy concerns and information disclosure. Prior research has found that health and financial information are considered the most sensitive (Andrade, Kaltcheva, & Weitz, 2002; Phelps, Nowak, & Ferrell, 2000). These studies show that information relevance and context are important to the individual when they evaluate information sensitivity.

Prior research has identified that there needs to be further investigations regarding the impact of control and trust to the individual's use of Internet services, and the associated privacy concerns (Dinev & Hart, 2003; (Xu, Dinev, Smith, & Hart, 2008). This thesis investigates how these aspects impact privacy concern in the context of wearable devices and the associated Internet services.

Another aspect that prior research has identified is the need to better understand how information types impact the individual's willingness to disclose information (Xu, Teo, Tan, & Agarwal, 2009). Since wearable devices collect different types of information it's important to understand how health information is different from other information types.

The third aspect that prior research has identified is a need to better understand the privacy concerns and the benefits people perceive with electronic health services (Angst & Agarwal, 2009). In order to utilize wearable technology with health care services it's important to gain a better understanding of the user perceptions of privacy in connection to their health information. Understanding the privacy implications of wearable devices and the associated privacy concerns has been identified as an area that needs more research (Motti & Caine, 2015).

This research area is particularly relevant since there has been a large growth in the number of wearable devices in use and also many of the health care providers are implementing more electronic health services. Multiple companies and organizations have worked together with the University of Jyväskylä to a gain better understanding of the use of wearable devices and utilizing the collected information. The findings of this thesis provide more understanding for these aspects to fill the need to understand user perceptions.

1.2 Research questions

The study had two main research questions to answer:

1. What are the user perceptions on the privacy and sensitivity of the health information collected with wearable devices?

2. When and why are users (not) willing to share this health information in exchange for services?

The goal of the first question is to understand how individuals evaluate the sensitivity of the information collected by their wearable devices. Especially important is to understand if the health information such as heart rate causes them privacy concerns and if health information is generally considered more private than other types of personal information. Users were asked to compare different categories of information and explain how they perceive the sensitivity and privacy of each type.

Companies and organizations can benefit from this as they design new products and services that take into account the needs and potential privacy concerns that individuals have. To assist the adoption of new technologies and services it can be beneficial to lower privacy concerns caused by organizations requesting too sensitive information.

The second research question has two parts, the first part deals with the user's willingness to disclose information collected by their wearable device. Users are asked about their previous experiences and also asked to think of potential situations in which their personal information might be asked. The second part tries to understand why users are willing to provide their information in some situations, but choose to withhold information in another. Users are asked to compare different organizations and services and to discuss if they would be willing to disclose their information and why.

Most services rely on users' information to operate so companies can benefit from understanding the aspects that impact disclosure. Some organizations can better utilize user information if they have a better understanding of what circumstances individuals are willing to share their information. Other organizations could benefit from user's health information, but they are not currently receiving it because of the lack of understanding of user privacy perceptions.

1.3 Research structure and results

The empirical data for the research was gathered by conducting interviews with users of wearable devices. Interviews are a qualitative approach to understand a phenomenon from the perspective of the individual. The interviews were based on themes and guiding questions, which approach is know as themed interviews. This approach allows the researcher and the participant to discuss more freely without following a strict format, and enables the participants to explain the reasoning behind their answers. For the study, ten individuals were interviewed. This group was made up of individuals with a variety of backgrounds, different ages, and different activity levels.

The study used privacy calculus theory as the theoretical lens and foundation to design and implement the interviews and analyze the findings. This theory is well established in IS research and was fitting for this study. This theory is based on the idea that individuals evaluate the risks and benefits of using a service or disclosing their information. This theory has not been used in the context of wearable devices and health information prior to this study.

Overall the participants perceived the information collected with wearable devices to be general and not sensitive. The collected information was seen as very different from the health information stored in electronic health records, which they evaluated to be very private and sensitive in nature. The greatest difference between these two information sources was that wearable devices only collected general and numerical values compared to the very specific information that doctors have in written form.

Individuals do not share their exercise information on social media, as they don't perceive that they would receive any benefits from it. Exercising and training was seen as a private matter so the individual's did not want to discuss them on social media. Participants were willing to give their collected information to be used by doctors or medical research. User's have a general trust towards the device manufacturers and accept that their information is being used for improving products and services.

The study found that individuals have privacy concerns, especially concerning the use of their health information. These concerns and the perceived risks didn't strongly impact the behavior of the individuals, but they had recognized some of the potential negative impacts that come from electronic health information. The results in their entirety are discussed in the later chapter.

1.4 Thesis outline

Following the introductory chapter the thesis will discuss the prior research, which is relevant to this area. Prior research on the area of privacy is discussed and how different aspects such as control and trust impact privacy concerns. This is followed by the discussion on different information types and how individuals evaluate their privacy and sensitivity. The third section in the privacy

chapter discusses how privacy has been studied together with wearable technologies. This section explores the aspects that impact the adoption and use of wearable devices.

Following the discussion of privacy research the theoretical foundation of this study is introduced. The development and modeling of privacy calculus is explored and its implications to privacy research. Relevant studies that have applied privacy calculus theory are discussed and how the theory fits to this present study.

The privacy calculus chapter is followed by the discussion of the research method. This chapter describes in detail the research method that was chosen for the study and how it was implemented. It also provides details about the research process and the planning and execution of the interviews.

Following these is the results chapter, which first describes the demographics of the study participants. This is followed by the discussion of research results and findings based on the interview themes and relevant sub topics. The results chapter is followed by the discussion chapter, which connects and compares the findings of the study to previous research.

The conclusion chapter highlights the impact of the findings to practice and research. It also discusses the limitations of this study and evaluates the reliability and validity of the findings. The conclusion chapter also suggests areas for future research.

1.5 Defining terminology

Privacy. The term privacy is used in a variety of ways in information systems (IS) research and literature. One of the first ways to define privacy was based on the idea that the individual has the right to be let alone (Warren & Brandeis, 1890). The definition that is used most often in IS literature is based on the idea of control and that the individual can control how information about them is used and to what extent (Westin, 1970). If an individual perceives that they are not able to control how and by whom their information is used this can cause them privacy concerns. This definition of privacy is the most commonly used one, which is why it was found to be suitable for this thesis.

Health information. Term used in this thesis to broadly capture different types of information about a person's health. Health information includes things such as heart rate (HR) and maximal oxygen consumption (VO2 max) collected by wearable devices. It also includes information stored in electronic health records such as laboratory results, procedure notes, and written notes by the doctor.

Wearable devices. In the context of this thesis, the term is used to describe all types of wrist-worn devices that collect information about an individual's activities and health such as activity trackers, fitness trackers, and smart watches. These types of devices have some minor differences between the brands and models, but for the context of this study they are all categorized under the same term, as the differences are not relevant for this thesis.

2 PRIVACY IN HEALTH CARE AND WEARABLE TECHNOLOGY

When using e-commerce websites, wearable devices, and other devices or services, individuals are always asked to disclose personal information. The information is collected and used by the requesting party and in exchange they provide a service or some other value to the individual. In the core of information privacy is the information itself. The research on privacy is a vast area as its impacts are seen in many different disciplines. This chapter is divided into three sections: privacy, information type, and wearable technology. Each of these sections discusses the relevant research done and creates a knowledge base for the study that is reported later in this thesis. Many of the studies discussed here focus on the comparison of health information to other types of information, but many other relevant studies are also reviewed. Table 1 in the following page includes majority of the privacy articles discussed in the following sections with additional information on the different themes each article covers.

2.1 Privacy

There is a vast amount of research in the area of privacy so the following sections highlight foundational and influential studies in privacy. The studies presented here are divided into three main sections: control, trust, and personalization. Studies often cover more than one aspect of privacy so there is some overlap between different studies and even different sections. The sub-sections are created around the central topics from the studies. Figure 1 shows the synthesis of the themes and their interrelationships present in the privacy research area. The figure does not cover all the aspects, but highlights the frequent themes and concepts (see figure 1).

TABLE 1 Themes found in privacy articles

Article:	Information Type	Trust	Control	Experience	Reputation	Context/Relevance	Personalization	Policies
Anderson & Agarwal, 2011	X	X				X		
Andrade et al., 2002	X				X			X
Awad & Krishnan, 2006				X			X	X
Bansal et al., 2010		X		X				
Berendt et al., 2005							X	X
Chellappa & Sin, 2005		X			X		X	
Gao et al., 2015	X							
John et al., 2011					X	X		
Kim et al., 2008		X		X	X			
Klasnja et al., 2009	X					X		
Lee, & Kwon, 2015	X						X	
Li, 2014		X			X			
Li et al., 2011	X					X		
Li et al., 2016	X							
Lwin et al., 2007	X	X				X		X
Malhotra et al., 2004	X	X	X					
Motti & Caine, 2015	X		X					
Patterson, 2013	X	X	X					
Phelps et al., 2000	X		X	X				
Rohm & Milne, 2004	X	X						
Willison et al., 2007		X	X			X		
Raij et al., 2011	X							
Schoenbachler & Gordon, 2002		X		X	X			
Sheehan & Hoy, 2000		X	X	X				
Sutanto et al., 2013	X						X	
Xu et al., 2008			X					X

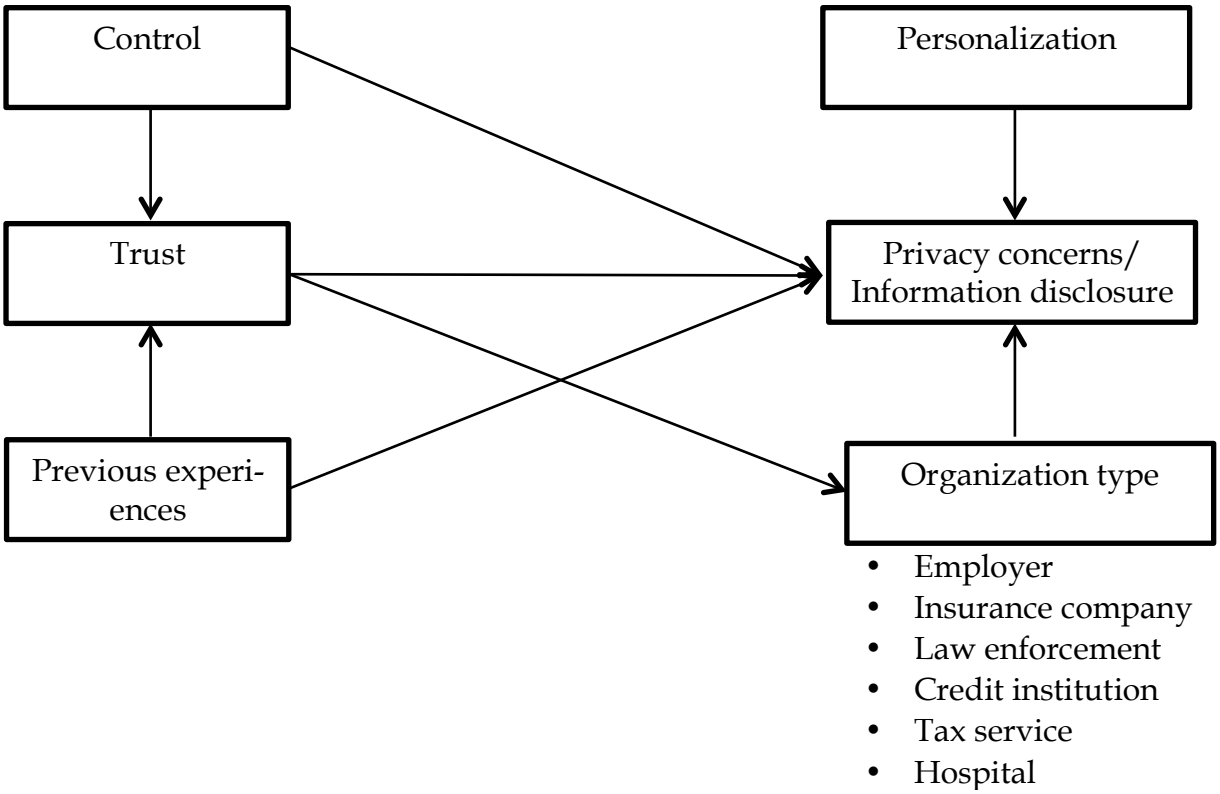

FIGURE 1 Synthesis of privacy research themes and their interrelationships

2.1.1 Control

Privacy research is a broad area and there are many aspects that can impact individuals privacy concerns. Control over one's information is one of the key concepts of privacy research and emerges from many of the studies as a factor (see figure 1). Stone, Gueutal, Gardner, and McClure (1983) conducted one of the first studies that considered the impact of the information requesting organization to the information privacy and willingness to disclose information. In the study six different organizations were compared, including employers, insurance companies, law enforcement, credit and lending institutions, and the national tax service. Then analysis was done on how the organization type impacts the individual's privacy concerns. Stone et al. (1983) explored in their study how the organization type could impact the individual´s information privacy values, beliefs, attitudes, information experiences, and behavioral intentions.

The study found that individuals that highly valued information privacy also perceived that they had less control over their information, and were less willing to participate in further studies (Stone et al., 1983). On the other hand, those that perceived having more control over their information had a more

positive attitude towards controls in place and were more willing to participate in further studies. Stone et al. (1983) also found that positive attitudes towards controls over information privacy made people less willing to support government legislations concerning information privacy. Negative past experiences and even negative experiences of acquaintances were found to increase the negative attitudes towards information privacy, which in turn lowered the perceived control over information. Negative past experiences have been shown in later studies to increase privacy concerns (Bansal et al., 2010; Phelps et al., 2000; Sheehan & Hoy, 2000), but this study demonstrated that an awareness of the experiences of acquaintances also has similar impact.

Stone et al. (1983) discovered that the organization type did impact the persons information privacy values, beliefs, and attitudes, but it didn´t impact behavioral intentions. Analysis showed that participants perceived having the most control over the information their employer and the tax service had. In addition they had the most positive attitude towards how they can control information their employer had compared to the lack of control with other organizations. The importance of controlling one´s personal information was found to a critical aspect impacting privacy concerns, which has been supported by multiple later studies (Dinev & Hart, 2003; Hodge et al., 1999; Patterson, 2013; Phelps et al., 2000; Willison et al., 2007; Xu et al., 2011). The person's ability to be in control is one of the key aspects that impact privacy concerns and in turn willingness to disclose personal information. Also as the study found, privacy concerns are different towards different types of organizations that an individual interacts with.

Sheehan and Hoy (2000) also studied the impact of control and they found that lack of control is the key concern that individuals have over the privacy of their data. Participants expressed concerns over what information was collected about them and how their information was used. The second important aspect found in the study was that the lack of notices from companies concerning how information was used increased privacy concerns (Sheehan & Hoy, 2000). Participants hoped to have greater awareness of the information practices of the companies, which in turn would help to mitigate their privacy risk concerns since users would be aware of the information collection process (Sheehan & Hoy, 2000). Another finding of the study was that individuals see use of online services as an exchange in which they evaluate the benefits received from disclosing personal information and the risks associated with it (Sheehan & Hoy, 2000). This finding echoes that of the studies in privacy calculus were individuals evaluate the potential benefits they received compared to the potential risks that come from disclosing personal information (Culnan & Armstrong, 1999; Dinev & Hart, 2006). Sheehan and Hoy (2000) found that previous experiences with a company helped to create relationships that helped to mitigate privacy concerns. This points to the importance of trust and fair information practices to create these relationships and retain customers as other studies have also found (Culnan & Armstrong, 1999; Dinev & Hart, 2003; Dinev & Hart, 2006; Li & Sarathy, 2007). Individuals want to know how their information is being used and for what purpose and have control over some of the aspects. Also as customers

become familiar with the information practices of a company and have positive experiences they lower their concerns, as they are able to have more trust.

Privacy concerns is frequently used term in many of the studies regarding privacy as it has been discussed here as well, but how the privacy concerns are actually formed has not been studied as thoroughly. One research showed that privacy concerns are formed by the person's disposition to value privacy as well as the situational context that person uses to evaluate information disclosure (Xu, Dinev, Smith, & Hart, 2008). This same study also found that an individual evaluates the information boundaries present, the privacy risks, privacy controls, and potential privacy intrusions risks when forming their privacy concerns. Xu et al. (2008) found that the perceptions of intrusion, privacy risks, and privacy controls were significant factors of privacy concerns in all the different types of websites used in the study. A person's disposition to value privacy was significant in predicting perceived privacy risks, and social norms were found to predict the person's disposition to value privacy (Xu et al., 2008).

Xu et al. (2008) confirmed that control has a significant influence on privacy as it has been found in numerous other studies (Dinev & Hart, 2003; Hodge et al., 1999; Patterson, 2013; Xu et al., 2011). Their study also found that privacy risks are mitigated through privacy policies on websites, which has been explored in other studies as well (Culnan & Armstrong, 1999; Lwin et al., 2007). Xu et al. (2008) found interestingly that in the case of a healthcare websites users disposition to value privacy was not a significant indicator of their perceptions of information intrusion. The explanation was that when individual's visit a health care website they often have a urgent need, and understand that in order to receive help they need to disclose personal information, which in other contexts they might not be willing to provide. So urgency of information might override other privacy concerns that are normally present when interacting with other types of websites. Since in the context of health care the value of information is high and an individual is willing to take more risks.

In many information privacy studies the participants are being asked to evaluate their privacy concerns on a scale or compare it to some other aspect. The caveat is that individuals might rate certain information types or situations to be very sensitive, but these evaluations don't actually reflect their true behavior. Berendt, Günther, and Spiekermann (2005) conducted a study in which participants were interacting with a fictitious web-store that had a bot that asked questions and offered suggestions. Participants were first given a survey to measures their privacy concerns through different types of questions and given examples. After the survey participants interacted with an online store and the bot that would occasionally ask questions from the participants, which included information such as address, hobbies, or product preferences and then provided personalized feedback. Berendt et al. (2005) found that based on the survey results, even the users grouped within the high privacy concern groups, did not behave according to their preferences in the actual online setting. The study found that levels of information disclosure were high across all the different types of groups, indicating that the stated preferences did not translate into actual behavior (Berendt et al., 2005). Berendt et al. (2005) argued that situational contexts such as gains or benefits are important factors and that individual's

don't rationally consider their behavior when interacting with a website. This seems to indicate that individuals don't always follow the cost-benefit calculus, at least in conscious level. Berendt et al. (2005) also discovered that privacy statements or policies don't significantly impact disclosure of information, which finding is different than that of other studies (Andrade et al., 2002; Awad & Krishnan, 2006; Lwin et al., 2007).

2.1.2 Trust

Individual's trust towards an organization has been found to impact the willingness to disclose personal information (see figure 1). Schoenbachler and Gordon (2002) conducted a study in which they measured trust and its relationship to information disclosure. Participants of the study had previously made actual purchases from a mail-in catalogue and when asked to participate in the study, they were asked to base their answers on this recent experience. This is an important distinction compared to many other studies, which often have participants evaluate either fictitious events or unspecified previous experiences. The study found that perceived risk, previous experiences, and credibility of the organization didn't have a significant impact on the trust towards the organization (Schoenbachler & Gordon, 2002). This finding differs from other studies that have found that previous experiences do impact the individual's trust towards an organization (Bansal et al., 2010; Sheehan & Hoy, 2000). Schoenbachler and Gordon (2002) reasoned that the design of their study might have caused the outcome that the previous experience variable wasn't found to have impact. Many of participants were first time buyers and those that had previous experiences with the company had had positive experiences, as they had been willing to purchase again.

Reputation of the company and its perceived dependability did show significant positive relationship to trust (Schoenbachler & Gordon, 2002). Other studies have also found that the reputation of the company or a given website helps to lower the privacy concerns that an individual has, which in turn increases disclosure of information (Andrade et al., 2002; Kim et al., 2008; Li, 2014). Schoenbachler and Gordon (2002) found interestingly that individual that had high levels of trust perceived having a relationship with the company instead of just making a transaction. When the study analyzed differences between industries that the products ordered belonged to, they found that the credit card industry had some differing characteristics when it came to trust. Schoenbachler and Gordon (2002) found that perception of dependability and willingness to provide information were not significant in creating trust with the credit card industry, which they explained by customers understanding that financial information needed to be provided in order to receive credit. It can be difficult to measure an individual's willingness to disclose information when the information requested is necessary to conduct the transaction. As the studies on trust are numerous and their findings show its significance, it seems to indicate that it's one of most important factors impacting privacy concerns together with control. Studies have found that trust can be developed in many ways and

things such as prior experiences, company reputation, and customers control over their information can impact trust.

Kim, Ferrin, and Rao (2008) conducted a study, which looked at the impact of different factors to individual´s making purchases on e-commerce websites. Some of key aspects in the study included trust, perceived risk, and perceived benefits and how they impact the intention to buy, which in turn has significance in making the actual purchase. Other factors that Kim et al. (2008) included in their test model were familiarity with the website, disposition to trust, company reputation, and perceived protection. The study tested how these factors impact either the individual's trust or perceived risks, which then impacts purchase decisions.

Kim et al. (2008) discovered that trust did have a significant positive impact on the user´s intentions to purchase, and it also helped to reduce the perceived risks factor. As expected, perceived risks did reduce intention to purchase and perceived benefits did help to increase the likelihood of purchase, but the trust factor was still the best predictor of purchase behavior (Kim et al., 2008). The study also found that perceived privacy and security protection as well as company reputation did lower the perceived risks and increase the trust. This finding indicates that both privacy and security are important factors to individuals. The positive impact of company reputation has been found in other studies to increase disclose of information (Andrade et al., 2002; Li, 2014), but the study conducted by John et al. (2011) found that unprofessional websites did actually increase information disclosure.

Kim et al. (2008) also looked at the impact of privacy seals present at the website and found that they didn´t increase trust, but did help to reduce perceived risks that individuals had. When a website was familiar to the user it increased purchase intentions and trust, but didn´t impact the perceived risks that the user had, which finding is aligned to that of Li et al. (2011). Kim et al. (2008) also confirmed that personal disposition did increase trust as has been found in other studies as well (Li, 2014). Trust has emerged together with control as some of most significant factors impacting privacy concerns.

Study conducted by Li (2014) looked that the impact of individual´s disposition towards privacy, and how a website reputation and the individual´s familiarity to it impacts their privacy concerns. Li (2014) found that personal disposition towards privacy did have a significant impact on privacy concerns when the website had low reputation and low familiarity to the individual. On the other hand websites that were familiar and had high reputation did not see a significant connection between personal privacy attitudes and privacy concerns. In the case the website was unfamiliar to the participant reputation did fully mediate the privacy concerns of the individual (Li, 2014). These findings indicate that organizations should give attention to reputation building activities since high reputation can help to mitigate privacy concerns and attitudes that individuals have even if the website is not familiar to them. Li (2014) argued that based on the findings, personal disposition towards privacy does impact privacy concerns when interacting with websites. Risks, benefits, reputation, familiarity, and disposition to trust are all aspects that seem to play a role as part of the individual's privacy calculations.

2.1.3 Personalization

One area of privacy research is personalization and the paradox between individuals having to disclose information for services, but disclosure causes them privacy concerns (see figure 1). Chellappa and Sin (2005) studied the personalization privacy paradox and how individuals evaluate if they are willing to disclose information online. They found that when individuals trust an organization they are going to have higher intent to use personalized services, which will lead to purchases (Chellappa & Sin, 2005). A customer's evaluation of the value of personalization will have twice the influence as their privacy concerns when it comes to deciding if they use a service (Chellappa & Sin, 2005). So offering enough value or benefits for customers can help them to use a personalized service even when they might experience privacy concerns. Chellappa and Sin (2005) suggests that based on their findings trust and reputation building activities are worth more than trying to mitigate privacy concerns, and that making personalization valuable to the user helps to overcome privacy concerns. When users evaluate the usefulness of personalization they are not driven by just monetary benefits, but also other things such as the convenience it provides them (Chellappa & Sin, 2005). Individuals will use personalized services if the value they receive is higher than the risks or costs, which follows the privacy calculus theory.

Awad and Krishnan (2006) have also studied the personalization privacy paradox in connection with information transparency and the impact on willingness to disclose information online. Aspects included in their study were the impact of privacy policies, previous privacy invasions, privacy concerns, and demographic differences and how they impact the importance of information transparency. Information transparency can impact the individual´s willingness to be profiled online in order to receive personalized services and advertising. So the customers needs to be aware of how the company operates and uses the customer information.

Awad and Krishnan (2006) discovered that privacy concerns and importance of privacy policies did impact positively the information transparency ratings. In other words, information transparency is more important if a user has privacy concerns or if they value privacy policies on websites. Complete privacy policies have been shown to mitigate privacy concerns in other studies as well (Andrade et al., 2002). The study didn´t find that demographic information would have any significant impact on the user evaluation of the importance of information transparency. Awad and Krishnan (2006) also showed that individuals that are more willing to be profiled online for either personalized services or advertisings don´t evaluate information transparency to be so important. So the individuals that have higher privacy concerns and value information transparency don´t want to be profiled and receive personalization. Other studies have shown the personalization of services can reduce privacy concerns, which in turn increases individual´s willingness to disclose personal information (Lee & Kwon, 2015; Wang, Duong, & Chen, 2016; Xu, Luo, Carroll, & Rosson, 2011; Xu, Teo, Tan, & Agarwal, 2009). Awad and Krishnan (2006) also found that prior privacy invasions did lower the willingness to be profiled

for advertising, but it didn´t impact personalized services, which was explained by the users perceiving more benefits from personalized services than from advertisement. Privacy policies that promote information transparency can help to mitigate privacy concerns, which can lead to more engaged customers.

Personalization privacy paradox has also been studied in the context of advertisement in mobile applications and the impacts on privacy concerns (Sutanto, Palme, Tan, & Phang, 2013). The study had three different types of applications that were installed to the participant's smartphone, which enabled them to browse advertisements and save them for later. The first group had an application that offered ads without personalization, the second group received personalized ads and their preferences were sent to a server for data analysis, and the third group also received personalized ads but their information was processed locally on the device to give the user higher privacy safety. The goal was to see if personalization and different privacy settings impact usage of the applications. To evaluate the impact of personalization Sutanto et al. (2013) measured process gratification by measuring how often participants opened the application, and content gratification was measured by counting how many ads the users saved to be viewed later.

Sutanto et al. (2013) found from their results that the two applications, which provided personalization, were launched more often indicating that they provided process gratification. The study also found that even though the applications offered personalization it didn't increase content gratification meaning that the amount of ads saved was not impacted (Sutanto et al., 2013). Sutanto et al. (2013) also discovered that the application that was considered privacy-safe as it processed information locally did provide higher process and content gratification, which meant that this group opened the application most often to see ads and also saved the highest amount of ads for later, compared to the other two applications.

After the initial study the researchers also conducted a survey with the participants to further understand their behavior and thoughts. Results found that the group that received non-personalized ads found the number of ads to be more excessive and annoying than the other two groups (Sutanto et al., 2013). The group that used the privacy-safe version of the application had lower privacy concerns and provided more answers to profiling questions that are beneficial to personalization. Sutanto et al. (2013) discovered that users assume that if they receive personalization then their information is being gathered and used for different purposes. The study also found that participants were less concerned about giving personal information such as age and dietary preferences, but more concerned about saving advertisements as they perceived that it would be more sensitive and personal (Sutanto et al., 2013). This again confirms that information type does impact privacy concerns and information disclosure. The main finding of the study was that offering privacy-safe applications that offer personalization will increase the use of the application and help to mitigate privacy concerns that an individual has. So even though personalization by itself only increased the value individuals received from the use of the applications, pairing it with privacy features also increased its usage. For companies developing products and services these findings are useful as they can

evaluate if including these features would improve the adoption and usage of new technology or services.

2.2 Information type

One of the research areas in privacy is the impact of different information types to privacy concerns. Not all information is considered equally sensitive or private by individuals, so the type of information that they are asked to disclose impacts their thoughts and behaviors. The following sections present studies that discuss the impact of different information types in addition to other aspects that also impact privacy concerns. The sub-sections also discuss how personality traits, context and relevance, and different types of health information impact privacy concerns. Many of the studies chosen use medical or health information as one of the information types used in the comparison. Focus has been given to these types of studies as they create a foundation to enable the analysis of this study's findings, which are reported in the later chapter. Figure 2 below highlights the themes most relevant in the research area of information type and privacy concerns. The figure combines the concepts into one and shows their interrelationships as they are found in different studies (see figure 2).

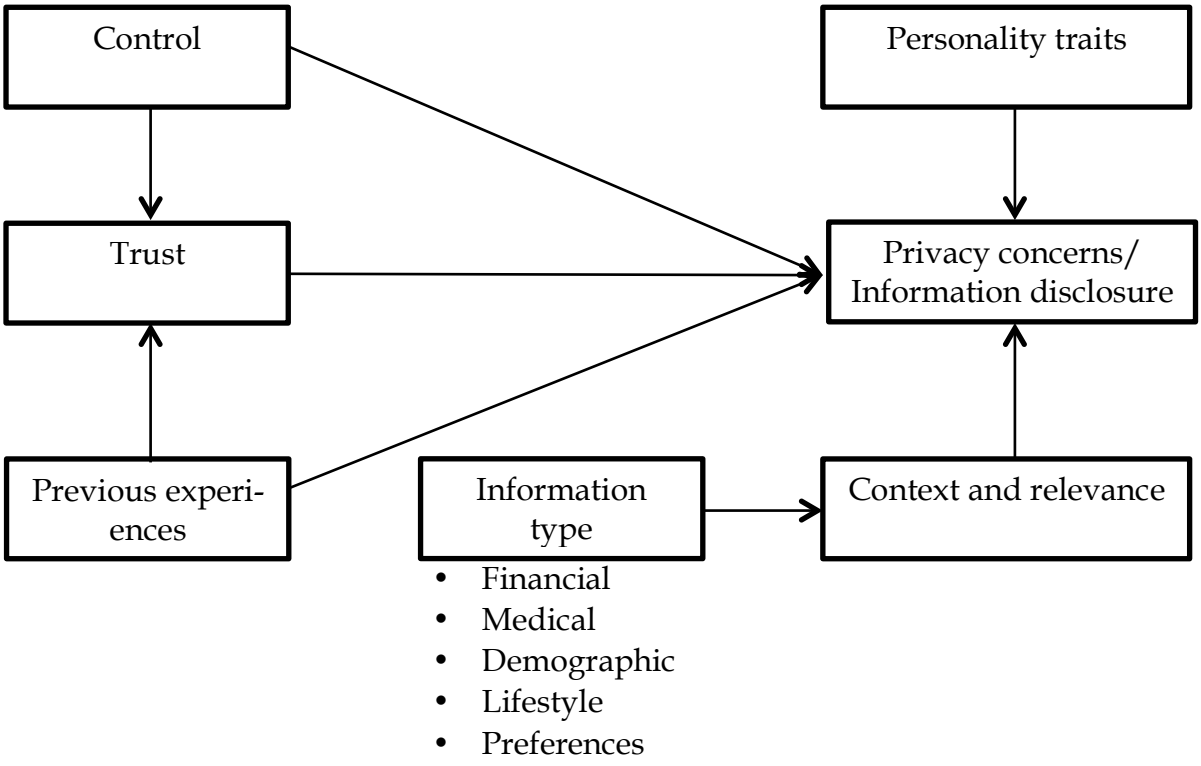

FIGURE 2 Synthesis of information type research themes and their interrelationships

2.2.1 Comparison of information types

When using online services or interacting with websites individuals are asked to provide personal information. Individuals are more willing to provide some types of information about them compared to some other information that they perceive to be more sensitive (see figure 2). Phelps, Nowak, and Ferrell (2000) studied the impact of information type and consumers willingness to disclose personal information and how they relate to levels of privacy concerns. What they found was that individuals are more willing to provide demographic and lifestyle information for marketers compared to financial information or personal identifiers such as name, address, and social security number (Phelps et al., 2000). Individuals were the least willing to provide information concerning their income, types of credit cards, or social security numbers. These findings indicate that individuals evaluate information about them and consider the information to have different levels of sensitivity, which requires different levels of privacy. When the information is considered to be more sensitive, then the individuals will not be as willing to disclose it. Demographic information or lifestyle choices might not identify the individual so they are less concerned about providing this type of general information about themselves.

Phelps et al. (2000) also found that individuals have concerns for how their information is being used by the marketers. Participants felt that marketing companies did not care about privacy, and that they knew too much information about the consumers. Participants wanted restrictions on the volume of information that was collected about them. Participants wanted to have more control over their information and how it's being used, which helps them to have less privacy concerns (Phelps et al., 2000). When individuals don't feel like they are in control it is easier for them to worry about the possible ways that the information they provide might be misused.

Those individuals that had purchased something from a direct marketing catalogue in the last 6 months had decreased amount of privacy concerns towards the misuse of their information, indicating that the prior experiences did have an impact (Phelps et al., 2000). Phelps et al. (2000) did an analysis of the impact of demographic information and privacy concerns and found that individuals with some college education or vocational training had the highest concerns, followed by high school graduates, and the lowest privacy concerns were in the group of college graduates. Education level seems to have an impact on privacy concerns and especially college graduates had significantly lower concerns compared to the two other groups. In addition to the information type, the prior experiences with a company can help the individuals to have fewer worries about making transactions. It can be important to make sure that users have a positive first time purchase so that they would have less concerns when making future purchases.

How the information type being requested from an individual impacts privacy concern has also been studied in connection with other aspects. Malhotra, Kim and Agarwal (2004) developed a model of privacy concerns and conducted a survey to see how different aspects impact the willingness to disclose information. Types of information requested in the survey were either

more general shopping related information such as preferences or more personal financial information such as income, debt, and current account balance. It was found that when more sensitive information was requested it reduced trusting beliefs and also the intention to disclose, and also increased risk beliefs (Malhotra et al., 2004). These findings join the other studies that have found that information sensitivity does impact privacy concerns. Individuals evaluate financial and health information to be the most sensitive information types (Andrade et al., 2002; Phelps et al., 2000). The importance of trust was also found to be significant since participants that had higher trust beliefs also had lower risk beliefs, which in turn helps to increase the intentions to disclose personal information (Malhotra et al., 2004). Building trust between the individual and an organization can then be seen as a possible way to help to lower privacy concerns as Rohm and Milne (2004) found in their study.

It can be expected that since there are individual differences between the levels of privacy concerns, that one of the factors impacting them is demographic characteristics. Malhotra et al. (2004) analyzed in their study the impact of age and education and found that older participants were less willing to disclose information, and higher education levels actually lowered trust beliefs in individuals, which is similar to the findings of Phelps et al. (2000). In addition to these findings other individual differences were found to be significant as well. Experienced Internet users had lower risk beliefs and those that had provided fake information previously were more likely to disclose fake information in the future. Malhotra et al. (2004) argued that the most important result from their study were that individual's want to have control over their information and awareness of the type of information that is collected about them. It's easier for individuals to trust organizations if they understand what information is being collected, how it is being collected, and that the individual can also control how this information is being used. Information type, demographic and personal characteristics, and levels of control all impact the willingness to disclose information and the type of privacy concerns individuals have.

Lwin, Wirtz, and Williams (2007) created a study that investigated the impacts of information relevance and information sensitivity and how users perceive privacy concerns in these cases. Participants were shown a fictitious car rental, banking, or medical service websites and they were requested to provide different types of information depending on the group they were assigned. The types of information included; name, number, marital status, income, occupation, and medical history. The goal was to see how context, relevance, and information type impact privacy concerns and the following information disclosure. Individuals evaluated how responsible a company was based on the quality of their privacy policy that was posted on the website and this evaluation directly impacted the levels of privacy concerns (Lwin et al., 2007). User's trust towards a website was also impacted by the relevance of the information that was being requested from them.

There are different ways that individuals mitigate the privacy concerns that they face, which include things such as falsifying information, using tools or services to protect their identity online, and withholding information from websites. Good privacy policy can lower concerns, but the study found that was

true only when information requested had low sensitivity level (Lwin et al., 2007). Financial and medical information was found to be the most sensitive as other studies have shown (Andrade et al., 2002; Lwin et al., 2007; Malhotra et al., 2004; Phelps et al., 2000), and if this information was requested, even good privacy policies didn't help to mitigate the concerns individuals had. Lwin et al. (2007) argued that when requested information is highly sensitive the context and relevance of the information becomes more important as the user determines if they are going to disclosure correct information.

2.2.2 Impact of personality traits

Personal disposition towards privacy and information disclosure together with other personality traits and demographics can all impact privacy concerns (see figure 2). One study focused their research on the impact of demographic characteristics to privacy concerns and information disclosure (Laric, Pitta, & Katsanis, 2009). Participants had to consider if their medical records contained information about certain conditions or treatments they had received how concerned they were about that information being disclosed. When comparing the privacy concerns of different medical conditions and treatments it was found that in most cases females had higher privacy concerns and considered this information to be more sensitive than men (Laric et al., 2009). Laric et al. (2009) found in their study that health related privacy concerns increase with age, and they argued that younger individuals having less medical ailments and treatments done to them explain this. The study also looked at the impact of race and found that white Americans and Asians had the highest privacy concerns towards medical procedures. They evaluated medical procedures to be the most sensitive. On the other hand black Americans were found to have higher privacy concerns across all types of medical information and treatments. Laric et al. (2009) also found that the findings were consistent for the most part when gender, age, and race were also studied in Canadian population during the second part of their study. These findings seem to indicate that gender, age, and race do impact a person's privacy concerns toward health information and that there will be differences between different ethnic groups.

When individuals interact with a company online or a website, there are many aspects that impact the relationship as has been reviewed in earlier articles. Bansal, Zahedi, and Gefen (2010) conducted a study in which they look at the impact of personal dispositions to privacy concerns and the levels of trust individuals had. The study focused on disclosing health information in an online setting to see what could impact behavior. Aspects that the study looked at were personality traits, health status, information sensitivity, and personal circumstances, and it analyzed how these can impact trust levels and privacy concerns (Bansal et al., 2010). The privacy calculus model, which was first developed by Culnan and Armstrong (1999), was found to be relevant in this study as it was found that individuals use this decision-making process to evaluate the risks and benefits of disclosing their health information. The way health care websites operate is by requesting personal information including

details about health from individuals in exchange for providing benefits such as online health advice, access to a doctor, or evaluating an individuals health status.

The study found that disclosing personal health information raises concerns such as discrimination, unauthorized access to the data, negligence from the company, and other abuses of the information provided (Bansal et al., 2010; Hodge, Gostin, & Jacobson, 1999). An important finding from the study was the significant impact a poor health status had on perceived information sensitivity, which in turn increased the privacy concerns experienced by the individual. In addition to having poor health, personality traits were found to impact the evaluation of health information sensitivity (Bansal et al., 2010). It is possible that healthy individuals have lower concerns towards disclosure of health information since they perceive that their medical history doesn't include anything sensitive compared to the individuals that have health problems and might wish to hide them or protect them. All health related information can be sensitive, but individuals with poor health status can be even more sensitive towards disclosing details about their health (Bansal et al., 2010). In addition to poor health status, personality traits were found to impact health information sensitivity, privacy concerns, and trust towards companies (Bansal et al., 2010). Trust is also impacted by good and bad experiences individuals have had with disclosing information, and it impacts their future behavior. Bansal et al. (2010) discovered that trust is not just impacted by external factors such as the website itself, but also internal factors such as personality traits and previous experience. This is an important point that needs to be considered when designing healthcare services and products, in addition to the privacy-oriented design. Individuals that need online health care services the most are those that have health problems. The challenge is that this group of people also has the highest privacy concerns and more prior experiences, which can impact their willingness to use such a service. Building trust between companies and individuals can help to lower concerns, but it can be difficult to apply to different personality traits.

Some of the obstacles for users to accept and adopt mobile healthcare services are the privacy concerns they have. In order for the individual to benefit from wellness and healthcare applications and services, they need to disclose information about themselves and also enable tracking of certain information about their movement and activities. Lee and Kwon (2015) argued that the established research on privacy calculus could explain the differences found between different categories of information that they studied (Culnan & Armstrong 1999; Dinev & Hart, 2006). Participants in the study were first given a survey to collect demographic information, medical history, and psychological factors such as fatigue, stress, and depression. After the survey participants wore an activity sensor that collected information about environmental factors such as humidity and noise, and medical information such as pulse, BMI, sleep, and activity levels. Lee and Kwon (2015) found that when individuals were asked to rate the level of privacy concerns they had about the different types of information collected, people had higher concerns with medical and psychological information compared to demographic and environmental data. They ar-

gued that based on these findings physical and mental health information raises more privacy concerns to individuals than other personal information such as age, gender, and ethnicity (Lee & Kwon, 2015). These finding align with previous studies that have found that health information is considered to be the most sensitive along with financial information, and other information such as demographic information is considered to be less sensitive (Andrade et al., 2002; Angst & Agarwal, 2009; Li et al., 2011; Lwin et al., 2007; Malhotra et al., 2004; Phelps et al., 2000).

One approach to mitigate these concerns is to increase the value the users get by personalizing the services and products. Personalization is needed for the users to find value in disclosing their health information and to mitigate the perceived risks when individuals are considering the risks and benefits of their decision. Lee and Kwon (2015) also argue that healthy people have less motivation to disclose health information for an application compared to those that have diseases or symptoms, and need more motivation. Motivating this group can help them to see that the value of personalized health services is higher than the perceived privacy risks. This is an interesting argument that is based on the idea that healthcare and wellness applications would be geared towards those individuals that already have health problems, and healthy individuals that might want to improve their health would be a secondary group. Of course it can be hard to define and determine who qualifies as a healthy individual and who doesn't. Bansal et al. (2010) found in their study that poor health status raised an individual's privacy concerns, which impacted disclosure of health information. Also, a study by Anderson and Agarwal (2011) found that individuals who had negative emotions towards their health and had health problems were actually more willing to disclose health information. Findings from these three studies seem to indicate that individuals with health problems are more motivated to use health care technology and services and to disclose information in order to benefit from them. At the same time these same individuals actually might have higher privacy concerns than healthy individuals. Information context and relevance can be important aspects to explain this and that individuals with poor health can overcome even their high levels of privacy concerns when the benefits they receive from a health care service are higher than the risks associated with disclosure.

2.2.3 Impact of context and relevance

In addition to information type and personality traits, other aspects also impact privacy concerns such as the context in which information is being requested and how relevant it is to the situation (see figure 2). A study conducted by Andrade, Kaltcheva, and Weitz (2002) explored how privacy policies, company reputation, and rewards impact the willingness to disclose personal information. Since e-commerce sites rely on data about the consumers, they either gather this information or attempt to encourage individuals to self-disclose the information. The information can be used for marketing and advertising or offering users

personalized offers and services. Andrade et al. (2002) found that when companies have a high reputation the customers that interact with them have lower privacy concerns. This shows that it can be beneficial for companies to build their reputation in order to help mitigate privacy concerns that new and existing customers might have. Many websites have some type of privacy policy posted that highlights some of the organizational practices and processes when it comes to protecting the privacy of the individuals. Andrade et al. (2002) discovered in their study that complete privacy policies that were detailed did help to reduce the concerns that individuals had, so in addition to the existence of the privacy policy, quality also matters.

In order to encourage self-disclosure the study offered rewards through the website, but found that this type of direct offer for information exchange actually increased privacy concerns (Andrade et al., 2002). In the study the participants thought companies were being suspicious when offering monetary rewards for their information, and that the rewards were a type of decoy to get their information. Andrade et al. (2002) also studied the impact of the information type that was requested and found that medical information caused individuals to have higher privacy concerns and made them less willing to disclose it when asked. Health information can tell a lot about an individual and identify details about them, so it's not surprising that this information type in addition to financial information has been identified as sensitive (Phelps et al., 2000) and can cause high privacy concerns. Type of information, website reputation, completeness of privacy policy, and rewards were all found to impact privacy concerns, which in turn impact the willingness to disclose information (Andrade et al., 2002).

Some basic information about us is stored in many different places such as credit reports, car registration, insurance applications, and medical records. In a research conducted by Rohm and Milne (2004) they found that when a company accesses personal information such as name and address it makes a difference to the individual where this information was retrieved from. Individuals had significantly higher privacy concerns when companies access their information from medical records compared to any other information sources. Even though the information accessed was the same, the location where it was stored and retrieved impacted how the individuals felt about it. This finding indicates that personal health records as a whole are considered highly private potentially because they contain information about person's health in addition to the demographic information that is available in other places (Rohm & Milne, 2004). This finding is aligned with that of Andrade et al. (2002), which found that medical information was evaluated to be the most sensitive compared to other information.

It is possible for companies to purchase health related information about an individual even though they haven't had any type of prior contact. Rohm and Milne (2004) found that individuals had high levels of privacy concerns when they learned that this is possible, since they felt they hadn't given consent. Privacy concerns and trust also vary between different types of organizations that might request information about an individual. Overall individuals tend to have quite low levels of trust towards different organizations and high levels of

privacy concerns at the same time (Rohm & Milne, 2004). An employer, insurance company, pharmacy, or grocery store might request information about an individual and they might use this information in a variety of ways. Rohm and Milne (2004) found that employers and insurance companies did cause the individuals to have the highest privacy concerns from these different types of institutions, but at the same time individuals also indicated highest trust towards employers compared to all others. These findings indicate that medical records have a special importance to individuals and a company accessing the records needs to be aware that there are many privacy concerns related to them. Companies should also consider the impacts that it might have when they access or purchase information from different sources as the individuals might have the perception that they have not given consent. Individuals also don't have the same level of trust towards all different types of organizations indicating that many aspects impact privacy concerns.

An individual's first impressions of a new website has shown to impact their privacy concerns, and these impressions have the power to lower their disclosure of personal information during the interaction with the website (Li, Sarathy, & Xu, 2011). Individuals also consider if the requested information on a website is relevant to the given context and this impacts the level of privacy concerns they experience (Li et al., 2011). Companies might want to maximize the amount of information they collect and might request all types of details, but this behavior can influence the user and make them more concerned about their privacy and choose to discontinue their interaction with the website. Li et al. (2011) found that after the initial impressions, the user's were influenced by the fairness of information practices of the website, which adjusted their privacy beliefs and concerns and this impacted their willingness to disclose personal information.

As previous studies have found, the sensitivity and type of information as well as the context in which it is requested will impact the individual's privacy concerns and disclosure (Bansal et al., 2010; Culnan & Armstrong, 1999; Laric et al., 2009). Relevant information to the context can lower perceptions of the sensitivity of information and promotes disclosure of information. Not all information is considered to be as sensitive and Li et al. (2011) found that demographic data such as name and gender are considered low sensitivity. On the other hand, their study confirmed the findings of previous studies, that individuals consider health and financial information to be the most sensitive (Andrade et al., 2002; Angst & Agarwal, 2009; Li et al., 2011; Lwin et al., 2007; Malhotra et al., 2004; Phelps et al., 2000). Li et al. (2011) found that information sensitivity, as a factor by itself, did not show significant influence on the privacy risk perceptions, but was overridden by the relevance of the information to the context. From these findings it seems that the context of the information requested and its relevance impact the perceptions of information sensitivity and are not at fixed levels. Li et al. (2011) proposes that the context and information sensitivity needs to be more fully studied to see if types of information are more or less sensitive depending of the context.

2.2.4 Comparison of health information

Previous sections have discussed the impact of different information types to the levels of privacy concern, but none of them have specifically compared different types of medical information. Anderson and Agarwal (2011) performed a large study with over 1000 participants to test if the type of information requested, the purpose the information was for, and who is requesting the information have an impact on the individual's willingness to disclose information about their health. This study is the only one to collect and analyze data on all three aspects mentioned and to find how privacy concerns surface in the personal health information area. This study looked at three different types of information, which were: general health, mental health, and genetic information. Some other studies have compared the disclosure of health information compared to financial or demographic information, but none of them have compared the different subgroups of just health information (Angst & Agarwal, 2009; Li et al., 2011; Lwin et al., 2007). In the context of this study the purposes that the information was requested was for patient care, research, or marketing. The study also looked at three different stakeholders that would request the information and these were; hospital and doctors, government, and pharmaceutical companies. All these different information types, purposes of use, and stakeholders' created 27 different values to analyze (Anderson & Agarwal, 2011). In addition the study was the first to look at emotions and how they could impact the willingness to disclose information in this health context. An important factor in the study was the impact of trust in the electronic medium used for making the transactions was explored (Anderson & Agarwal, 2011).

Anderson and Agarwal (2011) found in their analysis that the type of health information requested did not have a significant impact on the privacy concerns or the trust on the electronic medium used for the transaction. This in turn meant that the type of information requested did not impact the individual's willingness to disclose personal health information. The researchers argued that possibly all types of health information is sensitive to a person and that they don't distinguish between them, so the health information category as a whole is something that is sensitive (Anderson & Agarwal, 2011). As one would expect, individuals are more willing to provide personal health information for patient care, but the study showed that individuals have higher concerns for disclosing information for marketing or research purposes as these areas are less relevant to them (Anderson & Agarwal, 2011). This finding is no surprise since individuals understand that when providing health information for patient care they are receiving direct benefits compared to the less direct benefits that research or marketing might provide for them. Health information sensitivity might be static from the individual's perspective, but context and relevance will impact their privacy concerns that come with disclosing it.

The trust towards the company requesting information is important, but trust to the electronic medium used for handling health information also has an impact. Anderson and Agarwal (2011) found that trust in the information medium was the most important when information was requested for research purposes, but less so in other contexts. Individuals that had low levels of trust

to the medium used were less willing to provide health information to government and pharmaceutical companies compared to hospitals. When the government requests information individuals had higher privacy concerns since the context and relevance is low, but in turn they had less concerns providing health information for hospitals and pharmaceutical companies (Anderson & Agarwal, 2011). Overall, individuals are willing to provide information about their health to companies that are a part of the health care value chain, and they are seeing it to be relevant and beneficial to them.

Prior research has found that poor health status would increase privacy concerns and reduce the willingness to disclose personal health information (Bansal et al., 2010). Anderson and Agarwal (2011) found in their study that individual's who had negative emotions towards their heath were more willing to disclose health information, and that positive emotion towards one's health wasn't found to be significant in impacting willingness to disclose. Those that have propensity to trust or that had altruistic emotions were reported to have higher levels of willingness to disclose information. Also higher levels of education and exposure to media concerning the misuse of health information did lower the willingness to disclose (Anderson & Agarwal, 2011). Anderson and Agarwal (2011) also asked participants to imagine having a cancer and evaluate how that would impact their willingness to disclose personal health information. What they found was that individuals that didn't have experience with cancer and were asked to imagine its impact had significantly lower levels of willingness to disclose health information compared to those that had current cancer diagnosis. Further more individuals that experienced sadness, anger, or anxiousness about their health were more likely to disclose information, which is somewhat different from previous findings about the impact of poor health status to disclosure (Bansal et al., 2010). Anderson and Agarwal (2011) found that people that didn't have negative emotions towards their health were not able to predict the impacts of poor health in their willingness to disclose health information in the future, when the benefits would be much higher compared to the current state. Individuals with poor health need health care services the most but they might have the highest privacy concerns that can limit disclosure, but if they see the benefits they receive from the tradeoff they are more likely to use these services.

2.2.5 Research and health records

In the same way that companies rely on information from customers for their business, so do researchers rely on information collected of individuals for their studies. A research done in Canada found that 97% of people thought that privacy protection was important to them, and more than half of those surveyed indicated that their privacy concerns had increased in the last five years (Willison et al., 2007). It seems then that privacy concerns are something that have continued to grow in this era of new technologies and networking possibilities provided by the Internet, and one can expect that wearable medical devices will also contribute to the increase as well.

Some studies collect their own survey data or conduct interviews, but other studies rely on the access they are given to existing data about individuals. Willison et al. (2007) studied the privacy concerns that individuals have regarding disclosing their personal health information for research purposes, and for researchers having access to anonymized versions of their health information without explicit consent. The survey revealed that ninety percent of people had privacy concerns about having their health information used for research purposes without consent. Individuals want to be in control of their information and how it is being used as other studies have also found (Malhotra et al., 2004; Phelps et al., 2000). It matters to the individual how the information is being used and for what purpose. Willison et al. (2007) found that if health information was requested for the purpose of improving healthcare or tracking spreading of diseases then individuals were more willing to disclose information or give access to them compared to if information was requested for commercial purposes.

In addition to how the information is being used the organization that is requesting information does impact the individuals trust. Willison et al. (2007) found that individuals had higher trust towards hospitals, university researchers, and national statistics organizations, but on the other hand lower trust towards insurance industry, drug companies, and governments. A study by Rohm and Milne (2004) found that individuals have the highest privacy concerns towards insurance companies and employers, but they do trust their employers.

Overall individuals are willing to disclose health information or give researchers access to their health records, but individuals want to have a choice to opt-in or opt-out, as well as having the choice to change their consent later (Willison et al., 2007). Even though a high percent of individuals are willing to give access to their information either by one time consent or by consenting to each study separately, it is important for participants to have control over the choice concerning one's information. Willison et al. (2007) found that support for giving access to health information was much lower for electronic health records compared to traditional paper based filing system. They argued that there were higher privacy concerns for an electronic system because of the increased concerns for secondary use of the data. It matters to the individual how information is being used and by whom when they evaluate if they want to disclose information or give consent. Trust and control continue to be themes that resurface in the privacy research as factors that matter to willingness to disclose and privacy concerns.

Many healthcare providers have turned their paper records of patients to electronic systems to enable more efficient work, but this has at the same time raised privacy concerns to the individuals about their data. This type of data can be very sensitive and personal and includes things such as medical conditions, medications, family history, mental health, and demographic data. Digitizing data enables it to be accessed more easily and patients can be given access to their own data, but at the same time it has created privacy concerns. Angst and Agarwal (2009) and Rindfleisch (1997) have studied the adoption of electronic health records (EHR) systems and how individuals try to mitigate the

privacy concerns that come from these systems. Angst and Agarwal (2009) found that individual's behavior intentions towards adopting the use of EHR are impacted by argument framing, issues involvement, and by privacy concerns. Individual's attitudes and privacy concerns also impact the individual's choice to have their health records digitized when they are given the option to opt-in or opt-out (Angst & Agarwal, 2009). The study found that education about the benefits of EHR through positive messages helped to mitigate privacy concerns, even for those individuals that indicated to have high levels of privacy concern. In many cases individuals are not given a choice if their health records are digitized since this is a part of the evolution of health care and society as a whole. Education is one of the ways that privacy concerns could be mitigated, as individual's would gain better understanding of new systems and procedures. Health information is important for treatments and diagnosis, but individuals have many concerns specifically towards the information about their health (Andrade et al., 2002; Lwin et al., 2007).

2.3 Wearable technology

One technology area that is quickly growing is wearable devices such as activity trackers and smart watches. These devices enable the collection of a variety of information including; heart rate, steps, distance, and physical location. With the ability to easily collect and store information concerning one's health and activities it also brings potential privacy concerns. The following sections discuss the adoption of wearable devices, the importance of control over information, and the type of inferences that can be made from the collected data. Figure 3 has gathered the relevant concepts in the research area of wearable devices and privacy concerns and illustrates their interrelationships.

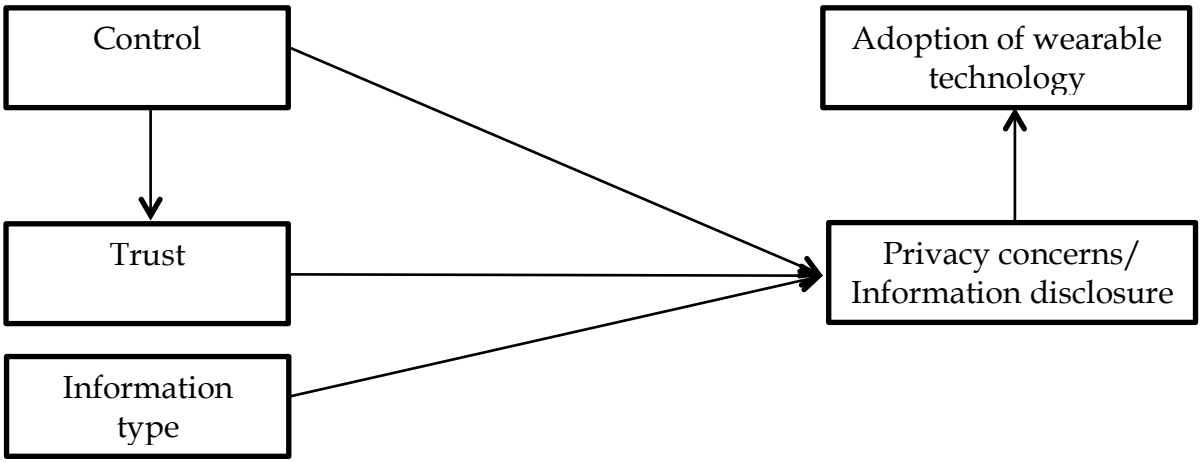

FIGURE 3 Synthesis of wearable technology research themes and their interrelationships

2.3.1 Adoption of wearable technology

In the category of wearable devices there are those devices that are used for tracking exercise and fitness and then there are devices that are more strictly for medical purposes. The intended groups for these devices are a bit different even though there is some overlap, so the adoption of these technologies shows some differences. Activity trackers and fitness devices are often designed for younger healthy people as the focus group, and wearable medical devices are geared towards elderly or individuals that have health problems. Of course the line between these two types of devices is not well defined, but the differences between adopting these technologies as separate categories have been studied (Gao, Li, & Luo, 2015).

Gao et al. (2015) found that those that would adopt fitness oriented device care about hedonic motivation, functional congruence, and perceived vulnerability, but on the other hand individuals adopting medical devices care more about perceived expectancy, effort expectancy, self-efficacy, and perceived severity. Adopters of fitness devices value the devices ability to motivate them to exercise more and they care about things such as the device being comfortable and durable. Gao et al. (2015) found that adopters of fitness devices care more about social influence and privacy risks, and argued that this was explained by the younger age demographics. Users of medical devices on the other hand value the effectiveness of the device to measure, how easy it is for them to use, and how it enables them to manage their own physical wellbeing. This difference makes sense since medical devices used at home can enable older individuals to reduce the amount of doctor visits, and the devices are used for managing health without a social aspect that a younger user would value (Gao et al., 2015).

Previous studies have found that poor health status would actually raise privacy concerns for disclosing information (Bansal et al., 2010), but this study found that actually the group with more health problems was not as concerned about their privacy when adopting new technology (Gao et al., 2015). Privacy calculus was used as part of the framework in the study to show that individuals consider the risks and benefits when considering adoption as it has been established in privacy calculus models (Culnan & Armstrong 1999; Dinev & Hart, 2006).

Other studies have continued to confirm that individuals perform privacy calculus when deciding whether or not to adopt a wearable health care device (Li, Wu, Gao, & Shi, 2016). Li et al. (2016) found in their study that perceived benefits of adoption could strongly mitigate perceived privacy risk, which is consistent with other studies on privacy calculus (Li & Sarathy, 2007; Xu et al., 2011). The study's findings showed that privacy concerns might be the most influential factor when individuals consider adoption of healthcare devices. Since there will always be privacy concerns and not all of them can be mitigated,

one of the approaches guided by privacy calculus is to offer better value for the users so the benefits are higher than costs or risks.

Li et al. (2016) discovered that health information sensitivity and a person's willingness to try new technologies did have a significant impact on the perceived privacy risks, which in turn impacts adoption. So individuals who consider health information to be more sensitive are also less likely to adopt a device that collects health information. Li et al., (2016) also found in their study that the company's prestige and legislative protection did have a significant impact in lowering the perceived privacy risks that individuals had. This is again another approach that can be used to mitigate privacy concerns and increase adoption of new technology and information disclosure.

Li et al. (2016) argued that based on their findings the three most important factors for user adoption of healthcare devices are; perceived prestige of the company, functional congruence of the wearable device, and perceived privacy risks. When an individual performs the privacy calculus process, the antecedents of risks were found to be health information sensitivity, prestige of the company, and a person's willingness to adopt new technology. The benefits calculus was driven by usefulness of the device and the value of the information that the device can provide (Li et al., 2016). Since privacy concerns cover a large spectrum of issues there are also many approaches to mitigate these as the findings from this research have shown. Since the privacy concerns won't disappear, companies might try to offer better value and build its reputation to attract new users.

2.3.2 Control and disclosure

The introduction and growth of wearable devices to the market has brought with itself new dimensions to privacy research and health care research. The impact of control to information disclosure has been explored also with wearable devices. A study was conducted in which participants used mobile phones and personal sensing devices for three months to gather information about themselves (Klasnja, Consolvo, Choudhury, Beckwith, & Hightower, 2009). Klasnja et al. (2009) attempted to see what type of concerns individuals had during the long experiment and how the type of information, context of the information, and perceived value impacted these privacy concerns. The goal was to see how individuals evaluate privacy and information sensitivity when they have had actually experiences instead of just providing evaluations on fictitious circumstances.

The study found that participants did not consider information gathered by accelerometers and barometers, which was used to measure physical activity, as sensitive, but physical location gathered by GPS was considered sensitive information by 42% of individuals (Klasnja et al., 2009). One's actual location even when it was not real time data can cause people to reflect on the possibility that someone might know all the places they have been and are likely to go in the future. Klasnja et al. (2009) asked the participants if they would be willing to use a wearable sensor that would also be able to continuously record audio

to which the participants responded almost unanimously that they wouldn't. Recorded audio had similar concern characteristics as GPS location and participants indicated they would be worried about being spied on and that this type of data gathering was too intrusive for them.

Klasnja et al. (2009) did discover that the length of time the data was stored as well as where the data was stored impacted privacy concerns. Storing information only for a few minutes for processing reduced concerns, and storing information only on the personal device that was used to gather the information also helped to decrease privacy concerns. The study also found that the context in which the sensing devices were used did impact concerns such as strict work environment or controlling spouse.

Participants evaluated the perceived costs and benefits when they evaluated the use of wearable sensors and which ones they would be willing to accept (Klasnja et al., 2009). Some of the health benefits can be gained from these devices even without GPS capabilities, which is something that users will consider when thinking of adoption of new devices. From the service provider and device manufacturer perspective this can be valuable information. They might consider limiting the capabilities of the devices to the intended purposes and if possible focus more of the information processing on the device itself. This approach of course would limit the type of data that companies can gather about their users, which is a part of the business model in some cases.

Patterson (2013) interviewed users of the Fitbit wearable device to understand their behavior and use of the devices as well as what type of concerns they have. Previous studies found that there are many types of privacy concerns users have, especially in the healthcare context, such as; insider abuse of information, secondary use of information, and outsiders' access to the information (Rindfleisch, 1997). Individuals in this study were found to mostly have their devices on them at all times to enable continuous tracking of their activity and steps, and many even kept them on during nights (Patterson, 2013).

This study found that users were happy that the devices lacked GPS capability as they had many privacy concerns about their location being disclosed to others, which finding is aligned with previous studies (Klasnja et al., 2009; Raij et al., 2011). Patterson (2013) discovered that users are sharing much more of their health and personal information with the service provider than they realize, and being made aware of this made users to question the reasons why certain information was necessary. A problem with these types of devices is that the individuals don't have a firm understanding of how their information is stored and handled, which has led to individuals purposely withholding information about their health and habits (Patterson, 2013).

Since users are not fully aware of the information privacy practices of companies it is hard for them to evaluate the trustworthiness of different companies providing tools and services for health tracking. Patterson (2013) found that individuals based the trustworthiness of the company on their business model, and not so much on their personal experience as they were inclined to trust a company that promotes health. Users grouped different types of organizations together in order to make evaluation of their trust beliefs (Patterson, 2013). Individuals might be prone to trust doctors and hospital for their health

care and they might consider these new technology companies providing health care tracking as a part of the same group of organizations.

Fair information practices can lead to better quality of health data and can contribute to the trust between individuals and organizations, but the lack of these practices can lead to withholding information or individuals providing false information (Hodge et al., 1999). Trust and the perception of trust has been found to correlate to more information disclosure in previous studies as well, and the lack of trust promoting processes can impact an individual's full adoption of a technology (Culnan & Armstrong, 1999; Dinev & Hart, 2003; Dinev & Hart, 2006).

The study also found that individuals disclose different amounts of information depending on the organization that is requesting it. Most interviewees chose not to disclose health information on social media as they saw that as something outside of the social norms (Patterson, 2013). Individuals were also concerned about providing their health information to law enforcement, insurance companies, employers, commercial research, and advertisers, as they perceived more potential risks. They felt that more harm than good could occur if they disclosed their information to these entities (Patterson, 2013). The impact of the requesting organization and the context and relevance has been found to impact privacy concerns in other studies as well (Rohm & Milne, 2004; Willison et al., 2007). Control over one's health information seems to be one of the key ways that privacy concerns can be mitigated, but also reforming and adding more regulations to the way digitalized health data is handled can lower privacy concerns (Hodge et al., 1999; Patterson, 2013).

Motti and Caine (2015) analyzed in their study the privacy concerns that individuals have concerning wearable devices. When using wearable devices users were most concerned about the GPS tracking of their location, and the risk that this information would be shared to other parties, which has been found in other studies as well (Klasnja et al., 2009; Patterson, 2013; Raij et al., 2011). Motti and Caine (2015) also discovered that users had concerns of other people around them using devices that take pictures or record audio, in which situation they are not in control of the information collected and shared. This finding is very interesting, as many studies have shown that control over one's information is one of the main ways to mitigate privacy concerns (Dinev & Hart, 2003; Hodge et al., 1999; Patterson, 2013; Phelps et al., 2000; Willison et al., 2007; Xu et al., 2011), but that the concern also extends to the control over information that others might gather of individuals.

Wearable devices that tracked health information such as heart rate, glucose, and steps were found to raise lower levels of privacy concerns for the users as other studies have also found (Motti & Caine, 2015; Raij et al., 2011). Motti and Caine (2015) argued that the lower levels of concerns could be attributed to the lack of awareness on how the health data might be misused or shared, since users might not be aware of the inferences that could be made. Overall, individuals were concerned about disclosure of their information if information was collected without their knowledge, and lack of control over who can access their personal information (Motti & Caine, 2015). GPS capability can be important for certain athletes but many regular consumers seem to prefer that this

feature is not present, as they do not see any provided value. If an individual wants to tract their health related information then physical location can seem to be not relevant, especially if this information is collected outside of the exercise periods.

2.3.3 Inferences from data

Not all privacy risks can be realized now, since with the use of machine learning and big data the previously collected data can be analyzed for new information. These risks are something that users most likely wouldn't consider, as these problems might not be realized until a later date. Raij, Ghosh, Kumar, and Srivastava (2011) have studied the privacy concerns that individuals have over the data that is gathered from wearable sensors. Sensors in the study could gather information from three broad groups including physiological, behavioral, and psychological data, and the analysis of the data enabled them to make different inferences about the subject.

Wearable devices gather information such as heart rate, oxygen levels, and GPS location, but Raij et al. (2011) demonstrated that these types of information can be used to infer other things such as; stress, use of alcohol or drugs, social connections and important locations such as were an individual lives. Raij et al. (2011) argued that subjects are not aware of the possible inferences that can be made from the data gathered by the sensors. With the use of current technology to analyze the data, an unexpected privacy risks are produced for the users of such devices. One group of participants wore sensors to gather data about them and was then asked to complete a privacy survey, after which they were showed analysis of their data and asked to take the privacy survey again. This was done to see if privacy concerns were increased as the participants became more aware of the use of the data. The second group of participants only completed a privacy survey without any analysis of the data collected on them.

Raij et al. (2011) found that individuals in both groups were the most concerned about the data that would tell about their exercise habits, places they commuted, when they had conversations, and stress levels. Those that wore sensors to gather data about them showed increased privacy concerns for all the different cases, and after they were shown the visualization of their data for only 15 minutes their privacy concern levels increased significantly (Raij et al., 2011). So when an individual adopts a wearable device they might be more primed to consider the potential risks that are associated with use and this can increases their privacy concerns. In addition, when users actively view their data it can also increase their concerns, as they might perceive some of the potential risks. Participants in the study were concerned that they were being tracked and that the data was revealing more about them than they hoped (Raij et al., 2011). This finding is aligned with previous studies that have found that physical location provided by GPS is considered to be very sensitive (Klasnja et al., 2009).

The study also discovered that participant's privacy concerns were the highest for the data that showed the time something happened such as a stress-

ful event and also the location where it happened (Raij et al., 2011). Time of event by itself did increase privacy concerns for stressful episodes, but together time and location had the highest impact to the privacy concerns. Raij et al. (2011) noted that even though individuals have privacy concerns for exercise habits, these were much lower than with the other three activities and the information for time and place of exercise didn´t increase concerns. This seems to indicate that wearable devices used for exercise purposes wouldn´t cause high privacy concerns, unless they are worn also during non-exercise periods in which case other data is being gathered.

Raij et al. (2011) also found that disclosure of information did increase privacy concerns and they were significantly higher if information would be disclosed to the public. It was also discovered that the group that had data gathered about them had even higher concerns when it came to disclosure of the data. This finding indicates that individuals have higher concerns for information disclosure if they have first hand experiences in information being collected. The most important findings of this study are that individuals are most concerned about the data that can be used to make inferences of their psychological state, and these concerns are increased when it is paired with location and time (Raij et al., 2011). The non-health related information collected by wearable devices does not cause high levels of concern that actual health information or physical locations do.

3 PRIVACY CALCULUS

One approach to analyze and understand human behavior when it comes to disclosing information is privacy calculus. The base for this way of thinking comes from mathematics and how individuals calculate or make assessments to determine their behavior. This chapter reviews the origins of the privacy calculus term and the development of the concept into a model used among information systems (IS) research. Prior research of the use of the model and its later extension will be reviewed and the usefulness of the model for the current research is evaluated.

3.1 Origins of privacy calculus

The concept of privacy calculus was first introduced in social sciences and the research areas focused on human behavior when using services that were working offline (Laurel & Wolfe, 1977; Milne & Gordon, 1993; Stone & Stone, 1990). Laurel and Wolfe (1977) used the term calculus of behavior to describe the individual's evaluation about their intentions. The privacy calculus idea developed out of these earlier researches and is defined as the individual's assessment of the costs or risks associated with the disclosure of their personal information, and the possible benefits they receive as a part of the exchange.

This assessment is not so much a calculation as it is a way to weigh the benefits and costs of a transaction, giving something up in order to receive something in return. An individual goes through this mental process somewhat automatically as they consider their future behavior. The consideration includes things such as, how is their information being used or for what purposes it's being collected. Then the individual considers the potential benefits for disclosing their information, such as using a service or receiving offers. This privacy calculus way of thinking enables people to consider if giving up something personal to them is worth it when they consider the potential benefits. Milne and Gordon (1993) found in their study that individuals consider the relationship between them and the target organization to have a social contract, which the

individual uses when evaluating the exchange between their information and the received benefits.

3.2 Privacy calculus development

Culnan and Armstrong (1999) were the first ones to use the privacy calculus concept with transactions between customers and organizations in their research. Their study was also the first to model privacy calculus and how it plays a role in the transactions between individuals and companies. Privacy calculus was defined in their study as the individual's evaluation of the benefits of disclosing their personal information and if they exceed the risks that they perceive (Culnan & Armstrong, 1999).

They found that when individuals were explicitly told that the organization followed fair information practices, the individual's concerns for privacy were diminished (Culnan & Armstrong, 1999). This fairness was found to represent trust between the organization and the individual and in turn helped the individuals continue their relationship with the organization. This was an important discovery since companies need customer information for competitive advantage, so it's beneficial for companies to alleviate any concerns an individual might have.

Following these fair information practices was found to build trust, which in turn allows the organization to collect more information about their customers as they continue the relationship (Culnan & Armstrong, 1999). As long as the firm behaves the way they have described in their information policy the customer will continue to gain trust and continue disclosing more information. If a firm's practices are not fair and the customer perceives the risks are too high, they will depart and the firm loses the future information gathering possibilities (Culnan & Armstrong, 1999). It's important to mitigate the privacy concerns so that the perceived benefits are higher than the potential risks, so the individual will continue to disclose their information as a part of the transactions.

3.3 Privacy calculus model

The privacy calculus theoretical framework developed by Culnan and Armstrong (1999) was expanded by Dinev and Hart (2003) by modeling the trade-off factors users consider. These factors include the perceived personal benefits and the privacy costs that an individual would experience. The definition of privacy calculus they used focused on the judgment that an individual makes when considering the potential negative impacts of them disclosing their personal information (see figure 4). These impacts included things such as information misuse, access by other parties, or other potential negative effects to the person (Dinev & Hart, 2003). The natural extension of the previous privacy calculus model created by Culnan and Armstrong (1999) was to test it in online

setting instead of general transactions between customers and companies that had been done prior.

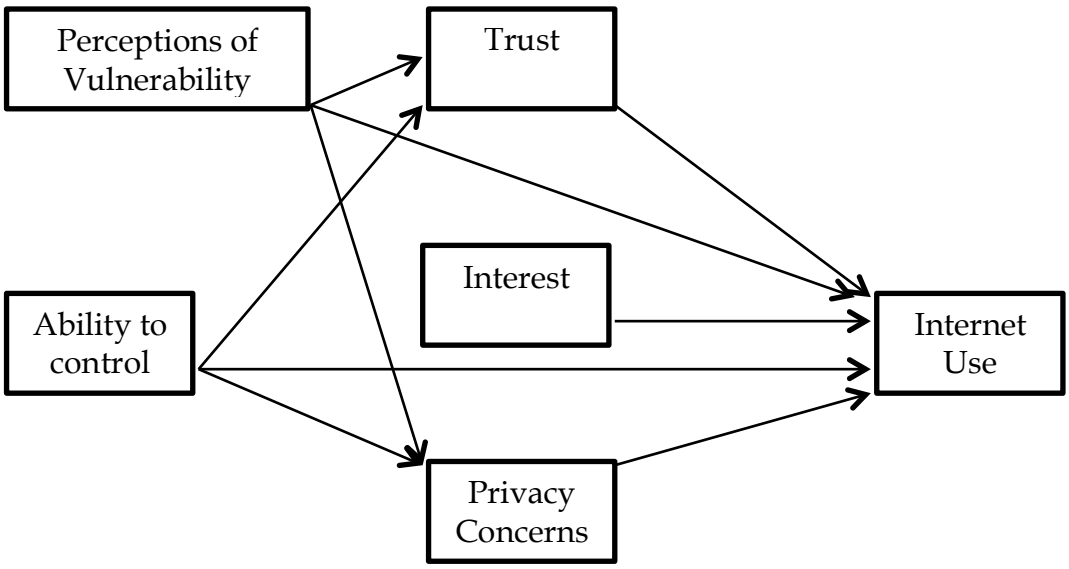

FIGURE 4 Privacy calculus model of Internet use (Dinev & Hart, 2003)

Dinev and Hart (2003) studied how privacy concerns impact the individual's Internet use, which is turn, impacts their use of e-commerce sites and further the disclosure of information. They also found that having a perceived ability to control the information helped to diminish privacy concerns. Giving individuals control or at least the perception of control is an important factor when risk-benefit calculus is done. As was found in previous research, Dinev and Hart (2003) confirmed that trust plays a central role in an individuals use of Internet and in turn e-commerce sites (see figure 4).

Organizations can enable disclosure of personal information if they can develop trust (Culnan & Armstrong, 1999). One of the ways that trust can be developed is by the use of fair information practices as discovered by Culnan and Armstrong (1999). Dinev and Hart (2003) found that trust was the strongest aspect that impacted the person's use of Internet, since there are risks associated with disclosure of information and these should be mitigated to increase transactions.

Dinev and Hart (2004) in their subsequent study focused on only three parts of the earlier model and their impact. This study explored the impacts on perceived vulnerability and perceived ability to control, and their relationships to perceived privacy concerns. Perceived vulnerability was found to have a significant relationship to the privacy concerns that an individual might experience, but on the other hand control had only a moderate relationship to privacy concerns.

The study identified the two factors that drive privacy concerns as information access and information abuse (Dinev & Hart, 2004). As a person is going through their decision-making process (i.e., privacy calculus) they consider how

accessible their information becomes if they disclose it for online service, and then how the information can be misused for something other than what they intended (Dinev & Hart, 2004). Control is an important factor when determining trust and privacy concerns, but this study highlighted that from the privacy calculus perspective the cost and risk factors in the decision-making process might be more important. It can be important to offer control to mitigate some risks, but if risks or cost for disclosure are perceived to be very high compared to the benefits then even offering control might not be enough.

3.4 Extended privacy calculus model

Dinev and Hart (2006) introduced the extended privacy calculus model (see figure 5), which focused on e-commerce transactions and expanded further the work of Culnan and Armstrong (1999) as well as their own previous model (Dinev & Hart, 2003). In place of costs and benefits as the antecedents of privacy calculus they used risk beliefs and confidence and enticement beliefs (Dinev & Hart, 2006). These risk beliefs were specific to the privacy of the person submitting information as a part of the e-commerce transaction. It includes things such as sharing information to third parties and misuse of information by unauthorized access or theft. Confidence and enticement beliefs used by Dinev and Hart (2006) included things such as trust, reliability and safety of the transaction environment, and intrinsic motivation.

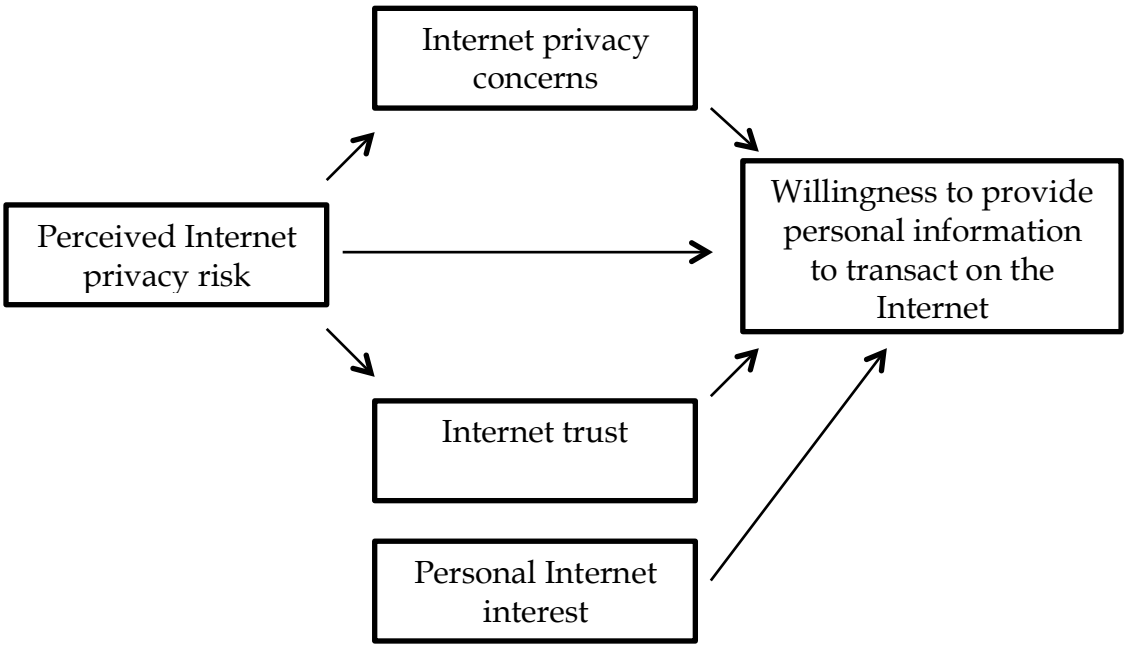

FIGURE 5 Extended privacy calculus model (Dinev & Hart, 2006)

They found that trust and personal interest together had a larger impact on the disclosing of information than did the privacy risks by themselves (Dinev & Hart, 2006). These findings backed by the extended model confirmed that a person's privacy worries can be mitigated, and they might also behave differently than their reported privacy preferences due to other factors. This point is important for the research discussed in a later chapter as individuals are interviewed concerning their privacy beliefs through their previous experiences. Websites and e-commerce can benefit from the understanding of how individual behavior can be evaluated and the privacy calculus they use to determine their information disclosure.

The extended privacy calculus model was retested with some changes by Dinev et al. (2006) by doing a cross-cultural study between Italy and the United States. The newer model gave more focus on the aspect of trust by dividing it into propensity to trust and institutional trust to better understand the privacy calculus process (see figure 6). Propensity to trust is described as the individual's inclination to trust people. Institutional trust on the other hand includes things such as the reliability, trustworthiness, and experience.

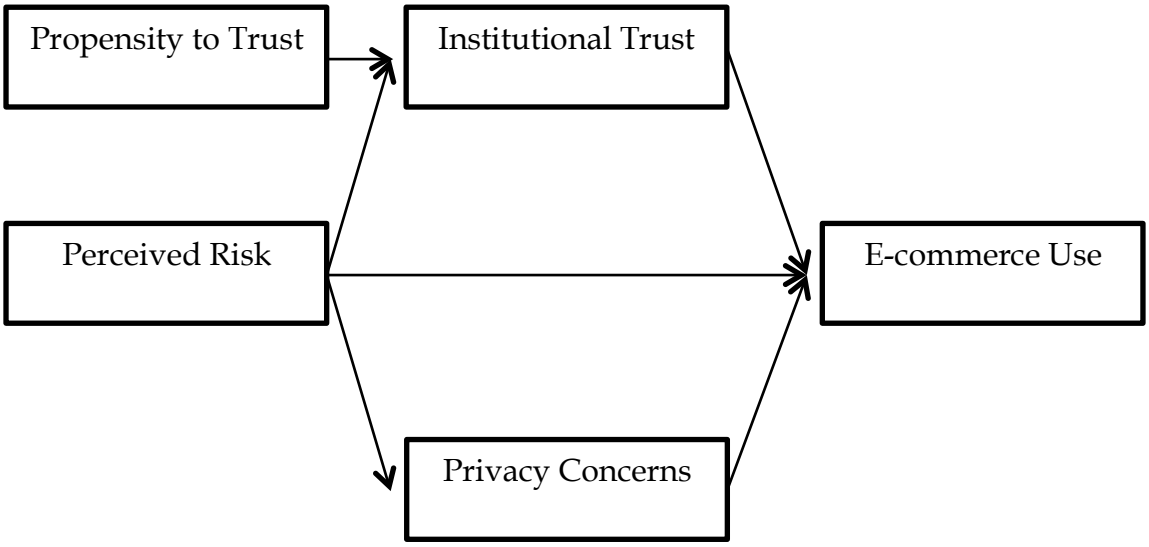

FIGURE 6 Privacy calculus model with enhanced trust (adapted after Dinev et al., 2006)

This study further validated the privacy calculus model (Dinev & Hart, 2006) and showed how it can be used in different context when evaluating user behavior in e-commerce transactions and website use. Dinev et al. (2006) also confirmed the findings of their previous study that trust has more of an impact than the perceived risk when an individual is going through their decision making process. They did found that there are some differences between low-trust societies like Italy and high-trust societies such as U.S., but in both cases trust building enable an increase in e-commerce use (Dinev et al., 2006).

3.5 Privacy calculus model in research

Privacy calculus theory has been used in multiple studies to learn how people behave in different situations. Li and Sarathy (2007) in their research concerning disclosure of personal information and the privacy calculus decision-making process argued that there exist situation specific factors that the individual evaluates. These factors have not been an integral part of the previous studies on privacy calculus, but still confirmed that the individual does an evaluation between the risks and benefits. Li and Sarathy (2007) included factors such as the type of information that was being collected, the nature of the website itself, and privacy beliefs that are formed as a part of the interaction with a website in a specific situation. The underlying privacy calculus thinking is still the same, so the individuals perceived benefits have to be higher than the potential risks in order for them to disclose personal information as a part of a transaction.

It was found that if collected information was highly relevant it helped to mitigate the privacy risk beliefs, but monetary rewards actually have a negative impact on disclosure (Li & Sarathy, 2007). Perceived benefits of the transaction combined with the perceived privacy protection beliefs were found to mitigate the privacy risk in privacy calculus, and lead the person to disclose their personal information. Li and Sarathy (2007) also found that fairness of the information practices did impact disclosure by increasing it, confirming the findings of Culnan and Armstrong (1999) of the importance of fairness to mitigate privacy risks. Their findings are also parallel to those of prior research that indicate that when an individual is disclosing personal information as a part of a transaction they consider that there is a implicit social contract, which indicates that the information practices are fair (Culnan & Armstrong, 1999; Milne & Gordon, 1993).

Privacy calculus model has also been used in a location-based services (LBS) context. The study explored the impact of different types of privacy approaches and their impact on the decision-making process (Xu, Teo, Tan, & Agarwal, 2009). LBS enable individuals to receive services based on their location, but it also requires them to disclose information about themselves for the service to work. In this study, compensation, industry self-regulation, and government regulation were explored as possible approaches to mitigate the privacy risk beliefs users have, and in this way they expanded the existing privacy calculus model. Industry self-regulation was found to have significant impact, but the other two approaches' significance depended on the type of information delivery mechanism that was used (Xu et al., 2009). These align with the findings of Li and Sarathy (2007) that found offering rewards don't help to mitigate privacy concerns. Prior experience was also confirmed to impact the user's privacy calculus process, especially if they had experienced undesirable consequences (Xu et al., 2009).

Similarly to the previous study, location-aware marketing (LAM) and personalization has been studied with the use of privacy calculus model. LAM requires the user to disclose personal information to a mobile application, specifically their physical location, so that they can receive personalized advertise-

ments and offers based on their location. Xu, Luo, Carroll, and Rosson (2011) looked at the personalization privacy paradox with the use of privacy calculus model and tested the impacts of personal characteristics and types of marketing approaches. Previous privacy invasion experiences, a person's willingness to try new technology, and tendency to respond to offers were characteristics that were hypothesized to impact the individual's intent to disclose information (Xu et al., 2011). The two marketing approaches present in the study were overt and covert, overt requires the user to request offers and covert works by the company pushing notification offers to the individual without a request.

Users are more willing to disclose information when offers and services are personalized, since they perceive them to be more valuable to them (Xu et al., 2011). Xu et al. (2011) also found that individuals that are more willing to try new technology were also more willing to disclose personal information and had lower privacy concerns. Previous privacy invasions and a tendency to respond to offers were found to mitigate privacy concerns when overt marketing was used, but the findings were opposite in a covert marketing approach. Xu et al. (2011) argued that when users are given the chance to request offers in the overt approach they perceive to have more control and in turn have less privacy concerns, which finding is in line with prior research (Dinev & Hart, 2003).

Impacts of personalized services in mobile applications and a willingness to disclose personal information have also been studied in other contexts. Wang, Duong, and Chen (2016) used the privacy calculus model to understand the disclosure of personal information inside mobile applications and explored the psychological and contextual factors that could impact the decision-making process. These factors included perceived severity and risks, perceived benefits, and the impact of personalization as a contextual factor.

Wang et al. (2016) found in their study that perceived severity negatively influenced the retention of a customer and the trust between the individual and the company, which has been seen in other studies (Culnan & Armstrong, 1999; Dinev & Hart, 2003; Dinev & Hart, 2006). They also argued that users lack the understanding of the potential risks associated with mobile applications using cloud, which leads to the discrepancies between perceived risks and actual risks. One finding that differed from previous studies was that higher perceived control did increase the perceived risks in some cases (Dinev & Hart, 2003). Wang et al. (2016) extrapolated that this finding might indicate that when it comes to users of mobile devices, their high levels of perceived control is associated to high levels of awareness of the potential privacy threats. When user perception of risk and severity was low the perceived benefits had a higher impact on the choice of the individual to disclose personal information (Wang et al., 2016). Overall, benefits were more impactful than perceived risk to the disclosure of personal information. Personalization features did show increase in perceived benefits of the applications, and lowering the perceived severity of disclosure did have a positive impact (Wang et al., 2016).

3.6 Privacy calculus model used in this study

The extended privacy calculus model by Dinev and Hart (2006) was chosen for the present study (see figure 5). This model captured the topics that would be in the study and offered a good foundation for the study. The present study focused only in parts of the model, including perceived privacy risks, perceived privacy concerns, and how these impact willingness to disclose personal information. The goal of the study is not to build a new privacy calculus model, but to explore if privacy calculus model can be used in the study of the use of wearable devices and specifically the disclosure of health information that they collect.

To better illustrate the goals of the study a simplified version of the privacy calculus model is shown here (see figure 7). This illustration only includes the parts that were focused on the present study. The previous privacy calculus models have look at the impact of different factors to the disclosure of personal information when interacting with online services, but this study looks at how the privacy risks and privacy concerns impact an individual's willingness to provide their health information. The study specifically looks at the health information that is collected with activity trackers and smart watches.

FIGURE 7 Simplified privacy calculus model

The privacy calculus theory and the model were used in preparation of the interview themes and questions. The privacy calculus theory was also used as the theoretical lens to analyze the collected interview results to see how risks and concerns impact individuals. Part of the analysis was to see if individuals consider the risks and benefits of sharing their health information to different parties or organization when making the choice to either disclose or to withhold information. The fit of the model and the subsequent findings are explored in the discussion chapter of this thesis.

4 RESEARCH METHOD

This chapter discusses the research method used for the collection of the empirical data and the following analysis. Data collected for this study was through interviews and the strengths of this qualitative approach are discussed in the following sections. Following the descriptions of the method, the research process is described and the interview setup and process is explained. Appendix 1 has the interview outline that was used for the interviews.

4.1 Choosing the method

This study uses a qualitative research method and analyzes prior research with use of established theory as a background and its empirical material is gathered through interviews. According to Saaranen-Kauppinen and Puusniekka (2006) qualitative research is based on these factors as well as the addition of researcher's own thoughts and reasoning. This methodological approach enables researchers to analyze the words, expressions, and situational aspects of the interview, but there is a risk that personal bias or presence in the interview will impact the results (Hirsjärvi & Hurme, 2011). Even though the qualitative approach doesn't produce statistically significant information, the analysis of the results can provide some generalizability in understanding the phenomenon (Saaranen-Kauppinen & Puusniekka, 2006). Since the study focused on a phenomenon that is reasonably new, this research approach was found to be the most suitable in order to answer the research questions.

The goal of the study was to understand the subjective experiences individuals have had with relation to wearable devices and their health data. This type of information can be gathered through individual interviews, which enable the participant and the researcher to interact naturally through conversations. Interviews are a scientific method that enables the gathering of information concerning the experiences and thoughts of participants (Hirsjärvi & Hurme, 2011). Interviews are often used as a qualitative method to gather in-

formation from a few selective cases, which can help to understand a phenomenon or individual perceptions.

Compared to quantitative method, which often has larger group size, interviews do not produce results that are as generalizable since the goal is to understand some phenomenon more in depth by gathering information from only a few cases. According to Hirsjärvi and Hurme (2011) using the qualitative interview method enables the voice of the individual and their experiences to be heard. It was important for this study to understand how participants perceive the privacy of their health information based on their own actual experiences or in hypothetical situations that mimic those of their real experiences.

Hirsjärvi and Hurme (2011) explain that interviews are useful in order to understand the motives behind answers that participants give as they have a chance to explain their reasoning, for example how they evaluate the sensitivity of different types of information. A survey method would enable the gathering of numeric evaluations of information sensitivity, but interviews enable the ability to discover why certain information is perceived to be more or less private. The interviewer also has the ability to ask further questions and lead the discussion in order to discovery more rich details behind an individual's answers. Of course the behavior, gestures, and expressions of the interviewer can have an impact on the situation to simultaneously encourage disclosure, but the interviewee might also feel the need to give socially acceptable responses (Saaranen-Kauppinen & Puusniekka, 2006).

4.2 Semi-structured interviews

Themed interviews were used in this study, which are also known as semi-structured interviews or focused interviews. Hirsjärvi and Hurme (2011) developed themed interviews, which are similar to semi-structured interviews but in addition, the interview outline follows different theme areas that guide the interviewer and interviewee. Semi-structured interviews have some set topics or questions that are going to be asked, but doesn't follow step-by-step questions such as surveys. This type of interview gives the interviewers an outline to follow to make sure important questions are asked but gives room for changes and further questions based on the answers given.

Themed interviews focus on certain themes that are relevant to the research topic and have guiding questions or lists of words to help the interviewer (Hirsjärvi & Hurme, 2011). This type of method ensures that important topics are discussed but gives a lot of room for the interviewer to ask different questions based on the answers the participants have given to previous questions. This interview style is also more casual in its approach, which allows the interviewees to freely discuss their personal experience in depth and not be restricted to short answers for a list of questions. Interviews are conducted to find information that can then be used to develop a hypothesis, not to test an existing hypothesis (Hirsjärvi & Hurme, 2011).

Themed interviews are also suitable when studying a topic that might not be well known since asking a set of questions might limit the responses given (Saaranen-Kauppinen & Puusniekka, 2006). Themed interviews give the interviewees room to freely express themselves and their thoughts instead of answering only given questions. When conducting semi-structured interviews it requires the interviewer to be familiar with the research area so that important themes can be recognized. The benefit of this interview approach is that the interviews can be analyzed based on the themes selected, but new themes might also emerge from the data analysis (Saaranen-Kauppinen & Puusniekka, 2006).

Semi-structured interviews were a way for this study to encourage individuals to fully share their personal experiences, so that their responses could include rich details. The goal for the interview approach was to provide interviewees an environment in which they can express their true feelings towards privacy and information sensitivity without having to be asked directly how they would rate the sensitivity of different types of information on a scale. This approach was chosen since studies in information privacy have shown that an individual's stated privacy preferences don't match those of actual behavior (Ackerman, Cranor, & Reagle, 1999; Berendt et al., 2005).

The themes for the interviews emerged from the study of prior research and were guided by the privacy calculus theory. Relevant and frequently mentioned topics from the related research articles were selected as suitable themes for the interviews following the best practices of planning themed interviews (Saaranen-Kauppinen & Puusniekka, 2006). Privacy calculus theory was used as the theoretical lens for the study and the aspects of control, risk, and privacy concerns were included in the themes of the interviews.

This interview approach made it possible for participants to not be primed to think of information privacy. It gave possibility for interviewees to bring up the topic of privacy themselves in the case they had concerns or previous experiences that would relate to it. The interview questions were meant to guide the participants to evaluate information sensitivity, especially their health information, without asking them how private they would rate it. If the interviewees didn't express any thoughts on privacy concerns then during the last theme of the interview they were asked their feelings towards privacy and were asked to consider hypothetical situations. This interview type gave the possibility for the individuals to express their thoughts freely and tell stories since the interview was only guided by the planned themes.

4.3 Conducting interviews

The following section describes the interview process for the conducted study. After the initial interview themes and guiding questions were developed, three preliminary interviews were conducted. The participants were chosen from individuals who had some familiarity with the goals of the research in order to provide feedback and suggestions. These interviews were conducted the same way as the actually data gathering was planned to take place in order to mimic

the upcoming situation as much as possible. These interviews were recorded the same way, as the later interviews would be. After the interviews, the participants were given time to give feedback on the content of the interview and how it was conducted.

This round of preliminary interviews was valuable as it gave confidence and experience for the interviewer, but also the feedback was used to improve the questions and flow of the actual interviews. It also helped to ensure that the themed identified with the use of privacy calculus theory were fitting and interviews provided answers to the research questions. The results discussed in the following chapter do not include the responses from the preliminary interviews. Their responses were very similar to that of the actual interview group but their previous knowledge of the study and its aims could impact the results.

The empirical data for this study came from ten interviews that were conducted during September and October of 2016. The study was advertised in a social media group for individuals interested in running, and also a few flyers were posted on the university campus. These approaches produced four participants and the other six were individuals that the researcher approached personally. The aim was for the interview part to last 45 minutes since some additional time was sometimes required by the participants to travel to and from the place of interview. Also, some time was spent on small talk before the interview to get familiar and comfortable with each other. The interview time goal was accomplished as the average interview lasted 43 minutes. This amount of time enabled the discussion of themes in detail but it also limited the time required from the participants and helped to motivate participation.

Since the study had time and resource constraints, only ten people were interviewed for the study. As a token of appreciation the participants were also offered a free movie ticket for their time. This was used to motivate individuals to participate in the study and methods such as this are often used, since individuals receive many requests of their time. Most of the participants had agreed to the interview before they knew that they would be compensated for their time with a movie ticket, so they were driven by personal interest instead of the compensation.

The interviews were scheduled to take place in a location convenient to the individuals, which would also have low levels of distractions. Participants were told that the interview is about their personal experiences on the use of activity trackers or smart watches. As previously mentioned, it was chosen by the researcher not to tell participants that the focus of the interview is on privacy, so that the participants wouldn't be primed to answer all the questions with this in mind. The latter part of the interview asked specifically about their feelings towards privacy, but this was done after the participants had ample time to mention these concerns themselves.

The interviews followed the themes and questions prepared, but the order of questions and topics varied between individuals based on their responses and thoughts (see appendix 1). The interviewer allowed the individuals to express their thoughts as they came to capture any unexpected subthemes that were not planned. The first part of the interview focused on how the individual uses their device, what type of information it collects, and how the individual

makes use of the data. Next, the interview focused on how information is being stored and the access of the information from the device, mobile application, or cloud service. This was followed by discussions on how the individual shared their collected information with others, and in what type of situation they would be willing to give their information for the use of another party. During these topics any privacy concerns were noted and individuals were asked to explain the why behind their answers. The last section dived into privacy and asked the individual to compare different types of information such as financial and health information and have them explain any privacy concerns they might have and their implications.

4.4 Data analysis

Interviews were recorded with two recorders to guarantee that the discussion would be stored and that in the case of technical problems at least one device would function properly. Participants were asked permission before recording to which everyone agreed. The interviewer also took some notes on paper to highlight things that would be important to notice during transcription and analysis. This included things such as interesting expressions or concerns towards privacy that were noteworthy. According to Hirsjärvi and Hurme (2011) the researcher should record relevant details of the interview situation and environment that could be beneficial in later analysis.

Transcribing the interviews was done during the following days to keep the material fresh in mind and to enable the start of the analysis soon after the last interview. According to Hirsjärvi and Hurme (2011) material should be processed and viewed promptly after it has been gathered so the task of transcribing and analysis won't be as laborious. Interviews were transcribed from the recorded audio to text editing software and divided into the interview themes. Each participant was assigned a color so the responses from different participants could be gathered under one topic, but to be able to identify the participants from each other.

The interview themes were chosen based on the prior research and guided by the privacy calculus theory. The transcribed material was then divided into relevant sections that followed the themes and questions of the interviews. Data analysis started by first looking at the transcripts of the interviews and the chosen themes. The material had answers to the research questions and provided details on different aspects of the privacy calculus theory. According to Saaranen-Kauppinen and Puusniekka (2006) when data is organized and coded, the analysis process attempts to find answers to the main research questions and the supporting questions that the researcher developed as a part of the study. These questions might not be fully answered or they might have more than one answer, meaning that the variations of the individual's responses have to be taken into account and the data shouldn't be forced to fit the research question.

According to Hirsjärvi and Hurme (2011) starting analysis early can enable the researcher to think about the material from a high-level before going

into the details of the analysis. This analysis approach is considered a strength in qualitative research, as it's not necessary to wait until all data is gathered before analysis can start. To follow this recommendation the researcher did some high-level analysis after conducting each interview as it was being transcribed.

The interview themes captured much of the interview content, but it was necessary to create further sub themes during the analysis and writing of the results. For example, during the discussion of control and disclosure of information there was a wealth of material so it was further divided into sub-themes that each covered one organization that would potentially request information. Individuals also expressed many types of privacy concerns so this theme was divided into sub-themes that would gather the material based on some aspect such as misuse of health information. When conducting data analysis in qualitative research, certain topics and concepts emerge from the data as frequently mentioned ideas, but this requires the researcher to ask questions from the data (Saaranen-Kauppinen & Puusniekka, 2006). These additional categories and themes gave clarity to the analysis and improved the interpretation of the results.

The privacy calculus theory provided the theoretical lens that was used to analyze the recorded data and to identify answers to the research questions. The strength of themed interviews is that it gives the researcher the possibility to approach the data analysis from different directions and using a variety of approaches (Saaranen-Kauppinen & Puusniekka, 2006). Due to the in-direct nature of some of the questions in the interview, some expressions were analyzed to identify if participants expressed privacy concerns without explicitly saying it. Interpretation of meaning is something that is often used in qualitative research to find attributes that do not come directly from the spoken words (Hirsjärvi & Hurme, 2011). This means that there is some speculation on the part of the researcher concerning the possible meanings or hidden sides of things said.

Once the material was organized, read through, and analyzed, the next part was writing. According to Hirsjärvi and Hurme (2011) research papers often only present the findings, but don't provide the researcher's interpretation of the findings. The researcher is supposed to give meaning to the findings and to indicate why they are relevant. This shows that the findings have some value either for a group of people or for further research. More detailed analysis of the material and its implications are reported in the discussions chapter. The discussions chapter also compares the findings of this study to prior research reported in the earlier chapters of this thesis.

5 RESULTS

The previous chapter described how the study was planned and conducted. This chapter continues from that by describing first the demographic information of the interview participants and then explaining the results of the study. The results discuss the different themes and sub-themes from the interviews and how the participants expressed themselves. The results discuss how the participants used their wearable devices and what kind of benefits they have received from the use. Then the results discuss how participants share their information on social media or to other organizations. Lastly the results discuss the participants' perceptions of information sensitivity and the types of privacy concerns and risks they have.

5.1 Interview participants

Table 2 highlights some of the demographic details of the research participants. The table (see table 2) also includes information about the participant's self-evaluation of their activity level and how long the participants had used their wearable device.

TABLE 2 Demographic information of the ten study participants

Demographics	
Men	4
Women	6
Ages 19 to 30	4
Ages 31 to 50	6
Students	5
Employed	3
Both	2

Activity Level	
Levels 2 to 3	2
Levels 3 to 4	4
Level 5	4

Length of Use	
Less than 12 months	4
12 to 18 months	3
More than 18 months	3

There were a total of ten participants, which consisted of four men and six women. Ages of participants ranged from the youngest of 19 to the oldest participant being 50, which well represents the activity tracker users in the adult population. Five individuals were full-time students, two individuals were students who also work, and three individuals were full-time employed. Participants represented a variety of backgrounds in their study or work area. A few individuals were studying or working in health related areas such as physical therapist, sports massager, or exercise sciences. Two individuals were studying in technology related fields and the rest were involved with fields such as English language, teaching, social studies, and management. The interview group presented a large age range with differing backgrounds, which made them a rich source of experiences.

Participants were asked to rate how active they were on a scale from 1 to 5, starting from "not very active" to "active every day". Four of the participants rated themselves a level five and explained the types of sports or exercise they do on an almost daily basis. Another four individuals rated themselves between three and four indicating that they did some type of exercise or physical activity multiple times a week. Two individuals consider themselves to be at the level two to three, indicating that they exercised only some during a given week.

Eight participants were currently using some type of wrist worn activity tracker and two participants had a smart watch, which offer additional features such as receiving text messages or notifications. From the perspective of gathering health data both of these groups of devices are similar, and the main difference was that two of the activity trackers didn't have GPS capability. The devices were also from five different manufacturers and included different models, which further increased the diversity of the group.

There was also a difference in the length of time individuals have had these devices in use. Four individuals have had their devices from a few months to less than a year. Three individuals had used their devices between one year and one and a half years. The last three had used their devices longer than a year and a half. When all these aspects are taken into account, the group represented a diverse group of individuals, which increased the reliability and validity of the findings as similar concerns or thoughts were found among participants.

5.2 Use of the device

In the beginning of the interview the participants were asked to explain how they use their device in their daily lives. Table 3 highlights some of the physical activities they participate in and have found their devices to be of use for. Walking, jogging, and running were the most common activities among the participants as these were something that everyone did at some point. Two other common activities were biking and gym or weight training, which most of the participants did occasionally.

TABLE 3 Types of physical activities

Activity Types	
Walking	Skiing
Jogging	Gym
Running	Weights
Biking	Golf
Swimming	Futsal

During the interviews, participants were also asked to list the types of information that their wearable device collects. These information types are listed in table 4, which are all common among the wearable devices. Not all the devices offered all the functionalities on the list, but this is an aggregate list of potential things that the devices could collect.

TABLE 4 Information types collected by wearable devices

Information Types	
Steps	Sleep
Distance	Time
Speed	Activity level
Heart Rate	Burned Calories
Location	VO2 max

Devices are often used as wristwatches and then in active use during the exercises or training activities. Outside of these times the devices passively collect and calculate activity levels, which are shown as a number or percent for the user on their devices screen. One of the concerns that was brought up by two participant was that step counting, which in turn impacted daily activity levels wasn't being measured accurately outside of exercises. This issue made it so that these individuals didn't find as much use for the devices except during training periods.

Participants enjoyed and found it useful to receive feedback or information during their exercises and for many, this was the main reason to purchase the device. Being able to see one's heart rate (HR) during training was the most important feature and the reason individuals had bought a device that can measure HR from their wrist without needing a chest strap. Been able to see average speed or pace was also useful information during running and biking. One of the participants said the following concerning the use of their wearable device:

> I purchased an activity tracker because I wanted to measure heart rate during exercises and using a chest strap is uncomfortable. An activity tracker is already with you as a watch, so it's easy to turn on the heart rate functionality during the exercises.

Information was viewed from the device right after the exercise to make sure that the activity is saved. Many of the participants review their daily activity levels in the evenings, and also at the end of the week when they synchronize their devices data to their smart phone, computer, or cloud. One user described the use of their device in the following way:

> I use the information during exercises and then download the graphs to my phone. Then I'm able to see in what heart rate ranges I have been exercising. I also write notes about my training that I can use later when comparing my exercises.

Not all the participants were certain if their information is also being stored to a cloud service provided by the manufacturer, but most assumed that this must be the case. Most devices offer a companion mobile application that stores the data from the wearable device and also enables the user to modify the data and make additions such as missed exercises. Most device manufacturers provided cloud service with an online interface and most the participants used this service at some level, but less than the mobile application.

Most of the participants wear their device during the entire day, but take it off for sleeping. Most of the devices offer some form of sleep tracking, but only two individuals wore it regularly during nights. Most of the other participants had tried the sleep-tracking feature, but don't use it at all or rarely. The two main reasons not to track sleep was that participants didn't find the information useful for them and the second hindrance was that the devices were consider large and bulky and interfered with sleeping.

There are also some other occasions when participants are not wearing their devices. One of the participants said they take the device off during extended periods of sitting, the reason being that the device is quite large and heavy. Other times the device was taken off was during some exercises that limit wearing watches and jewelry such as martial arts. Two participants were unable to wear their devices during most working hours as they were doing physical therapy and massage and the device would be in the way of their work. One user described it in this way:

> I mainly use the activity tracker for measuring my heart rate during jogging and check the steps count while I'm wearing it. I'm unable to use it at work because it's in the way, so for almost 10 hours per day I can't use it. I had a different tracker before, which I actually wore on my ankle to measure steps, but that wasn't very accurate.

Two participants keep a rest day during the week from their exercises to give time for their bodies' time to recover. During these resting days they choose not to wear the device at all because they knew they wouldn't reach the daily activity level goals that the device shows. They preferred not to see the low activity levels during these days as this might cause them anxiety and make it harder not to do more physical activity. Also some of the devices give notifications if a person doesn't move enough to encourage to get moving and this was found to be useful, but not desirable during the resting days.

5.3 Benefits from use

There were some differences between the reasons the participants had purchased their device and the benefits they had received were also quite broad. None of the participants had purchased the device to motivate themselves to move more, but even though this was the case some of them had received motivation from it. One of the participants found it useful to see their calories burned, as this enabled them to adjust their daily eating when needed. The information provided by the device helped some to do longer runs or exercises, but for many it improved the quality much more than the quantity. One of the participants stated the benefits of an activity tracker in this way:

> Having an activity tracker has allowed me to drop the intensity of my exercises so I am able to be more efficient. This has lead into better recovery after exercising, but has not changed the amount of time I spend training.

Still there were some individuals who noticed that when their activity level values were low in the evening, it would motivate them to go for a walk, or to extend their evening exercise. Having the information about their levels easily visible on their device made them aware of their daily activity and provided some form of motivation, and also some devices would give notifications to users to encourage them to move more. For many, the device motivated them to move more after the initial purchase, but overtime their activity levels didn't continue to increase, but the device continued to support the existing exercise routines. A few of the participants said that trying to reach the daily activity goal did keep their motivation up, and the device helped them to have something measureable to reach towards. Greater awareness of one's exercises and training was the most mentioned benefit of using their device. One of the participants had some unexpected motivation from the activity tracker:

> Sometimes in the evening I check the steps count and if it's only a few thousand steps for the day I go for a longer walk with my dog. The tracker does have some impact and gets you to move more.

Participants valued the ability to see concrete information about their exercises. For some of the participants being able to see the number values or graphs from the mobile phones companion application was important since there was something they could look back to and something they could record. One participant said how sometimes they would forget to take their device for a run or to start the exercise on their device, which afterwards made them feel like, why did they even go for a run if they couldn't record it to their daily activities. Two of the participants shared how the devices increased their awareness of the lack of physical activity. They had previously estimated how much they move and walk and how many calories this would burn, but after starting to use the device they realized that they had been overestimating their activity levels.

Having values provided by the device during the exercises made the activity more enjoyable to some as they could see progress and this kept their mo-

tivation going. Most of the participants would compare their daily or weekly activity levels, and some would actively compare individual training sessions with each other to gain additional insight. Data being available on a mobile application or online was a useful feature for many, since this enabled them to see the values in visual format. This also enabled them to see the full exercises and the values associated with it.

Participants were asked in the interview if they have evaluated their own health based on the information provided by the device, or if one could do so with this information. None of the participants had evaluated their health or medical conditions specifically, but had used the information to evaluate their fitness level or how good of shape they were in. One user explained it by saying:

> I have not evaluated my health based on the information. With the collected information you can see the amount of exercising, their intensity, and heart rate levels, which tells about the shape you're in and also something about your health.

Many raised the concern that the information collected by the devices is not accurate or relevant enough to truly evaluate one's own health. One participant said that by looking at the activity type and the collected HR during it, one could evaluate the state of a person's health. One participant talked about how when they have flu symptoms they perform an orthostatic test with their device to be able to better evaluate how their health is doing.

One of the participants in the study had previously been a professional athlete and still trained vigorously. For this participant the device had helped them to learn that many times they train too hard, and they could get better performance from their training by decreasing the intensity to the appropriate level. This in turn enabled them to have better recovery from exercises, which improved their subsequent training sessions. Others who had somewhat regular training routines found HR data to be the most useful so they could focus their training to the desired HR range. This enabled them to have a mix of high and low impact exercises by making sure they don't train too hard all the time.

In one part of the interview, participants were asked if would like to collect additional information about their health such as oxygen saturation, blood pressure, or other health information either with a wrist worn device or some other medical device at home. Many found that this additional information wouldn't be useful for them, but many indicated they would have interest to do so. When asked if a long term illness would change their thinking most indicated that then they would be even more willing and interested to collect this information themselves. One of the concerns that came up many times was that the information provided by a wearable device needs to be in a useful format, since just number values don't provide value for many users unless they are given context such as what levels are normal or desirable.

5.4 Sharing on social media

The participants in the study were asked about their willingness to share information they have collected with their wearable devices to different purposes. Table 5 below highlights the findings, which are discussed in the following sections in detail. Wearable devices often have a companion application that works together with the device or an online portal that one can use to access their collected information. One of the features that these have is sharing information about one's exercises to others. Information can be shared to different social media outlets such as Facebook, but also some device manufacturers have created their own service, which allows users with similar devices to share with each other. During the interview participants were asked if they have been sharing through these services and about their thoughts on sharing the information they have collected with their wearable device in social media.

TABLE 5 Willingness to share information

	Yes	No
Social media	1	9
Doctor	10	0
Medical research	10	0
Occupational health services	8	2
Device manufacturer	7	3

Out of the participant group, only one individual shared information about their exercises on social media (see table 5). This person would take screenshots of some of the exercise statistics they had done and post it to social media. They also belonged to a group on social media made of running enthusiasts, in which they would share their activities. This participant also had created a personal profile to the service provided by the manufacturer, which enables individuals to send requests in order to follow other users. This individual had a few friends that followed their exercises and were able to see all the data related to their activities. In turn the data of these friends was visible to the participant, but not public for others. This participant also had an informal trainer or mentor that gave suggestions on their training and they had login information provided for them to access all the information including any past historical data.

Other participants in the study ranged from individuals that use and share on social media very little to those that engage actively, but still choose not to share information about their exercises. For many, they saw no benefit from sharing information about their exercises on social media. They preferred to keep the information to themselves and for many they thought that the information would be of no value to others if they chose to share. Participants saw that talking about health is something you do with friends and family, but in regular conversations outside of social media.

Few of the participants expressed a willingness to share if they would have friends that would have activity tracking devices, but even for these individuals they would prefer to share in a closed group. These groups would consist of family members and friends who also own activity-tracking devices. One participant saw this as a great feature as it would bring an aspect of competition and good social pressure to move, but the drawback was that none of their family members or friends had a device from the same manufacturer. The participant described the problem in this way:

> None of my friends have an activity tracker and because of this the social aspect is missing. I could see that I would move more if there would be this social pressure, which could motivate me.

One of the participants expressed concern that anything posted on social media is public and that's why they choose not to share any exercise related information. Another participant said that it's a private matter when one goes to the gym, so it's something they want to keep to themselves. One participant had concerns of sharing exercise information or pictures from their exercises, as they were worried about potential negative comments. Comments such as the lack of progress or their physical appearance and because of this, they keep information about their exercises as private matter. This participant expressed their concern:

> If I go to the gym five or six times I don't want to get negative comments about my lack of progress. People might expect that I would have the ideal body because I go the gym often, so I don't want to see the comments. In the end, it is a private matter if you go the gym or exercise.

One participant said that they think about their privacy when it comes to using online services such as social media. They choose not to disclose any personal information such as birthday, physical locations, and what they might be doing and when. They are not as worried about the information they have provided during the process of registration to these services, but how the information that people post and share can end up being used for other things. Their rule for sharing on social media was that they share only things you would be willing to yell publicly at a market.

5.5 Benefits from sharing with doctor

Sharing one's activity tracker information with a doctor was found to have perceived benefits to the participants as well as some concerns. Even though the participants hadn't shared any of the collected data with their doctor they saw it as something they could potentially do, but they also had some concerns if data is shared with the doctor online without any human interaction.

During the interview the participants were asked about their willingness to share information collected by their wearable devices to a doctor and if using

such a device could decrease the frequency of visits to the doctor. All the participants were willing to share the information collected by their device with their doctor (see table 5). None of the participants had brought up their use of activity tracker with their doctor during past visits, but they would be willing to give the doctor access to the data if asked.

Many participants raised concern that the information would not be very useful for the doctor, but it might be something that the doctor might want to store as a reference if needed at some later point. All the participants considered themselves to be basically healthy so they couldn't see what benefit would come from a doctor seeing their activity levels or HR, but they had no problems in providing this information if asked. One of the interviewees said the following:

> I don't know if the information would be useful for the doctor. Is there any use for the information about how much I have walked? I could share this information with the doctor because I have nothing against the doctor having it.

Participants saw that someone with an illness or medical condition could benefit from collecting information with the wearable device or some other medical devices and then providing this to the doctor for use. Participants expressed their willingness to collect additional health information about themselves and providing it to the doctor if they would have a health condition that would benefit from the additional information.

> If I would have an illness then I could collect additional information and share it with my doctor. If there is any benefit from you collecting information and sharing it with the doctor of course it's worth doing.

Using activity trackers and doing self-measuring at home with other devices was seen as something that can improve the current situation with medical care, but cannot replace doctors. Two of the participants considered that using an activity tracker can help an individual to live a more active life, which can help them to be less sick or to avoid injuries from training and this could lead to going to the doctor less often.

Most of the participants saw that potentially, this type of self-collection of information that is then transferred to the doctor could decrease the amount of doctors visits needed. This was found to be useful, especially for those individuals that have an illness or condition that requires frequent visits just for measurements. The benefits would be that it would take less time to do measuring at home instead of needing to schedule a visit to the doctor. Participants saw that especially with smaller problems it would be convenient to be in contact with the doctor through some online service and provide them with data collected with their device without needing to visit a health center.

One of the participants said that the reason activity trackers and similar devices cannot replace a doctor is that you normally don't go the doctor because of your HR. They explained that you go to the doctor because of getting sick and that the activity tracker data wouldn't be adequate for the doctor to

diagnose the patient. Activity tracker data could be use as a support, but a person would still need to see a doctor.

5.6 Concerns from sharing with doctor

One of the concerns that participants expressed in the example of self-measurement was that someone at the health center would need to actively look at the data and send replies to the individual. It would require someone to actively look at the incoming information so they the individual's would get feedback if something was wrong.

Others raised the concern that there would be a high risk of measurement errors especially with elderly individuals that would attempt to take measurements at home. These wrong values could lead into misdiagnosis, which could lead into worsening the condition. One of the participants explained the benefits and concerns of self-measuring:

> A doctor can make a wrong diagnosis if they base their judgment on the self-measured information, but at the same time it would be possible to be in contact with the doctor about less severe problems. It would save time if you don't need to schedule a time to visit your health care center.

One participant also expressed concerns that health information sent to the doctor would be evaluated only by a machine running an algorithm and not by a real person. There were also concerns that especially the elderly would have problems with the use of devices and transmitting the data to the doctor. These individuals would need clear instructions and training on how to use devices. One of the participants had worked in elderly care and visited homes and helped to measure blood pressures. This individual had seen how poorly many elderly individuals used these devices causing measurement errors and potentially causing them even panic as their measured values were outside of the expected ranges. One interviewee explained their worry about the elderly using self-measuring devices:

> The change to self-measuring needs to be done in a human way, so that the job of looking at your information is not taken from the doctors and given to some algorithm. Activity trackers should be used as an aid, so that especially the elderly can continue to have an understanding of their own conditions.

The idea from many of the participants was that activity trackers could be useful devices to support healthy lifestyle changes, which leads into fewer illnesses and fewer doctor visits. Few of the participants raised concerns that activity tracking devices themselves are not enough to motivate people to make long term changes in their lifestyles, but can help to support by motivating and creating awareness.

Few of the participants also expressed concerns on the lack of social interaction with the doctor if the health care model would move into self-

measurements and interaction through online services. Especially challenging it was seen how this change would impact the elderly, as they might not be comfortable with technology. One of the participants recognized that health care would likely move to more self-measuring and in time individuals will become more comfortable with this model. They also saw that by the time younger people get older they would have the skills to use the technology so that they would be comfortable with them even at an old age.

5.7 Sharing for medical research

Participants were also asked in the interview if they would be willing to give the information they have collected with their wearable device to medical research. Participants were given an example of research in cardiovascular health and how the information could be used to find new treatments. Everyone was willing to provide their information to be used in such a way without any hesitation (see table 5). One interviewee said the following:

> Information collected by the activity tracker is quite general and nothing personal. I would be willing to give it to research since I have nothing to hide.

Some had concerns that information would need to be kept private and confidential in order for them to feel comfortable. One participant was in general willing to give their information, but said that it mattered what organization asked for it. Another participant was willing to give if the requesting organization was someone official or a well-known company, but would be hesitant to provide to some individual researchers. One of the participants explained it in this way:

> I would give my information to be used in medical research if it is useful. They would just need to maintain my privacy so that information would not be used for the wrong purposes.

One participant expressed concern that they wouldn't want their information to end up into some marketing organization, but they would be willing to take the risk to be able to help other people. For another participant it was important that they were just one of the subjects of the study as they weren't comfortable that someone would just look at their individual data. One individual had a preference that information would be provided without their name, but this was not a determining factor for them.

5.8 Sharing with occupational health

During the interview the participants were described a scenario and then asked about their thoughts and willingness to participate. In the scenario their employer would provide the participant a new activity tracker and the data from the device would be transferred to an occupational health provider. Participants were asked if they would be willing to wear such a device and what positive and negative aspects this could have.

Most of the participants would be willing to use an activity tracker or at least consider it with some conditions (see table 5). Some of the participants right away expressed concerns of the given situation and everyone was able to think of multiple negative aspects once they were asked to think about potential risks.

The participants saw this scenario as something positive as long as the intensions would be to help people and this would be expressed transparently. They saw the value that providing such as device could motivate individuals to be more active, but at the same time it might not be encouraging for someone that is not very active. For this reason, using one of the devices should be a choice instead of a requirement by the employer. One participant explained the benefits by saying:

> If information collected with the activity tracker is used for the benefit and improvement of health for the individual, then I would be willing to use a device.

The important factor for participants was that the data would only be sent to an occupational health service provider as they already handle employer's health information. Participants expressed trust towards health service providers and that they wouldn't intentionally disclose patient information to the employer. The concern that most had was the employer might somehow get access to the information and because of this risk some of the participants would choose to not to use the device. Few participants had worries that the employer might choose to promote only those individuals that are physically active, which would punish those in worse health. It was also expressed that this information could be used when determining which individuals are laid off if a company is downsizing:

> If you would not take care of your health and end up with a lot sick leave this could impact your employment. These aspects could impact your job in a negative way because the world is an uncertain place.

Even though participants thought of these potential risks, they considered them to be not very likely to happen and that the benefits are higher than potential risks. There were two participants that wouldn't want to take a device from their employer as they felt like then the employer would feel like a custodian to them, or they didn't wish to receive any additional help from occupational health concerning their exercise habits. One of them explained their thoughts:

> I'm cynical about sharing my information or giving it for use of the occupational health. You don't know were the information ends up and how it might be used.

5.9 Sharing with a device manufacturer

Participants were asked if they would be willing to allow the manufacturer of their activity tracker to use the collected information to improve their products and services. Some companies might already be doing this, but the participants were asked if they were given the choice, would they allow their information to be used in this way or not.

Most participants were willing to have the company use their information for improving services and products (see table 5). Some of the participants did think that this is what the companies are most likely doing now, even though they aren't aware of it. Still this didn't cause them any worries even though companies might be doing it. One participant said that their information could be used for personalized services or marketing as long as their personal information is not shared with outside parties. One of the interviewees said this about sharing their information:

> There is nothing secret in the information I have collected with my activity tracker. I'm a bit skeptical about companies collecting my information, but I would be willing to share the collected information.

Two participants said that they probably wouldn't give access to their information, and that they often choose to give only mandatory information during registration for a new service and choose the option not to have their data used for other purposes. One individual had multiple email addresses so they could use different emails with different services and only give their most personal email address to important services.

One participant expressed concern that whenever you use a mobile application or other service you have to give them permission to use your information and potentially even give access to other information on your phone or laptop. They felt that it is inevitable that their information is going to spread and for example be used in direct marketing. They didn't see this as causing them any major harm, but was seen as more of an annoyance.

A few of the participants said that they have no worries how the manufacturer of the device would use the information as they couldn't see anything that would be harmful to them, but they had concerns if some other party would get their information. One the users explained their thoughts in this way:

> I'm not worried about how the company might use my information, as I don't see that there would be any harm to me. Even though the information is not important, there still needs to be a reason for the collection of my information.

The manufacturer sharing the information with it's partners or other parties had mixed results. Some accepted that the manufacturer can share this information if they are transparent about to whom it's getting transferred to, while others had concerns that their information could end up being spread to other parties that have no good reason for having it.

5.10 Information sensitivity

During the interview, the participants were asked to think about the type of information that their wearable device is gathering and to evaluate how personal, private, or sensitive it is. Many of the participants had discussed their feelings towards the sensitivity of their information even before they were specifically asked, but during this part of the interview the participants were asked to focus on this aspect.

Participants described the information collected by their devices as not sensitive, not secret, not confidential, and quite general. No one saw that the information the devices were collecting to be sensitive, but they still expressed some concerns. Participants saw that the information told about their exercises, training habits, and HR and these types of information is nothing private to them and doesn't identify them.

Many had no worries for whom would get access to the information as they saw no harm to them. One participant felt that the information was quite useless and criminals for example wouldn't have any use for it, but still they wouldn't want the information to be given to just anyone. One participant said that they don't have anything to hide and this is also what others often say, but they still think that it matters to people if their information would spread to the public. One the participants said this about the information collected by their activity tracker:

> I'm not worried about someone looking at the information collected by my activity tracker. You could probably find my information also from different records, but this does not concern me.

One person described that the data would tell where they live, when they sleep, where they go during the day, so there is an aspect of sensitivity. This is possible because many of the devices have GPS functionality that tracks physical location, which risks were mentioned by other participants as well. The individuals described how someone could track or follow them by the use of this information, but they saw this as being very unlikely and they weren't concerned about it. Another participant expressed their thoughts that other mobile applications also gather location data even without asking, so this information is already available to other parties. One interview described their thoughts in this way:

> A criminal could follow my jogging with the use of the information, but I see this as unlikely. Why me? No one wants to follow me because I'm not interesting. This could change if I would become famous or would go into politics.

A few of the participants described the information collected by their wearable devices as just numeric without any strong connection to the individual, so it's not harmful or meaningful for someone else to see. They did have slight concerns if the data would be accompanied with their name and address. One participant wasn't concerned about their physical location being collected as they figured that someone wanting to follow them or steal something from them could get their address information from some other service. One participant talked about how they are irritated that their information is being collected everywhere and they try to protect all their information even though it's not sensitive, just because of the principle that it is their data.

5.11 Comparison with medical records

To understand how sensitive and private individuals perceive the data collected by their wearable device, they were asked to compare the collected information with the information stored on their electronic patient records that doctors have (see table 6). There was a clear distinction between these categories to the participants as they saw them quite differently. Participants saw the information collected by a wearable device as numerical and general and the information that the doctor has is written from verbal conversation and more specific.

TABLE 6 Wearable device information compared to medical records

Wearable Devices	Medical Records
General	Specific
Numerical	Text
Not personal	Identifiable
Exercise habits	Medical conditions
Not private	Private
Not sensitive	Sensitive

One participant described how the information from their device doesn't tell much about them, but the information from the doctor's records is more sensitive, private, and detailed about their physical health. One participant did note that the information that the doctor has is medical history so it's past things, but activity tracker creates new information all the time and it's a better descriptor of the current situation. Still, the participants consider their patient records as more sensitive because of the potential content, such as illnesses or medication

that might be recorded there. One participant explained their thoughts about the difference:

> You go to the doctor when you need help with something so the information is quite specific. Activity trackers on the other hand only collect general information.

Some of the participants expressed concern that the doctor has information such as blood type and other lab results, which are very sensitive and very specific factors of one's health. The main difference that was brought up by the participants was that patient records include information that is not in numerical format that describes details about the person. These include written details about procedures, details about personal discussions between patient and doctor. This is the information participants thought to be the most sensitive and private and as something that the activity tracker doesn't have. One user described the difference between numerical and written information:

> General information about your health such as blood pressure doesn't matter if it goes to someone, but it matters if you discuss personal problems with the doctor. It is not the numerical information that is important, but the personal things.

5.12 Comparison with financial information

To better understand how individuals perceive the sensitivity of their health data, participants were asked to compare the information stored in their patient records to their financial information. Examples of financial information were given such as account balance, income, paid taxes, and loans. The goal was to see which information type was perceived as more sensitive and private and for what reasons.

This is an area that there was no consensus between the interview participants as some valued one type of information above the other (see figure 8). One participant felt that their financial information was more sensitive and personal than their medical records. For them it was a personal matter, for example, how they use their money and the things that they buy and this is something they don't want others to know. For another participant financial information was more private as they perceived that there would be more harm if people would know about their financial situation. They explained that if someone would find out how much money you have they could somehow take advantage of this information, but information about you having diabetes is very hard to misuse in any way. Two more individuals perceived that financial information is more private and sensitive, as they wouldn't want people to know about their finances. For them they saw that there would be less harm if their medical information would be made public. They explained it in this way:

> Of course financial information is more private than the information that the doctor has. You don't want your health information to be public, but financial information is more private.

When considering your health information to financial information (income, paid taxes, and loans), which do you think is more private/sensitive?

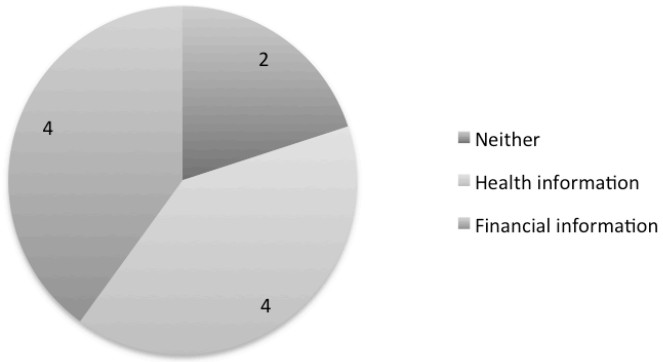

FIGURE 8 Comparing sensitivity of health and financial information

Two participants didn't consider financial or medical information to be very sensitive and in turn had no worries about people knowing about them. One of them explained that a person could find out salary and tax information about another person from public sources if they would want to. They saw that there was nothing in their financial or medical information that would cause them any harm if disclosed.

Four individuals perceived that their health information is more private and sensitive compared their financial information (see figure 8). For one participant they felt that health information tells more about them as an individual than does their financial information. For another participant they felt like even though there is nothing to hide, their medical records are more sensitive because there's potential that something could be stored in them. One participant expressed concerns that if someone's medical information would go public it could impact their insurance fees and their employment.

All the participants were asked if their evaluation between these categories of information would change if they would have some long-term illness and potentially use medications. For all the participants except one, they considered that in the given scenario their health information would be more sensitive (see figure 9). Those that had first given priority to financial information thought that given this scenario, the information stored in their medical records would have greater impact if disclosed to the public. Those that were uncertain before or had evaluated health information to be more sensitive thought that in the given scenario the value of the health information would be even higher. One participant perceived that even in the given scenario they still felt like their financial situation is more private to them and they would wish this information to be kept confidential. This participant described their thoughts like this:

> Financial information is more private. It's a private matter. I would prefer to keep it to myself compared to health information even if I had a long-term illness.

If you had a long-term illness, which information would you consider more private/sensitive?

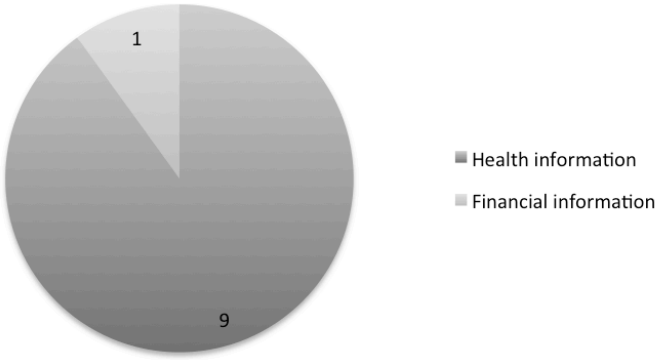

FIGURE 9 Health information sensitivity when long-term illness

5.13 Privacy concerns and risks

During the interview the participants expressed different privacy concerns that they had and also talked about the risks that comes with use of wearable devices or having health information in electronic format. During the entire interview, the participants were encouraged to more fully explain if they brought up any concerns. Then during the last theme of the interview the participants were asked directly about their thoughts on privacy. Some of the privacy concerns and risks have already been discussed in the previous sections briefly, but this section gathers all the different aspects together.

5.13.1 Misuse of health information

Participants were asked if they have worries about misuse of their health information. One participant said that they have no concerns about how their health information is being stored and that we have accepted all the risk as a group that comes from digitalization. They also had doubts that anyone would even want to access their health data or that the data could be misused in some manner. When this participant was asked to whom their health data would be of value, they stated, banks and insurance companies. They expanded by saying:

> How could they misuse the information? Banks could use it when making decisions about loans. Insurance companies could use it to determine if they make payments according to the policy. They're digging up this information already and the customer always loses. Having health information in all electronic formats of course has increased its availability to them.

One participant discussed their experience with interacting online with their health service provider during which they were asked to schedule an appointment. They never made an appointment and they expressed that the reason was

that it was easier to decline when they had no face-to-face interaction with the health care provider. They didn't have any concerns towards someone misusing their health information, but they explained that a person that is good with computers could potentially get access to their health information as well as their bank information and take their money and information.

During one of the interviews, a participant discussed that if a person's health information would be leaked then that could potentially impact their employment situation negatively and also the way other people think about them. Another participant talked about digitalization of health information and considered that the benefits are higher than the risks that come with it, but this completely digital world does bring them anxiety. One participant expressed no feelings of risk associated with electronic health data, but saw that it had made life easier and that information can be more easily shared when needed.

One participant expressed concerns about their privacy and how their medical records are all in electronic format only. For them it was scary that they didn't know where their records were physically located since it was in electronic format. They considered that misuse is easier with electronic records, but they saw the benefit of a digital fingerprint, which would be left if someone were accessing their data, which would not happen with paper records. They described it in this way:

> In some ways it's concerning that all health information has been moved to digital format. It's scary that the information is just stored somewhere and we don't know where this place is. Paper records were probably misused, but digital health records have made the information more accessible for others to misuse.

This participant also had concerns that we have become so reliant on computers and how losing one big server could destroy information that could not be recovered. They saw this especially worrisome if someone, for example, has important health information that is needed for their care. They also expressed concerns that this is a problem with financial information as it's all in electronic format and there are no paper bank statements anymore. These aspects made them feel like we don't have control over our information as we had when things were in paper format also and individuals for example had a physical bankbook that would show their account balance.

5.13.2 Security breaches and physical location

During the interview the participants were asked to consider if there were a security breach at the company they have purchased their activity tracker from and how this would impact them. None of the participants said that they would stop using their device if their information would have been stolen from the company, but for a few it would impact their future purchases.

One participant discussed that security breaches happen occasionally and it doesn't mean that the company has done something wrong. They expect the company to fix any issues to avoid further problems and this is an acceptable risk for them. They said if there would be reports that the company is purposely

misusing the customer information such as selling it to other parties, or doing something ethically or morally wrong such as using sweatshops to build these devices they wouldn't purchase from this company anymore. This participant explained security breaches like this:

> An isolated security breach is not the fault of the company. I mean that they have not done something really wrong, but they have just been too careless.

Another participant found it amusing that a criminal would end up with their activity tracker information as they saw that it would be useless for them. A security breach wouldn't impact them in any way and they considered that functionality and availability of services is more important when choosing to purchase a device than if there has been some previous security issues. One participant had high trust towards the manufacturer of their device and considered that there are no risks to them or harm from a security breach. They trust the brand and considered them to be trustworthy as they had a large user base.

During the interview one participant explained that security breaches are not so serious. These are events that happen frequently and it's something that everyone needs to accept as a part of the modern world. They explained that we would need to limit our every day life in many ways if we are not willing to accept the security risks. One of the participants said that they think people wouldn't change their bank even though there would be a security breach, so in the case of wearable devices and health care there is the same principle that these types of things happen but their impact is not high. One participant explained the small impact of breaches like this:

> If for example credit card information is being stolen and misused it doesn't impact just me individually. These types of incidents impact a whole group of people, so it's something that you just have to live with.

Social media and especially Facebook as a platform was mentioned multiple times during the interviews as there was discussion on data sharing. Most of the participants expressed concern that some outside party might misuse information they share on social media, meaning that they don't consider it very likely that Facebook would misuse their data. Participants had trust that Facebook takes care of the information they have provided during the registration process, but they saw that someone could potentially misuse the information that they have personally shared or posted. Two participants discussed how Facebook might use information that they have posted for targeted advertising or financial gain, but they didn't see this as a concern that would impact their use.

Many of the wearable devices have GPS capabilities either built-in to the device or they take advantage of the GPS of the user's smart phone. This functionality brought concerns to a few of the participants as they thought they could be potentially tracked or followed. One participant expressed concern that their location data might be collected secretly without them knowing and their movements could be followed. At the same time they didn't perceive this to be very likely to happen. Another participant expressed concern that their

location data could be used to follow them or to plan to steal something from their home when they're gone. They also considered that this type of scenario is not very likely, but this is a small risk that exists. One of the interviewees said:

> It's always possible that someone is secretly collecting your location information. Then a group of intelligence officers can track your movements, but this is highly unlikely.

One participant talked about their location data not being that sensitive since they as a person aren't interesting to someone else. They thought that if they would become more well known or choose to be in politics they would think differently about the sensitivity of their location data. Similar to the previous comment, another participant said that they have nothing to hide in their life, so it's not a big thing that someone could get access to their GPS data. For them it was not very likely someone would want to follow them when they go jogging.

5.13.3 General privacy concerns

During the last theme of the interview there was a lot of discussion about privacy in general and how the participants perceive it in their lives. One participant said that they were somewhat worried about privacy since their information is being stored in many places and they don't know if someone tries to get access to their information. They did express general trust toward services and thought that they are doing good job protecting people's information. Another participant wasn't too worried about privacy, but they did mention that they try to limit the amount of information they give to different places online. For them it was a useful way to protect their privacy, but limiting how much information they are storing to online services. One participant expressed their feelings like this:

> With new services you think about the information you give, but there are many applications that you need to use. You just have to agree to the terms and let them share your information. Information seems to spread either way.

One participant talked about how there are always risks when using a service or device such as an activity tracker. They explained how many services that are offered for free, collect the user's information and sell it to advertisers. The participant expressed dissatisfaction with this behavior from companies, but they accepted that this is the way they work. This is how they described it:

> I understand that when I use free services that my information will be collected and then they sell my information to others. It does not feel good, but I have accepted that this is the way services now work.

The perspective from another participant was that they don't know what the risks are as their understanding of digital technologies is limited. They said that they don't know what to be worried about, as they don't understand the harm that they could experience if someone accesses their information. They talked

about not reading the terms and conditions of a given website, but just hoped that those terms wouldn't have anything about hidden fees as this is something they found to be unacceptable. This participant said this about terms and conditions:

> I have not really read the terms and conditions to different services. I trust that if a service has a lot of users and is well known then I don't need to worry. I don't know if anyone reads the terms for services they use.

For them, direct marketing didn't cause any concern since that is expected to happen, but they did limit the amount of information they give if a website is unfamiliar to them. This participant also had an example to illustrate that they don't know the potential harms and that privacy is not something they worried about. They had a virus on their computer that would post explicit content to the walls of their Facebook friends when the user would log in with their computer. This participant thought it unfortunate and would get comments from their co-workers, but still continued to use the infected computer, as they didn't know how this could harm them. They explained their view like this:

> I don't really think about privacy often. I don't feel like there is anything secret about my life, so I don't think it's a big thing if someone wants to track me.

One participant mentioned being a bit worried about their privacy and they have had experiences where a new website or service had asked too detailed information from them and because of this they had chosen not to use the service. This participant also said that they don't agree if terms and conditions for a service mention that they share information with third parties, but don't actually specify whom the parties are. For them it was important to know who will get access to their information, even though in principle they had nothing against sharing information. They said this about third parties:

> It's more likely that some outside party would misuse your information compared to for example Facebook. I'm not worried about Facebook using my information, but other parties that might get access to it.

For another participant the aspect of control and transparency was also crucial. They think about how their information is going to be used when registering for a new service. They also explained that they do most of their daily activities on their smart phone and they are somewhat worried that there is so much information stored in one place about them. They said that they access many services with that one device including online banking and the information from the phone might be collected by applications. They accepted that there are these risks when using online services and mobile applications, but had worries about were their information could potentially end up. This is how they described it:

> It makes me worried how information about me is being collected and used. I do almost everything with my phone like online banking and rarely use a computer for

> accessing services. I know applications on my phone collect information about me, but I have accepted that there are risks.

Another participant was very cynical about all the potential third parties that might get access to their information and how they might be using it. They recognize that they leave a trace wherever they go and that someone might look at all the things they have done and places they have visited. For them there are many potential risks that come from someone getting access to their information, but still these risks don't impact their use much. This participant mentioned that identity thefts happen all the time and these criminals get information from many different places including Facebook. They talked about sharing on social media:

> I think about privacy with online services like social media. You should not put anything personal in there such as birthdate, where you live, or when you are going to different places.

Another participant was bothered by services selling their information to marketing, but thought that it would not likely cause them harm. They also mentioned thinking about privacy when new services are introduced, as there will always be bugs or problems during the transition to a new platform. This participant mentioned that they always read the terms and conditions, but reliance on online services did cause them anxiety. They described their behavior like this:

> When I register for a new service I rarely give my full name and I have multiple email addresses to choose from depending on how important the service is to me. It's not worth giving personal information for a service that you don't think the information is relevant.

One of the participants wanted to avoid risks to their privacy by not saving their password to the computer and by limiting the places that get their information, even their email address. When they specifically considered giving their health information for a service they would do so if there were direct benefits for them, but wouldn't if there were a risk of negative consequences to them. This is how they talked about privacy:

> I'm a bit worried about privacy because you don't know where someone can get access to and take your information. There are some services where I have stored some private information, but I think that services in general are pretty good at protecting your information.

5.14 Summary

Since there are many types of individuals, there is also many ways that one can use and benefit from a wearable device. Participants often wear their devices during the whole day and take it off during the night. Devices are used to check

activity levels during the days and evenings and other information such as heart rate (HR) is followed during the exercise periods. Even though participants had not purchased their activity trackers as a motivational tool they still saw at least short-term improvements. Quality of training was improved with slight changes to the quantity, as the participants were able to exercise in correct HR levels.

Figure 10 below incorporates the simplified privacy calculus model that was used in this study and highlights the relevant findings for each section. The lists are not exhaustive but focus on the frequently mentioned privacy risks and concerns and for what purposes individuals are willing to disclose their information (see figure 10). Most participants do not share information about their exercises in social media as they see them as a private matter and perceive no benefits from sharing. On the other hand they are willing to give the information they have collected to their doctors or medical research. They are also willing to collect additional information and provide it to the doctor, but for many they saw no benefit from doing this in their current situation.

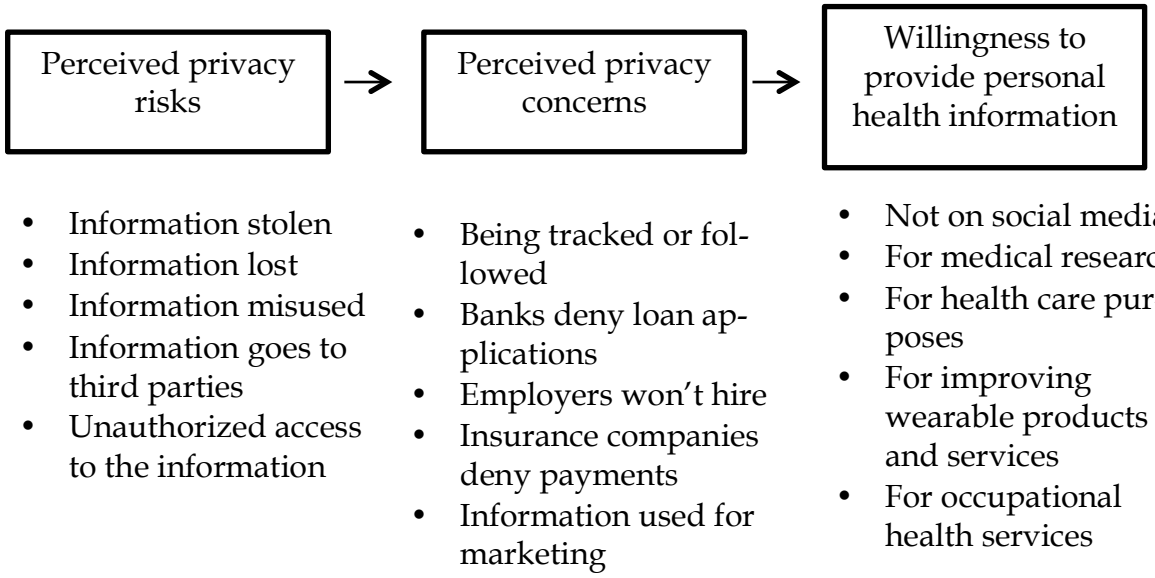

FIGURE 10 Simplified privacy calculus model with findings

Using a wearable device given by an employer to improve employee health was seen as a good idea, but some participants had concerns for how it was implemented. It needed to be ensured that the collected information would only be accessed by an occupational health service provider and not by the employer. It was seen as potentially harmful to the person's work situation if their employer could track their health. Overall, participants had no concerns for how the manufacturer of their device is using their information. They are willing to have their information used for improving products and services.

For some individuals health information is the most private and sensitive information about them, and for others it's their financial situation. Participants had reasons to be worried about the disclosure of their health or financial information and how it could harm them. Release of health information was per-

ceived to potentially impact work situation and for example loans from the banks or insurance rates. On the other hand release of financial information was perceived as impacting personal relationships and also could more easily be misused. Participants saw that financial information could be used to steal money from them, but health information couldn't be used to harm them. All expect one individual perceived that if they would have long-term illness then they would evaluate this information differently and that health information would become more private and sensitive compared to financial information.

There are number of potential risks and privacy concerns that the participants had during these interviews. For many, they are able to recognize how their information might be misused or accessed by another party, but this small risk doesn't concern them much. Overall there were not many perceived risks specifically to the use of a wearable device, but the focus was electronic health records or other personal information that is given during registration to different services. Participants wished for transparency on how their information is stored, used, and shared, providing them some control.

The consensus among the participants was that there are more benefits than risks with the use of wearable devices and digitalization of health data. Many said that information collected by different parties for their own use is something that is part of our modern world. One participant said that if information is being misused or stolen somewhere they expect that it impacts many people and not just them and because of this they are not concerned. One participant stated that better access to their health data can improve diagnosis and because of these benefits, any risks that come with it are worth it.

6 DISCUSSION

This chapter discusses how the results presented in the previous chapter answer the research questions. It provides a summary of the main findings and compares them to the prior research. The use of privacy calculus theory is discussed and the implications of the findings to the theory. This is followed by the implications for practice that the findings of this study provide.

6.1 Research questions and main findings

The study had two main research questions to answer:

1. What are the user perceptions on the privacy and sensitivity of the health information collected with wearable devices?

2. When and why are users (not) willing to share this health information in exchange for services?

The following sub-sections highlight the findings to the research questions and discuss how they compare to the findings found in other studies.

6.1.1 Perceptions on information sensitivity

As discussed in the results chapter, the participants in the study viewed the information collected by their activity trackers as general. The information was not considered as sensitive or very private and the disclosure of the information was not seen to cause them much harm. Other research has found that individual's who have high privacy concerns towards the collection of their health information are less likely to adopt wearable devices (Li et al., 2016). This needs to be considered also in the context of this study as the evaluations of information sensitivity are from the perspective of users of activity trackers.

GPS information was the only type of information that was an exception as it was considered somewhat private and sensitive. Many other studies have found that it's the GPS information collected by wearable devices that causes users the most concern and is considered sensitive (Klasnja et al., 2009). Physical location data was seen as something that could potentially be misused and cause harm for the user, but the risk of this happening was considered to be very low. Participants raised concerns over being tracked or followed, and these same concerns have been found in other studies (Raij et al., 2011).

A previous study found that only athletes value GPS functionality on wearable devices and regular users prefer that their device would not have GPS (Motti & Caine, 2015). This finding differs from the present study, since even those participants that had privacy concerns about GPS information did value the speed and distance information that was provided by the GPS. In the previous research the participants were concerned specifically with location data that is being collected outside of their exercise periods (Motti & Caine, 2015). This finding is similar to the present study as the benefits of GPS were during the exercises, and the privacy concerns were concerning the normal daily movements and activities.

Participants in the present study were asked to compare the information collected by their wearable devices to the information stored in their medical records. In comparison medical records were seen as very private and that the information stored is more sensitive and specific about the individual. Participants did not have anything to hide in their medical records as they considered themselves to have good basic health, but they had concerns how the information could be used to identify them. Prior research has found that individuals have more privacy concerns over their health information than other personal information such as age, gender, and ethnicity (Lee & Kwon, 2015).

Medical records were seen different because they store more specific information about a person's health, and details about private conversations with the doctor that is written down. Other studies have confirmed that health information causes high privacy concerns and that individuals are hesitant to disclose it (Andrade et al., 2002).

Earlier research has found that individuals consider all types of health information sensitive and they don't differentiate between them (Anderson & Agarwal, 2011). This present study found that health information such as heart rate collected by wearable devices is not considered sensitive, but laboratory results and details about medical procedures is considered highly sensitive. Also the participants in the present study evaluated health information written by the doctor to be more sensitive and private compared to just numerical values.

To gain more understanding of the user perceptions of information privacy and sensitivity the participants were asked to compare medical records to financial information such as salary, taxes, and loans. Prior studies have found that financial and health information are the most sensitive information types (Andrade et al., 2002; Lwin et al., 2007; Malhotra et al., 2004; Phelps et al., 2000). In these studies both of the information types were found to be the most sensitive, but the participants were not asked to compare the two categories between

each other. Comparison in the present study produced mixed results since the opinions of the participants were divided in half.

For those that considered financial information to be more sensitive they explained, for example, that their spending habits are very personal and that there would be more harm for them if people would know about their finances than their health. On the other hand, the individuals that considered health information to be more sensitive explained this by saying that health information tells more about them and there is potential that confidential information would be stored in them.

Clearly these two information categories are the most sensitive and cause individuals the most privacy concerns, but the findings from this study as well as others have some differences. Few studies have conducted a comparison between these two information categories and have found that health information is more sensitive than financial or other personal information (Lee & Kwon, 2015). Another study also confirmed that health and medical information are the most sensitive information types compared to other personal information (Li et al., 2011).

Participants in the present study were asked to consider if a long-term illness would affect their evaluation between these two categories of information. All participants except one would consider health information to be more sensitive than financial information in the given circumstance. Based on the present study it would seem that health conditions such as illness would affect the evaluation of health information sensitivity compared to financial information. This finding aligns with that of Bansal et al. (2010), which discovered that poor health status did have significant impact on evaluation of health information sensitivity and the privacy concerns associated with it.

A study conducted by Laric et al. (2009) found that health information privacy concerns increase with age, and this was explained by older individuals having more health problems, which are then recorded in their health records. Similar findings have been in other studies as well that have highlighted the impact of age to decreased information disclosure (Malhotra et al., 2004). The present study found no difference between the different ages, but this could be because the oldest individual in the study was only 50 years old.

In the study by Bansal et al. (2010) it was found that healthy individuals have lower privacy concerns, which in turn increases their willingness to disclose their health information. In a study by Anderson and Agarwal (2011) it was found that individuals with poorer health were more willing to share their health information online, which was explained by these individuals needing the health services that require disclosure. A study by Gao et al. (2015) found that individuals with health problems were less concerned about their privacy when they were adopting new technologies. The present study is unable to fully answer how health status impacts privacy concerns and evaluation of information sensitivity. Based on the present study, poorer health status would seem to increase privacy concerns, but this is based on an individual's perceptions and not on actual experiences.

6.1.2 Willingness to share health information

The second research question was made of two parts. The first part dealt with when or to whom the individuals would be willing to share their health information. The second part explores why individuals are willing to share their information in some situations, but choose to withhold information in another. The subsequent section will discuss the concerns that keep individuals from sharing their health information. In the present study, the participants were asked to consider sharing their health information on social media, for the use of a doctor, for medical research, for the use improving products and services, and for the use of an occupational health provider.

Sharing exercises and related information on social media was something that only one participant did. The other participants didn't see any benefits for sharing the information to other people. Even though the information itself wasn't seen as sensitive, the exercise habits were considered a private matter. A study conducted by Patterson (2013) found that individual's don't share health information on social media because it's considered to be outside of the social norms, which aligns with the findings of this study. Many of the participants explained that they were exercising for themselves and didn't require outside motivation or validation, so for this reason they had chosen not to connect their wearable devices to social media.

When asked, all of the participants in the study were willing to share the information collected by their activity tracker for doctors to use. Most of the participants had an interest and a willingness to collect even additional information about their health with wearable devices or other medical devices and then provide this information to their doctor. This interest became even stronger if the participants would have some type of medical condition that would benefit from frequent measurements. This finding aligns with other studies that have found that the willingness to disclose will increase with poor health as more benefits are seen from disclosure (Anderson & Agarwal 2011; Gao et al., 2015). Based on present and prior research poor health seems to increase privacy concerns and the willingness to disclose health information, but only for relevant purposes (Bansal et al., 2010).

The participants in the present study considered that wearable devices cannot replace a doctor, but could potentially decrease the amount of visits. They had some concerns about their privacy and the misuse of their health information. The main worries were about the accuracy of the measurements and the problems that the elderly would have with using these technologies. Their concerns were focused around the usability of technologies and services, and not privacy or information sensitivity.

Prior studies have found that individuals are willing to provide their information for patient care and have low levels of concerns associated with it (Anderson & Agarwal, 2011). Individuals are also willing to provide their health information for organizations that are part of the health care value chain as these are seen as relevant and beneficial to their health care (Anderson & Agarwal, 2011). The findings of the present study support these earlier studies. In another prior study it was found that individuals are willing to provide their

information for health care and tracking of diseases (Willison et al., 2007). It was confirmed in the present study that all the participants were willing to give their information from their wearable devices to the research of cardiovascular health. Other studies have found that individuals have high privacy concerns when asked to provide health information to research or marketing (Anderson & Agarwal, 2011). This prior study looked at research in general, which can cause high privacy concerns, but the present study looked at only medical research that is relevant to the context.

Most of the participants in the study were willing to provide the information they have collected with their wearable devices to the device manufacturer for the improving of services and products. Participants assumed that this information collection and use was already happening. Patterson (2013) found that individuals are inclined to trust companies that promote health, which is a possible reason for why the participants in this present study were willing to share their information with the device manufacturer.

Overall, participants didn't have concerns about having their information used in this way as they considered the information to be of low value and not that sensitive. They valued that they would be given a choice of how their information is being used. Transparency of a company's information practices and giving individuals control over their information increases trust as well as disclosure as found in other studies (Sheehan & Hoy, 2000; Stone 1983).

A finding by Anderson and Agarwal (2011) was that individuals wouldn't be as willing to provide their information for marketing because they find it not relevant. The reason that individuals in the present study would allow their information to be used in marketing and improving products and services could be because they were asked if the information could be used specifically by the company they had purchased their wearable device from. This connection to the company might make it that the individuals consider there to be some benefit to themselves or at least it would be relevant that they would be asked to give access to their information. Individuals might not be willing to provide their information to some other organization to improve their products and services, but this was outside the scope of the present study.

Participants in the present study were also asked if they would use a wearable device provided by their employer if the information would be shared with the occupational health service provider. Most participants were willing to do so and saw that there could be benefits in addition to the free device that they would receive. Many earlier studies have found that if the individuals are given control over their information, and in this example a choice to use the device, they are more likely to accept (Malhotra et al., 2004; Sheehan & Hoy 2000; Stone 1983). Individuals did have some concerns about how the information might be misused if the employer would get access to it, but this was seen as not likely. Overall, individuals had high levels of trust towards occupational health services the same way as they did towards doctors in general, and they considered the risk of misuse by the employer to be low. This aligns with previous studies that have found that individuals tend to trust health care providers (Patterson, 2013).

A study by Patterson (2013) found that individuals thought that there is more harm than good in providing their information to law enforcement, insurance companies, employers, commercial research, and advertising. Even though participants in the present study did raise some privacy concerns with providing their information overall, they figured that the benefits were higher than the risks. The difference could be that in the present study the participants information was given to the occupational health services, and not directly to the employer and the participants in the study trusted that the information wouldn't be shared with the employer.

A Study conducted by Rohm and Milne (2004) found that employers and insurance companies caused individuals the highest privacy concerns, but at the same time individuals also had the highest trust towards their employers. The present study confirms that both health care providers and employers are considered to be trustworthy, and even though the individuals can identify potential risks, they tend not to worry about them happening.

6.1.3 Concerns towards sharing health information

This section discusses the reasons behind why individuals are not always willing to share their health information. During the interviews the participants did express some privacy concerns and risks, especially with collection and unauthorized or misuse of their information. These concerns did not have a major impact on the use of different services or a willingness to disclose information, but understanding the user perceptions is valuable. Overall, the participants did not have high privacy concerns and did not see it very likely that their information would be misused in a way that would cause them harm. The use of wearable devices and collecting information with them was considered a low risk activity. As previously mentioned, prior research has found that only individuals that have reasonably low privacy concerns adopt wearable devices, so their evaluation might not represent the larger public (Lit et al., 2016).

Prior studies have found that it's the individuals privacy concerns that have the highest impact on the adoption of health care services (Li & Sarathy, 2007; Xu et al., 2011). This can be seen in the present study as well since individuals evaluate their willingness to share their health information based on the potential benefits and the lack of any major risks. For this reason it's important to understand what types of privacy concerns individuals have about the use of wearable devices and their health information.

Previous studies have found that privacy concerns associated with health information include things such as discrimination, unauthorized access, and abuse of information (Bansal et al., 2010; Hodge et al., 1999; Rindfleisch, 1997). These three privacy concerns were frequently mentioned with different organizations as will be discussed below. Participants in the present study mentioned that banks and insurance companies could misuse one's health information as these organizations could benefit financially from it. Individual's loan application could be declined or insurance policy costs rise if health information would be available to these organizations.

The participants expressed trust towards their employer as discussed earlier, but they identified some potential risks to their privacy if the employer would get access to their health information. Some of the individuals thought that it's possible for the employer to benefit from employee health information as this could be used when making decisions about promotions or layoffs. They saw that employers aren't likely to do this, but this kind of behavior would punish those that have illnesses. This finding also aligns with previous research that identifies an employer as a group that causes individuals highest privacy concerns, but at the same time they have the highest trust towards them (Rohm & Milne, 2004).

Participants in the present study discussed unauthorized access to their information if there would be a security breach. This was seen as possible and also as something that happens all the time to organizations, but even though they had identified this risk, it didn't concern them much. One of the reasons was that individuals couldn't see how a criminal could benefit from their health information in some way. Security breaches to services and companies were also considered as a risk, which is shared between everyone and its impact would be minor for an individual.

Participants in general were more concerned about outside parties accessing and misusing their information compared to the service providers. For example, individuals are not as worried about social media services or device manufacturers misusing their information, but that unauthorized parties would access the information in these services. There is a level of trust that the individuals have towards a service they have accepted to use, which is why their concerns are towards parties that they have not given permission to their information. This finding aligns with multiple other studies that have found that previous positive experiences with a company increase the trust they perceive towards the organization (Bansal et al., 2010; Sheehan & Hoy, 2000). It also aligns with studies that have shown that giving an individual control over how their information is being used lowers their privacy concerns (Malthotra et al., 2004; Sheehan & Hoy 2000; Stone, 1983). These findings also confirm that individual's perceive that there is a implicit social contract between them and the organization they interact with as found in prior studies (Milne & Gordon, 1993).

Multiple of the individuals explained how many services that are offered for free collect and use the user information, for example, for advertising. This behavior was not seen as harmful but reasonable, but some of the participants had a preference that their activities would not be followed. To balance this concern towards collection of information, individuals limited the amount of information they provided as a part of the registration process. They saw no benefit from giving more than the required information for the use of the service provider. Many prior studies have found that the reputation of the company impacts the way individuals interact with them and their willingness to disclose information (Kim et al., 2008; Li, 2014; Schoenbachler & Gordon, 2002). This was seen also in the present study as individuals limited the amount of information they provided or shared with services that they were new to, but shared more freely in services that they had used for a longer time.

Another aspect that causes individuals privacy concerns and anxiety is the dependency on digital services. Some are worried that they are required to accept the use of new services, since there is no alternatives anymore. Others are worried that their health information can be misused more easily as it's more accessible to others in digital format compared to the previous paper versions. One participant did see the benefit that unauthorized access to their health records should leave a digital fingerprint, which is an improvement compared to someone reading their paper records. Participants also expressed concerns that their health and financial information are only in digital format and some of the important information could be lost if big servers would break. This anxiety over privacy and disclosure of personal information has been found in other studies (Angst & Agarwal, 2009; Sutanto et al., 2013).

6.2 Implications for privacy calculus theory

The privacy calculus theory was used in designing the interview structures and themes used in this study. Privacy calculus was also used as a theoretical lens to analyze the answers from the research participants. This theory, which is explained in detail in an earlier chapter, is based on the idea that individuals consider the risks and benefits of disclosing personal information (Dinev & Hart, 2006). Information disclosure is often the requirement in order to interact with online services, or in the case of the present study with wearable devices and its manufacturer. Aspects of privacy concern, control, and risks were identified as central ideas of privacy calculus and used in the structure of the interview.

The privacy calculus theory was found to be fitting in the context of this study. As prior research in privacy calculus has found individuals don't necessarily go through a conscious decision making process in which they consider all the costs or risks of a new device or a service and compare them to the potential benefits (Berendt et al., 2005). This happens somewhat automatic at times, but the individuals can recognize the factors they have considered before purchasing a device or registering for a new service.

In the context of this study the participants had mostly focused on the benefits of a wearable device when they had considered purchasing one. They had considered the financial costs and how this would relate to their hoped benefits. They had also considered the reputation of the company and previous experiences when considering the risks that would be associated with the purchase of a wearable device. This aligns with many prior studies, which have found that company reputation and previous experiences impact the use of a service (Bansal et al., 2010; Kim et al., 2008; Li, 2014; Schoenbachler & Gordon, 2002; Sheehan & Hoy, 2000).

Participants perceived many times that they had control over the information they wish to disclose, which aligns with studies that have found that control can diminish privacy concerns (Dinev & Hart, 2003). Another study found that when individuals adopt a new wearable device they perform the privacy calculus process during which they consider the risks, health infor-

mation sensitivity, reputation of the company, and the benefits and usefulness of the device (Li et al., 2016). The present study aligns with these findings as these were the aspects that individuals considered before adopting the new devices or once they had started using one.

What the study found was that individuals did not perceive having any major risks or costs to their privacy by adopting a new wearable device and the associated service. The participants were able to describe different types of risks that come from sharing health information or someone misusing it, but nonetheless these risks seemed very low to them and not very likely to happen. Some of the potential risks or costs had surfaced after the wearable device was in use as the individuals became more aware of the potential. Even these newly identified risks were considered not likely to happen and the benefits of use were higher. Previous research has argued that individuals don't have high privacy concerns, as they are not able to think of the potential risks that come from making inferences from their data (Raij et al., 2011). Another study has found similarly, that individuals have low levels of concern because of the lack of awareness of the potential ways their information can be misused and inferences that can be made (Motti & Caine, 2015).

As the participants had not had any negative experiences from their use, all the risks and costs to their privacy they perceived were just possibilities. In general, participants had received the benefits they had perceived prior to adoption and also some additional ones. Any of their concerns had not actualized at this point in time, so individuals had not knowingly experienced any misuse of their information. It would require additional research to understand if negative experiences such as identity theft would affect the privacy calculus process that individuals go through. It could be expected that past experiences could affect future behavior as found in many studies (Bansal et al., 2010; Sheehan & Hoy, 2000).

6.3 Implications for practice

The findings of this thesis have many implications for practice that can be useful for different organizations. Health care providers and medical research can benefit from the huge amount of data individuals have collected with their wearable devices. When the use of the information is described clearly and transparently, individuals are willing to share their personal information for these purposes. Health care providers can serve individuals better as they are able to receive detailed and more frequent information about an individual's health. Participants in the study were willing to collect even additional information about their health if it could be found useful for their health care. In order to benefit from this data a system needs to be created that the individuals can use to transfers their data to the doctor.

Individuals with poor health seem to be more willing to collect and share information about their health. These individuals should be encouraged to use a device that collects information that would be relevant to their health care.

Findings also indicate that using activity trackers could motivate individuals to move more at least for a short period of time. The accuracy of the data collected by wearable devices also needs improvement so that individuals would trust them in their health care.

GPS information collected by wearable devices seems to cause some privacy concerns, which can impact the adoption and use of such devices. Device manufacturers should explore the possibility that GPS functionality is enabled only during exercises and off during other times. This could mitigate the concerns that individuals have about their locations being recorded outside of their exercise periods.

As companies continue to develop these wearable devices and increase their capabilities to better serve the individuals and health care industry, some things need to be considered. Based on the findings, privacy concerns could increase as the information collected by wearable devices resembles more the information stored in medical records. Companies need to consider the types of information that is useful and relevant to be collected. Based on the current study, written details by doctors cause the highest privacy concerns, so it could be better to avoid the wearable devices to have access to these notes.

It's important to note that based on the findings of this study, individuals assume that companies are collecting and using their personal information. Companies that are not doing this should clearly indicate it to users as this could benefit them by improving reputation and increasing customer trust. Users don't familiarize themselves with long terms and conditions, so companies that wish to build trust should be transparent about their practices and talk about their information practices openly.

7 CONCLUSIONS

This chapter summarized the goals of the study and it's findings. The summary is followed by the discussion of the limitations of the study. The last section provides areas for future research.

The growth of the wearable technology market is impacting how individuals collect and store their health information. Prior to these technologies, health information was stored in medical records accessible only by doctors that provide health care services. Now health information is being stored in a variety of places including wearable devices, smart phones, laptops, and cloud services offered by different organizations. As the health information services have become decentralized and individuals have easier access to their information this has brought some new privacy concerns and risks.

The goal for this study was to understand how users perceive health information sensitivity and privacy. Interviewing users of wearable devices and asking them to explain their perceptions and evaluations accomplished this objective. The other goal was to understand the willingness of users to share the information they have collected with their wearable devices. The objective for this was to understand what information users are willing to share and to whom. The study also explored why users are willing to share their information to some organizations, but not to others.

The study used a qualitative research method of themed interviews to understand the impact of these new technologies and health information sensitivity. Themed interviews follow themes identified by the researcher, but does not follow a strict question format. This approach enabled the collection of rich and detailed information of the participants' perceptions and experiences relating to the use of wearable devices and health information. This qualitative method and tools were found to be fitting for the type of study conducted. Ten individuals with differing backgrounds and experiences were interviewed for this study to provide an understanding on the topic. The goal of the study was not to provide results that are generalized to the public, but the results provide more understanding of the topic and foundation for future research.

The study found that information collected with wearable devices is not perceived as sensitive or private. However, health information stored in patient

medical records is considered to be very sensitive and private to the individuals. The important difference is that information collected with wearable devices is considered as general information about physical activities and it's only in numerical form. Health records in hospitals on the other hand contain detailed and very specific information about individuals that can be used to identify them. These records also contain text written by doctors about procedures and discussions that are considered to be the most sensitive type of information.

Both health and financial information are considered to be the most sensitive and private information, but individuals rate these differently. For some, information about their finances and spending habits is more private, and more risks are associated with this information being made public. For others, health and medical information is more private as for them it reveals more about a person and it's seen to be more harmful for them if disclosed. Interestingly when individuals consider having a long-term illness almost all would evaluate health information to be most sensitive and private and causing more harm if disclosed.

Most individuals don't share information collected with wearable devices about their exercises on social media. Users don't perceive any benefits from sharing this to others, and some consider their exercise habits to be private. On the contrary, users are willing to share the information they have collected to doctors if it can be used in their health care. Users question if the information collected currently would be useful for the doctor, but they show interest in collecting additional information about their health if it can be used to improve their health care. Wearable devices are not seen as a replacement for doctors, but as a way to supplement the current health care services. Transitioning to a more self-measurement health care model causes individuals some concerns over the accuracy of the data and how the information is being used for diagnosis. Users are also willing to give the information collected with their wearable devices to medical research, which could have a huge impact on research as the number of participants to studies could grow exponentially.

Most individuals would use a wearable device offered by their employer if the data collected would be transferred to an occupational health service provider. Many saw this as a great way to motivate some people to move more and make them healthier. An important factor for all was that their employer would not have access to the information as this was seen to cause a conflict of interest. Users had some concerns how an employer could misuse the health information, for example when choosing promotions or layoffs. Individuals did generally trust both employers and health care service providers and did not see misuse as a likely risk. Most of the users were also willing to give information collected by their wearable devices for the use of the device manufacturer for improving products and services. Many assumed that this collection was already happening and did not see any major concerns or risks with the company using their information for these purposes. Selling information for marketing or advertisers was not seen as risky, but causes some dissatisfaction on the part of the users.

Overall, individuals have privacy concerns over the disclosure of their information, especially concerning their health. They are able to identify potential

risks such as collection, misuse, and outside parties getting access to their information. Information collection and misuse are perceived as risks that are always present when interacting with online services. Nonetheless the likelihood that the risks or concerns are realized is considered to be very low. Since individuals don't perceive that the potential risks could cause them significant harm, these concerns are not impacting their use of products and services considerably. Individuals continue to use products and services that they find useful or receive benefit from, but they limit the amount of information they provide during registration and the use of the service. Increased awareness over one's exercises and the ability to increase the quality of training were the main benefits as well as the reasons for adopting wearable devices. These benefits were perceived to be greater than any of the potential risks or perceived privacy concerns that individuals had.

7.1 Limitations

The study had some limitations that are always expected in research. The study used a small group of participants, which limits the generalizability of the results. Many of the participants were also students, whom do not represent the demographics of the general public. The study was designed to learn more of the phenomenon by using a qualitative research method, which provides results that cannot be used to make statistical interpretations.

The study interviewed only individuals that had wearable devices so their evaluations of the sensitivity of health information can be different from those that do not use such a device. The researcher also lacks training in the medical field, which can impact the analysis of the results.

The quality of this research can be seen as its ability to answer the research questions and provide analysis on the collected data. Structured interviews were able to effectively provide the data that was needed to answer the research questions. There were differences in the subjective experiences of the participants, but the interview themes were able to capture the relevant information reliably. The quality and reliability of the research can be seen in the implementation of the study and the consistent results.

To maintain the quality and reliability of the study, the researcher maintained neutrality during the interviews and analysis. Participants were made to feel that there was no right or wrong answer and that they wouldn't be judged based on the things they shared. The researcher also maintained this objectivity during the analysis of the data so that the impact of personal bias would be minimal. The themes and guiding questions of this study could be used for further research to produce more information on the subject matter.

Individual interviews are not replicable as the interview method allows the interviews to be different based on the answers of the subjects. Also to maintain the reliability of the study the participants weren't primed to think about privacy in the beginning of the study so that their answers would not be seen through this lens. This allowed participants to bring up privacy concerns

themselves if they had some, and it was not until the latter part of the interview that participants were asked to specifically think about the privacy concerns and risks associated with services.

7.2 Future Research

To understand the aspects that impact the adoption of new wearable technologies and health technologies further research needs to be done. It's valuable to study further if privacy concerns impact the adoption of these technologies in order to find ways to mitigate those concerns. Understanding these aspects becomes crucial when wearable technologies become more common in providing health care services.

Further research needs to be done to better understand how GPS functionality and data impact privacy concerns. Many wearable devices offer this functionality, but the risks associated with it seem to cause concerns for individuals. It could be possible to design devices that turn off GPS when it's not needed in order to mitigate concerns.

The findings of this study show that there is a need to further investigate how individuals evaluate different types of health information. Future research could explore if evaluations of health information sensitivity is different between numerical values and information in written format. It would also be valuable to understand what type of health information is the most sensitive and what aspects impact the individual's evaluation. Further research could explore if the location where health information is stored impacts the privacy concerns that individuals have.

The present study found that individuals are willing to give information to medical research, but this needs to be investigated further. Future research could study what type of information individuals are willing to provide for research. There would be value to understanding the differences that might exist with different types of research such as medical and marketing research.

Further research needs be done in order to understand how older individuals evaluate health information sensitivity and the aspects they consider. It would be valuable to gain a better understanding on how health conditions impact the individual's willingness to share health information. Further research needs to be done in order to investigate if educating individuals about potential privacy risk would impact their risk perceptions and privacy concerns. It would be beneficial to understand if privacy concerns stem from lack of knowledge or if they stem from the awareness of potential threats.

REFERENCES

Ackerman, M. S., Cranor, L. F., & Reagle, J. (1999). Privacy in e-commerce: examining user scenarios and privacy preferences. In *Proceedings of the 1st ACM conference on Electronic commerce* (pp. 1-8). ACM.

Anderson, C. L., & Agarwal, R. (2011). The digitization of healthcare: boundary risks, emotion, and consumer willingness to disclose personal health information. *Information Systems Research*, *22*(3), 469-490.

Andrade, E. B., Kaltcheva, V., & Weitz, B. (2002). Self-disclosure on the web: the impact of privacy policy, reward, and company reputation. *NA-Advances in Consumer Research Volume 29*.

Angst, C. M., & Agarwal, R. (2009). Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. *MIS quarterly*, *33*(2), 339-370.

Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS quarterly*, 13-28.

Bansal, G., Zahedi, F., & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems*, *49*(2), 138-150.

Berendt, B., Günther, O., & Spiekermann, S. (2005). Privacy in e-commerce: stated preferences vs. actual behavior. *Communications of the ACM*, *48*(4), 101-106.

Chellappa, R. K., & Sin, R. G. (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information Technology and Management*, *6*(2-3), 181-202.

Culnan, M. J. (1993). " How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use. *MIS quarterly*, 341-363.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization science*, *10*(1), 104-115.

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., & Colautti, C. (2006). Privacy calculus model in e-commerce–a study of Italy and the United States. *European Journal of Information Systems*, *15*(4), 389-402.

Dinev, T., & Hart, P. (2003). Privacy Concerns And Internet Use - A Model Of Trade-Off Factors. In *Academy of Management Proceedings* (Vol. 2003, No. 1, pp. D1-D6). Academy of Management.

Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents-measurement validity and a regression model. *Behaviour & Information Technology*, *23*(6), 413-422.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, *17*(1), 61-80.

Gao, Y., Li, H., & Luo, Y. (2015). An empirical study of wearable technology

acceptance in healthcare. *Industrial Management & Data Systems*, *115*(9), 1704-1723.

Hirsjärvi, S., & Hurme, H. (2011). *Tutkimushaastattelu: teemahaastattelun teoria ja käytäntö*. Gaudeamus Helsinki University Press.

Hodge Jr, J. G., Gostin, L. O., & Jacobson, P. D. (1999). Legal issues concerning electronic health information: privacy, quality, and liability. *Jama*, *282*(15), 1466-1471.

John, L. K., Acquisti, A., & Loewenstein, G. (2011). Strangers on a plane: Context-dependent willingness to divulge sensitive information. *Journal of consumer research*, *37*(5), 858-873.

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision support systems*, *44*(2), 544-564.

Klasnja, P., Consolvo, S., Choudhury, T., Beckwith, R., & Hightower, J. (2009, May). Exploring privacy concerns about personal sensing. In *International Conference on Pervasive Computing* (pp. 176-183). Springer Berlin Heidelberg.

Laric, M. V., Pitta, D. A., & Katsanis, L. P. (2009). Healthcare Information Privacy: A comparison of US and Canadian perspectives. *Research in healthcare financial management, 12(1),* 93-111.

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of social Issues*, *33*(3), 22-42.

Lee, N., & Kwon, O. (2015). A privacy-aware feature selection method for solving the personalization–privacy paradox in mobile wellness healthcare services. *Expert Systems with Applications*, *42*(5), 2764-2771.

Li, Y. (2014). The impact of disposition to privacy, website reputation and website familiarity on information privacy concerns. *Decision Support Systems*, *57*, 343-354.

Li, H., Sarathy, R., & Xu, H. (2011). The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. *Decision Support Systems*, *51*(3), 434-445.

Li, H., Wu, J., Gao, Y., & Shi, Y. (2016). Examining individuals' adoption of healthcare wearable devices: An empirical study from privacy calculus perspective. *International journal of medical informatics*, *88*, 8-17.

Lwin, M., Wirtz, J., & Williams, J. D. (2007). Consumer online privacy concerns and responses: a power–responsibility equilibrium perspective. *Journal of the Academy of Marketing Science*, *35*(4), 572-585.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information systems research*, *15*(4), 336-355.

Milne, G. R., & Gordon, M. E. (1993). Direct mail privacy-efficiency trade-offs within an implied social contract framework. *Journal of Public Policy & Marketing*, 206-215.

Motti, V. G., & Caine, K. (2015). Users' Privacy Concerns About Wearables: impact of form factor, sensors and type of data collected. In *Financial Cryptography and Data Security Conference*.

Patterson, H. (2013). Contextual expectations of privacy in self-generated health information flows. In *TPRC*, 2013.

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing*, *19*(1), 27-41.

Raij, A., Ghosh, A., Kumar, S., & Srivastava, M. (2011). Privacy risks emerging from the adoption of innocuous wearable sensors in the mobile environment. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 11-20). ACM.

Rindfleisch, T. C. (1997). Privacy, information technology, and health care. *Communications of the ACM*, *40*(8), 92-100.

Rohm, A. J., & Milne, G. R. (2004). Just what the doctor ordered: the role of information sensitivity and trust in reducing medical information privacy concern. *Journal of Business Research*, *57*(9), 1000-1011.

Saaranen-Kauppinen, A., & Puusniekka, A. (2006). KvaliMOTV - Menetelmäopetuksen tietovaranto. Tampere: Yhteiskuntatieteellinen tietoarkisto. Accessed 5.8.2016 http://www.fsd.uta.fi/menetelmaopetus/

Sarathy, R., & Li, H. (2007). Understanding Online Information Disclosure As a Privacy Calculus Adjusted by Exchange Fairness. *ICIS 2007 Proceedings*, 21.

Schoenbachler, D. D., & Gordon, G. L. (2002). Trust and customer willingness to provide information in database-driven relationship marketing. *Journal of interactive marketing*, *16*(3), 2-16.

Sheehan, K. B., & Hoy, M. G. (2000). Dimensions of privacy concern among online consumers. *Journal of public policy & marketing*, *19*(1), 62-73.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS quarterly*, *35*(4), 989-1016.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: measuring individuals' concerns about organizational practices. *MIS quarterly*, 167-196.

Stewart, K. A., & Segars, A. H. (2002). An empirical examination of the concern for information privacy instrument. *Information Systems Research*, *13*(1), 36-49.

Stone, E. F., Gueutal, H. G., Gardner, D. G., & McClure, S. (1983). A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. *Journal of applied psychology*, *68*(3), 459.

Stone, E. F., & Stone, D. L. (1990). Privacy in organizations: Theoretical issues, research findings, and protection mechanisms. *Research in personnel and human resources management*, *8*(3), 349-411.

Sutanto, J., Palme, E., Tan, C. H., & Phang, C. W. (2013). Addressing the Personalization-Privacy Paradox: An Empirical Assessment from a Field Experiment on Smartphone Users. *Mis Quarterly*, *37*(4), 1141-1164.

Wang, T., Duong, T. D., & Chen, C. C. (2016). Intention to disclose personal information via mobile applications: A privacy calculus perspective. *International Journal of Information Management*, *36*(4), 531-542.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard law review*, 193-220.

Westin, A. (1970). Privacy and freedom. 1967. *Atheneum, New York*.

Willison, D. J., Schwartz, L., Abelson, J., Charles, C., Swinton, M., Northrup, D., & Thabane, L. (2007). Alternatives to project-specific consent for access to personal information for health research: what is the opinion of the Canadian public?. *Journal of the American Medical Informatics Association*, *14*(6), 706-712.

Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2008). Examining the formation of individual's privacy concerns: Toward an integrative view. *ICIS 2008 proceedings*, 6.

Xu, H., Luo, X. R., Carroll, J. M., & Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems*, *51*(1), 42-52.

Xu, H., Teo, H. H., Tan, B. C., & Agarwal, R. (2009). The role of push-pull technology in privacy calculus: the case of location-based services. *Journal of Management Information Systems*, *26*(3), 135-174.

APPENDIX 1 STRUCTURE OF THE INTERVIEWS

Background information:

- Age
- Gender
- Student or Employed
- Make and model of activity tracker
- Length of use
- Activity level

Theme 1: Usefulness and benefits (Risks)

- Types of information wearable devices collects
- How and when is information used
- Types of physical activities
- Motivational tool
- Benefits to health or exercise
- Frequency of doctor visits

Theme 2: Sharing of information (Control)

- Sharing on social media
- Sharing with doctor
- Sharing for medical research
- Sharing with occupational health
- Sharing with device manufacturer

Theme 3: Information sensitivity (Privacy concerns)

- Activity tracker information sensitivity
- Activity tracker information compared to medical records
- Medical records compared to financial information
- Impact of health status
- Concerns of digitalized health records
- Privacy concerns