Personal Consumer Environment

The consumer in control of his digital footprints.

Master Thesis

UNIVERSITY OF TWENTE.

adwise
YOUR DIGITAL BRAIN

University of Twente

Supervisors:
Dr. J. Karreman
Dr. I. van Ooijen
Drs. M. H. Tempelman

Adwise

Supervisor:
W. Nieuwerth

February 2020

Loraine Seliger

Personal Consumer Environment

The consumer in control of his digital footprints

University of Twente
Faculty of Behavioural, Management and Social Sciences
Communication Studies - Digital Marketing

Master Thesis

Name: Loraine Seliger
Student number: S2201534
E-mail: l.seliger@student.utwente.nl

Master: Communication Studies
Specialization: Digital Marketing
Faculty: Behavioral Management and Social Sciences

Date: 28/02/2020

Supervisor: Dr. J. Karreman
Second supervisors: Dr. I. van Ooijen & Drs. M. H. Tempelman

Abstract

Aim. An environment in which consumers have full control over their own information under their own circumstances can be a unique turning point in the marketing world. Although the GDPR has taken a step to give consumers control over their digital footprint, consumers still feel that they have no control over their retail data. Therefore, this study addresses the lack of control over retail data by exploring the principles and requirements of an, as yet unknown, Personal Consumer Environment (PCE). In this study, consumers will have control over their retail data from retailers with an online presence by means of a digital environment.

Method. A qualitative exploratory study was set up using focus groups among participants who differ in age, gender and level of education. A total of 30 participants, divided over 6 groups, participated in the sessions. Each group contained 5 participants in which three topics were discussed: knowledge about retail data, the need for control and finally the principles and requirements of a PCE. To provide direction to the research and the participants, a similar digital environment, Personal Health Record (PHR), was used as an example.

Results. As a result of this research, many participants have no knowledge of the collection of retail data from retailers with an online presence. Because many participants, with the exception of a few, do not know how to gain control over this collected data. Secondly, this study has shown that a large proportion of participants do need to have more control over their retail data. Awareness plays an important role in fulfilling this need. Thirdly, all factors of UTAUT2, with the exception of Habit and Hedonic Motivation, can influence the acceptance of a PCE. Furthermore, factors such as privacy and trust are unmistakable for the principles and requirements for this digital environment. Finally, in addition to these principles and requirements, consumers particularly identify risks in the leakage and abuse of retail data.

Conclusion. Based on this research, it can be concluded that thirteen principles and requirements have been discussed that provide insight into the acceptance of PCE. These thirteen principles and requirements contribute to increasing the consumer's control over their retail data originating from retail companies with an online presence.

Keywords: Digital environment, UTAUT2, retail data, principles, requirements, control

Preface

This thesis was written to complete the master Communication Science, with a specialization in Digital Marketing, at the University of Twente. During this period of research I had the opportunity to develop myself in the field of digital and data-driven marketing.

First of all, I would like to thank all the participants in this research. It was a huge challenge to plan moments in which multiple participants were available. I am very grateful to all participants for their flexibility and especially for their enthusiastic contributions to this research. Because of the amount of relevant input and positive energy I have experienced focus group sessions as pleasure and success.

Secondly, I would like to thank my supervisors from the University of Twente. I have felt very comfortable with you supervising me. Because of your knowledge and advice, this has helped me to work on this exploratory research.

I also want to thank Wouter Nieuwerth, my supervisor from Adwise, for supervising this research. You gave me the confidence and support I needed during my study. Your critical view of my work and your patience during this period helped me to deliver this achievement.

Finally, I would like to thank my family and friends for listening during this period. The amount of trust and pride you radiate in my work has ensured that I have invested maximum time and energy in this research.

Enschede, February 28, 2020

Loraine Seliger

Table of content

1 Introduction

With the rise of the European General Data Protection Regulation (GDPR), which was implemented in the Netherlands on 25th May 2018, consumers have gained more control over the personal data that organisations store and process. After the first six months, almost 10,000 people in the Netherlands have filed a privacy complaint with the Authority for Personal Data (AP), which shows that people actively and consciously stand up for their privacy rights and no longer allow the unwanted disclosure of data to third parties (NOS, 2018).

However, consumers have not necessarily gained more control over their data since the introduction of the GDPR. Recent research shows a strong influence of standard options or a limited understandability of data collection (van Ooijen & Vrabec, 2018). This is due to an possible information overload. Furthermore, other research has been carried out that address this need for consumers to gain more control over their digital footprint (Kamleitner & Mitchell, 2018; Shore & Steinman, 2015). In the health sector, this problem has been addressed by introducing a digital environment, the Personal Health Record (PHR). In this digital environment, individuals have access to their health information, which they can manage and share (Tang, Ash, Bates, Overhage & Sands, 2006). However, this problem has not been addressed in the retail sector which results in the lack of trust into the retail companies and concerns regarding their privacy (European Commission, 2015).

In this research, we address the lack of control over retail data by exploring the principles and requirements that contribute to consumer acceptance of a digital environment. We define this digital environment as the Personal Consumer Environment (PCE). The purpose of this PCE is to allow consumers to manage their retail, collected by the retail chain. This retail data includes information related to the interaction and communication with retail companies with an online presence. The interaction and communication can lead to aware or unaware data collection (Morey, Forbath, & Schoop, 2015).

We build upon the existing body of knowledge to determine which factors can influence the acceptance of a PCE. From a scientific point of view, this research is relevant as it attempts to explain whether the principles and requirements of a PCE differ from factors in an existing acceptance model, known as Unified Theory of Acceptance and Use of Technology 2 (UTAUT2) (Venkatesh, Thong & Xu, 2012). If we introduce a PCE, it could be used to regain consumer trust and commitment and gain insight into potential risks. With this research, this can be a contribution for different organizations. Furthermore, these principles and requirements can be used as heuristics in the development of a PCE.

From this objective, the following central research question has been investigated:

Central research question: *What are the principles and requirements of a Personal Consumer Environment (PCE) in retail that are expected to contribute to consumer acceptance?*

In order to answer this central research question, a qualitative study was carried out using focus groups. An exploratory study was applied to gain insight into the principles and requirements for a PCE.

Following the introduction, the theoretical framework has been set up in chapter 2. This introduces the key concepts and discusses the UTAUT2 model. In chapter 3, the method is explained. This chapter explains the approach to the central research question of this study by answering sub-questions. Furthermore, the method explains how the data has been collected and analysed. Chapter 4 describes the results of the analysis of the codebook and discusses the principles and requirements. Finally, chapter 5 verifies and discusses the results of this study. An answer is given to the central research question and a conclusion is formulated.

2 Theoretical framework

In this theoretical framework, the first step will be taken to gain insight in the characteristics of a Personal Consumer Environment (PCE). Next, the effects of providing control will be identified by comparing the PCE with a similar digital environment, the Public Health Record (PHR). Subsequently, an in-depth analysis will be made regarding the characteristics of retail data by defining the different types of data. Furthermore, acceptance models will be discussed in order to gain insight into the most important factors for the acceptance of a technology. Finally, information is collected on the factors of trust and privacy related to the acceptance and use of a PCE.

2.1 Personal Consumer Environment

A Personal Consumer Environment (PCE) is a digital environment in which consumers have control over their retail data. This digital environment can be part of an application or a tool for a website aimed at enabling consumer control. A PCE focuses on retail data originating from retail companies with an online presence. Many organisations, especially retailers, explode in the availability and collection of data (Shankar, 2019). Kamleitner and Mitchell (2018) propose this initiative of control by enabling consumers to manage their collected data. In the marketing world, this can be seen as a turnaround where the consumer decides for himself what information can be collected and used and under what conditions (Groot, 2014). A digital environment in which the control of an individual's data is already the focus is the Personal Health Record (PHR). In a PHR, individuals have access to their health information, which they can manage and share (Tang, Ash, Bates, Overhage & Sands, 2006). The study by Caligtan and Dykes (2011) defines a PHR as: “An electronic, universally available, lifelong source of health information held by individuals”. Senor, Aleman and Toval (2012) assumes that these individuals must have their data available at any time. In a similar digital environment such as a PHR, this gives additional insight into the characteristics of a PCE.

2.2 Effect of control

A digital environment such as the PHR can contribute to understanding the importance of having control over your data. Particularly, the research of Yao, Chu, and Li (2010) shows that based on the PHR, the relationship between the patient and care provider has become very important. As a result, more trust and openness has been created with regard to the data collected (Vance, Tomblin, Studney, & Coustasse, 2015). According to Warburg (2016), providing control of data to an individual, such as a patient or consumer, also affects the reliability of a system. With a decentralized system, such as a PHR or a PCE, these digital environments become more secure and less susceptible to fraud. As a result, information can be exchanged more quickly. With this change of control, better empowerment can be created for an individual (Labrecque, vor dem Esche, Mathwick, Novak, & Hofacker, 2013). However, leaving the decision making to an individual can also have consequences for the interpretation of the collected data (Cattaneo &

Chapman, 2010). But, in the case of the PHR, it can also pose a threat to some providers who want to retain control, autonomy and authority themselves (Logue & Effken, 2012; Tang et al., 2006).

2.3 Difference in sector

European Commission research (2015) shows that 74% of respondents trust health and medical institutions to protect their personal information. In contrast to the retail sector, a majority of respondents to this research (56%) do not trust online en offline retail companies to protect their personal information. This shows that individuals' trust in managing personal data differs in the medical and retail sectors. Recent research (Morey, Forbath, & Schoop, 2015) also confirms that the trust of individuals in sectors differs. From the perspective of retail companies, it acknowledges that making the exchange of data transparent will become increasingly important for building trust. This is where a PHR in the medical sector already makes its contribution. Finally, from the perspective of the medical sector, it is suggested the introduction of the PHR also introduced risks. A possible explanation is that individuals may feel that a system is skewed. Because users with less technical and health literacy do not understand how to use such a system (Showell, 2017).

Based on the insights from a PHR, it is important to find out how these aspects contribute to the need for control by individuals, in the context of retail data. Therefore, research will be done into the next sub-question:

Sub-question 1: *To what extent do consumers experience a feeling of control over their retail data?*

2.4 Retail data

When developing a PCE, one of the goals is to give consumers more control over their retail data. If we refer to retail data, we mean online or a combination of online and offline data derived and collected from retail companies. As an example, this could be a physical supermarket that offers its products offline as well as online and tries to combine the behaviour of the consumer at both channels (Gallino & Moreno, 2014). To define the characteristics of retail data, in relation to a PCE, we use the 3 key types of retail data identified by Morey et al. (2015). These 3 types can be defined as: 1) self-reported data, 2) digital exhaust and 3) profiling data. Self-reported data is information that individuals voluntarily provide about themselves, such as an email address or age. Moreover, digital exhaust is created by the use of mobile devices, web services or other technologies. It can be used to share location data or browsing history. Finally, profiling data is used to make predictions about an individual's interests and behaviours. This data is derived using a mix of self-reported data, profiling data and additional data that can be collected both online and offline. In line with profiling data, the study by King and Forder (2016) shows that consumers attach the greatest value to this type of data. This is because individuals have the least control over the use of this data, which gives rise to major privacy concerns. Moreover,

these profiling data may result from the combination of seemingly unrelated datasets that are not obvious to consumers (Jain, Gyanchandani & Khare, 2016).

2.4.1 (Un) awareness of data collection

With the collection of retail data, consumers of a PCE might experience awareness of data collection. This difference in awareness is also reflected in the research by Girardin, Calabrese, Dal Fiore, Ratti, and Blat (2008) in which a distinction is made between passive and active digital footprints. In the case of an active digital footprint, the consumer deliberately releases data via a website or social media, such as self-reported data. Information is deliberately and consciously left behind by the consumer. A passive digital footprint collects information that the user is unaware of. For example, this could be information about the location where the user has been online, such as digital exhaust. Depending on the amount of information, it is easy and fast for retailers with an online presence to collect and predict large amounts of information about the consumer (Matz & Netzer, 2017).

2.4.2 Sensitivity of data

In addition to providing insight into retail data at three different levels, there is also a difference in the type of sensitivity of the data (Schermer, Hagenauw & Falot, 2018). In the case of a PCE, retail data also includes personal data. Personal data is sensitive information about an identified or identifiable natural person. Think of; name, location or an online identifier. Information such as a name or a location can often be a starting point to supplement consumer information from different levels or types (Matz & Netzer, 2017). In contrast, there are also special categories of personal data. Compared to a PCE, this type of data relates more to medical data in a PHR. As stated in a recent study (Authority for Personal Data, 2018), data relating to a person's health belongs mainly to the special personal data. Other examples of sensitive data are race or religion.

Based on the insights of the characteristics of data, it is important to identify the extent to which consumers experience these differences. To gain insight in these characteristics, research should be conducted into the knowledge of consumers in the field of data collection. Therefore, research will be conducted into the next sub-question:

Sub-question 2: *What do consumers currently know about data collection in the context of retail companies with an online presence?*

2.5 Technology Acceptance Models

To get a better understanding which key factors influence the acceptance of a PCE, the research model TAM and UTAUT(2) can be used as a framework. Using technology acceptance models, it is possible to investigate the individual acceptance of different new and innovative technologies. When using a PCE, technology and the internet are needed as a source to manage retail data.

One of the first core technology acceptance models and associated factors is described in the Technology Acceptance Model (TAM). The TAM is specifically aimed at explaining how users accept and use a technology (Davis, 1989). In this model, *Perceived Ease of Use* and *Perceived Usefulness* are two primary factors that influence an individual's intention to use new technology (Heerink, Kröse, Evers, & Wielinga, 2010). *Perceived ease of use* is described as the degree to which a person believes that the technology is easy to use (Davis, 1989). According to this model, this factor has an influence on the *Perceived Usefulness* and also directly on the attitude of users. *Perceived usefulness* refers to the extent to which an individual believes that the use of a particular system would improve his or her professional performance (Davis, 1989). This second factor has, according to this model, an influence on the attitude and also directly on the intention to accept a technology. Using these factors, this model can be used to investigate a user's intention to use (Turner, Kitchenham, Brereton, Charters & Budgen, 2010). Although the core principles of TAM can be used to gain insight into the intention to use a PCE, the model has been further developed over the years.

Unified Theory of Acceptance and Use of Technology 2

In order to gain insight into possible factors that contribute to principles and requirements of a PCE, the Unified Theory of Acceptance and Use of Technology 2 (UTAUT2) model can offer additional support in this regard (Figure 1). UTAUT2 is an extension of the existing UTAUT model (Venkatesh, Morris, Davis and Davis, 2003) and is derived from eight previously developed models and theories, including TAM. Additionally, the approach of the UTAUT (organizational perspective) has been adapted to the perspective of the consumer (Venkatesh, Thong & Xu, 2012). The perspective of UTAUT2 is in line with the approach of this research into the introduction of a PCE. The consumer will be the end user of a PCE. UTAUT2 has been expanded with three additional predictors as compared to the UTAUT model. Therefore, this model identifies new determinants and relationships between factors. As a result, the UTAUT2 model has seven predictors and three mediating factors. In addition, the intention to implement certain behaviour still seems to be an accurate predictor of behaviour (Ajzen & Fishbein, 1977).

Because the perspective of UTAUT2 is similar to a PCE, we introduce the UTAUT2 factors in detail to understand if they can contribute to the principles and requirements of a PCE.

One of the seven predictors is *Performance Expectancy*. This concerns the extent to which technology has a positive impact on the completion of certain activities (Venkatesh et al., 2012). The technology used in a PCE should add something to the daily life of the consumer. Secondly, there is *Effort Expectancy*, which is described as the extent to which technology is easy to use by consumers. As a result of the use of a PCE, it is important that the PCE offers the consumer more control and does not cost too much energy. Thirdly, *Social Influence* is about the extent to which someone is influenced by his or her personal environment. An individual could change his or her mind due to the influence of another individual or a group (Venkatesh et al., 2003). Therefore, it is important that consumers are positive about the use of a PCE to motivate the intention to use.

The fourth influencer is *Facilitating Conditions*. This refers to the extent to which an individual thinks he or she has sufficient information and knowledge applicable to the possession of the product. As a result of sufficient knowledge and information that must be available about a PCE, this can directly affect the actual use. According to Venkatesh et al. (2012), these first four influencers are considered to be the important ones to investigate whether consumers have the intention to use a PCE. In addition to UTAUT2, *Hedonic Motivation* has been added as the fifth influencer. *Hedonic Motivation* can be defined as the fun or pleasure derived from using a certain technology. However, this factor is not important because pleasure and pain receptors have no influence on achieving a goal (Higgins, 2006). Sixthly, *Price Value* relates to the cost-benefit analysis that individuals make for the use of a product (Vroom, 1964). Research should reveal whether costs for the intention to use a PCE are a determining factor for consumers. The *Habit* factor will probably not influence the intention to use because a PCE does not yet exist. However, there is a possibility that consumers already regularly take the necessary actions to protect their data or actively use a PHR.

Finally, in addition to the UTAUT2 factors that influence behavioural intention, there are three mediated factors: *Age*, *Gender* and *Experience* (Figure 1). These factors increase the power of the model to better understand consumer acceptance. However, *Experience* with a related consumer technology is difficult to identify because the application and technology does not yet exist related to a PCE.

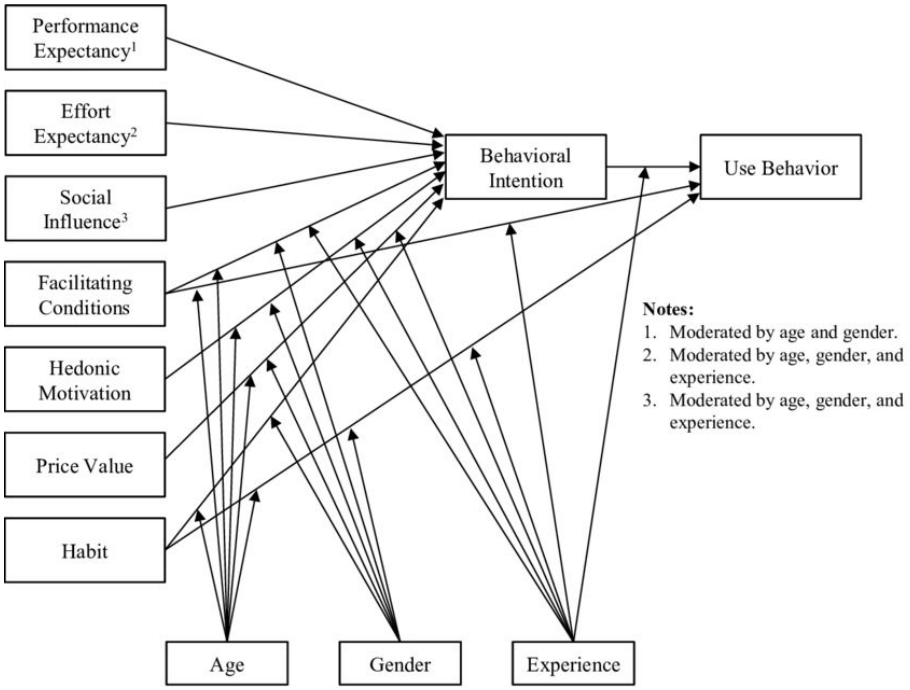


Figure 1. Reprinted from "Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology", by Venkatesh et al., 2012, *MIS Quarterly*, *36*(1), p. 157-178.

In order to gain insight into the principles and requirements of a PCE, the existing model UTAUT2 was analysed. Because a PCE does not yet exist, research must show which factors are taken into account as principles and requirements. To verify whether UTAUT2 is a strong basis for factors that determine the acceptance of a PCE, the following sub-question has been formulated:

Sub-question 3: *To what extent do factors of UTAUT2 influence the intention to use a Personal Consumer Environment?*

2.6 Trust in relation to a PCE

Apart from the factors of UTAUT2, trust could also be a factor that determines the intention to use a PCE. Mayer, Davis and Schoorman (1995) describe that the core definition of trust originates from a willingness to take risks. To explain the role of trust, the Commitment-Trust Theory of Morgan and Hunt (1994) can contribute to this statement. For example, the research by Fulmer & Gelfand (2012) has confirmed that successful relationships between an individual and an organisation result in trust and bonding. This can be translated to the situation between retail companies with an online presence and consumers in which trust could be an important factor. According to Grabner-Kraeuter (2002), consumers are looking for reliable partners (retailers) because buying a product and sharing data can be vulnerable. Moreover, a lack of control can reduce consumers' trust. Also, when the relationship with a company is weak, the relationship between consumer and company will be short (Koufaris & Hampton-Sosa, 2004). Besides the fact that trust in the relationship between consumer and retailer can influence the use of a PCE, trust in a PCE can also be an important factor. This is confirmed by the research of Delgado-Ballester and Luis Munuera-Alemán (2001) in which trust in a technology is essential. If the consumer does not trust the technology or the application of a PCE, the consumer can be more reluctant. Additionally, the intention to use increases when an individual has trust in the technology (Gu, Lee, & Suh, 2009).

2.7 Privacy in relation to a PCE

In addition to trust, privacy is also closely related to the intention to use a PCE. This can be confirmed by the research of Janssen and van den Hoven (2015). This research indicates that privacy is a key factor in technology related to the use and collection of (retail) data, such as a PCE. The study by Norberg, Horne & Horne (2007) also indicates that consumers are concerned about their privacy through the use of data collection. Because consumers leave electronic footprints of activities, consumers are concerned about how companies collect and use their private information (Graeff & Harmon, 2002; Janssen & Kuk, 2016; Morey et al., 2015). This issue derives from the fact that retail companies collect and process retail data in their own way, which has a direct impact on an individual's privacy (Pearson, 2013). As a result, this can be a risk for the privacy of a customer because, as soon as consumers get more control over their retail data, considerations will be made between the benefits and the risks (Xu, Dinev, Smith, & Hart, 2011). If the risks of collected retail data are not recognised, privacy concerns will not increase (Dinev & Hart, 2005). Consumers must be aware that retail companies are collecting information related to

the consumer. Otherwise, consumers will not feel the urge that they need to protect their privacy. When consumers don't experience this urge, the chance of the intention to use a PCE will not be significant. The research of Pierce, Kostova and Dirks (2003) confirms that individuals should have the sense of ownership of their retail data. This sense of ownership can decrease when the consumer's retail data is too complex or less perceptible (Kamleitner & Mitchell, 2018).

2.8 Privacy fatigue in relation to a PCE

Besides the fact that privacy, in general, can be related to the intention to use a PCE, privacy fatigue is an emerging factor in the world of the data-driven economy. The study by Keith, Maynes, Lowry and Babb, (2014) describes that privacy fatigue manifests itself when consumers' personal data is too complex to protect. This privacy fatigue can reduce the focus on privacy issues due to the complexity of having control over your data (Acquisti, Friedman, & Telang, 2006). Privacy fatigue can impact the use of a PCE and should therefore be reduced to ensure that consumers regain control of their retail data and protect their privacy. As a result of privacy fatigue, users may eventually think that they can no longer protect their own retail data, which may also cause psychological stress (Choi, Park & Jung, 2018). When confronted with this psychological stress, consumers may protect themselves and as a result, not actively protecting their privacy. For example, consumers accept cookie-statements because they see no other possibility. The cause of this reaction is related with minimizing decision-making by choosing the easiest option, such as accepting the cookie statements (Levav, Heitmann, Herrmann, & Iyengar, 2010). Furthermore, the study by Choi, Park, and Jung (2018) describes that privacy fatigue can also have consequences on the long term. Therefore, the consumer may consider the personal information collected in this way as unimportant. This urge may change later on. However, consumers may consider it impossible to protect their privacy any longer (Zhang, Zhao, Lu & Yang, 2016). The consequences of privacy fatigue relate to the weighing of decisions. With regard to online privacy, the decision of whether or not to disclose personal information is the result of these subjective evaluations (Dinev & Hart, 2006).

To gain insight into the extent to which the factors trust and privacy influence the intention to use a PCE, these factors have been viewed from the perspective of the consumer. Therefore, the following sub-question has been formulated:

Sub-question 4: *What is the effect of trust and privacy on the consumers' intention to use a Personal Consumer Environment?*

According to this theoretical framework, four sub-questions have been addressed. Together, these sub-questions should contribute to answering the central research question. In the next chapter we discuss how the central question has been approached:

Central research question: *What are the principles and requirements of a Personal Consumer Environment (PCE) in retail that are expected to contribute to consumer acceptance?*

3 Method

In this chapter we discuss the approach towards the research design. First of all, the research design is discussed with the required materials. Subsequently, the procedure, the pre-test, the participants and finally the analysis of this research are discussed.

3.1 Research design

To gain insight into the principles and requirements of a Personal Consumer Environment (PCE), a qualitative method was used for this exploratory study. Specifically, focus groups were used because this research focuses on a new emerging topic. By using focus groups, the group dynamics ensure the important aspects of a discussion. Furthermore, this research has focused specifically on consumers from the Netherlands. With this target group, the aim was to achieve a wide variation between various demographic factors: age, gender and level of education. By varying these demographic factors, 'natural groups' emerge in which interactions can be observed that are very similar to usual activities. To achieve this goal, a total of 6 semi-structured focus group sessions were held, with 5 participants in each session. In total, a sample of 30 participants participated in this research. As a result, saturation was reached after 6 focus group sessions. The duration of each session was between 52 and 71 minutes.

In these focus group sessions, three main topics, which follows from the theoretical framework, were discussed which contributed to answering the sub-questions and the central research question: knowledge about data collection (RQ2), need and feeling of control (RQ1) and principles and requirements of a PCE (RQ3, RQ4).

First of all, the topic of knowledge was discussed. The goal of this topic was to get an understanding to what extent the participants have knowledge about what retail data is and how it is collected. Secondly, the topic of control was discussed to get an understanding to what extent consumers experience control over their data and whether consumers want control over their data. Finally, the topic of principles and requirements was used to verify which factors of UTAUT2 and factors such as privacy and trust are important in the acceptance of a PCE, according to consumers. A complete overview of which sub-questions relate to which topic is shown in Table 1.

Table 1
Overview focus group topics

Approach to the method	Based on theoretical framework	Key concepts	Focus group topic
Sub-question 1	To what extent do consumers experience a feeling of control over their retail data?	Control	Need and feeling of control
Sub-question 2	What do consumers currently know about data collection in the context of retail companies with an online presence?	Retail data	Knowledge about data collection
Sub-question 3	To what extent do factors of UTAUT2 influence the intention to use a Personal Consumer Environment?	UTAUT2	Principes and requirements
Sub-question 4	What is the effect of trust and privacy on the consumers' intention to use a Personal Consumer Environment?	Trust & Privacy	Principes and requirements

3.2 Materials

This research required a number of materials and a suitable room to organize six focus groups. To be more specific, a room was used to welcome the participants and to discuss a PCE in a quiet environment whereas distractions might obstruct the session (Figure 2). A requirement of this room was a whiteboard and a TV screen to make the focus group session interactive. A TV screen was used as an aid to present the topics, the questions and an introduction video during the focus group sessions. The whiteboard was used to make an overview of the input of the participants, the principles and requirements, and to feed the plenary discussion. A digital video and audio recorder was used to record the sessions. These recordings were used to record conversations and discussions of the participants and to analyse non-verbal communication. In addition, the video material contributed to distinguishing what each participant said. Finally, the participants were thanked for their time and effort by providing a present.

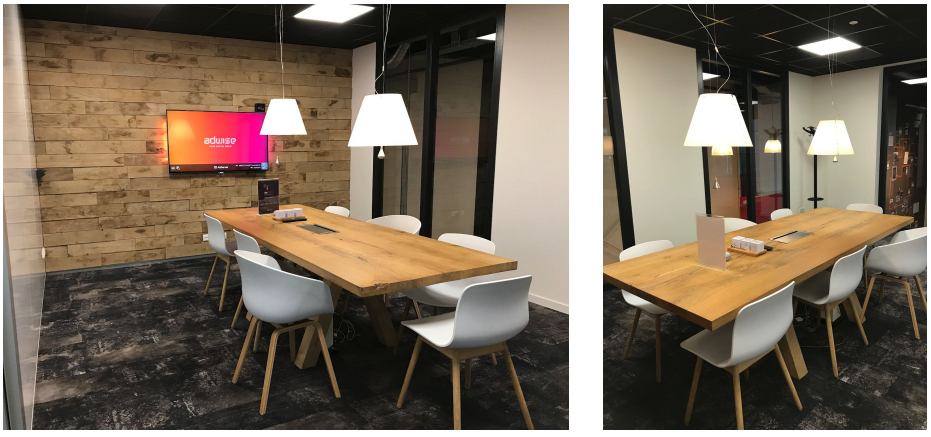


Figure 2. Room for the focus group sessions

3.3 Pre-test of the focus group

In order to test the protocol of the focus group session, a pre-test was organized. The goal of the pre-test is twofold. First to verify if the setting facilitates constructive discussions without obstructions. Secondly, to verify if the questions fed a fruitful discussion. With this protocol the aids, the room and questions were tested. The basis of these questions were linked to the three topics (knowledge, control, principles and requirements) of the session. The pre-test was carried out with 5 participants. These participants formed 1 focus group (Appendix A). This focus group session consisted of 3 men and 2 women. The average age of this group was 22 years (SD = 3.0). The youngest participant was 19 years old and the oldest participant 26 years old. In terms of educational level, the highest degree was Secondary vocational education or Higher professional education. Here, these participants of the pre-test were gathered from the researcher's network. Apart from the participants, the researcher (moderator) was responsible for running the pre-test and the assistant moderator was responsible for the evaluation of the pre-test.

After the pre-test the participants were asked for feedback about this session. Participants were asked to evaluate the pre-test as actively and critically as possible. The protocol and the setting were evaluated by the moderator and assistant-moderator using the gathered feedback. As a result, a new open question was created and extra time was reserved for the topic ‘control’ and the topic 'principles and requirements'. The new open question was needed to make sure that all participants could provide their input for the principles and requirements of a PCE. More time was required to get a better understanding to what extent participants like to have control over their data. An overview of these adjustments has been made in Table 2. Based on these adjustments to the protocol from the pre-test, a definitive focus group protocol is created. This protocol can be found in Appendix B.

Table 2
Changes based on the pre-test

Changes in the protocol		
	Related to	Modification
Adjustment 1	Time schedule for the topic: control	From 10 minutes to 15 minutes
Adjustment 2	Time schedule for the topic: principes and requirements	From 15 minutes to 20 minutes
Adjustment 3	Additional question for the topic: principes and requirements	"If you look at the overview of principles and requirements, would you like to add something here?"
Adjustment 4	Time schedule for the topic: closing	From 10 minutes to 5 minutes

3.4 Protocol

Based on the pre-test a final protocol has been developed for the focus group sessions (Appendix B). These focus groups followed the same structure as set up for the pre-test. This means that the following components are covered: introduction, topic 1 (knowledge about retail data), topic 2 (need and feeling of control), topic 3 (principles and requirements) and closing. In the following sections we discuss the protocol in more depth.

Introduction

The focus group session started with an introduction. During the introduction of the focus group session, the moderator and the moderator assistant introduced themselves to the participants. Subsequently, all participants introduced themselves by telling who they are and what their current employment is. Subsequently, on behalf of the moderator, the purpose and focus of the research were briefly discussed. After that, the first step in this process was to obtain written informed consent from the participants. Written informed consent was necessary to give the participant the opportunity to ask questions, to reflect on his/her participation and to agree that the focus group session was recorded. In addition to the written informed consent, a form was requested (Appendix C). This form asked for the participant's demographic factors: age, gender, and highest level of education. These demographic factors were used as confirmation for the variation of participants within a focus group session. Additionally, these factors were used to investigate if there were correlations between the results and the demographic factors. Both the informed consent and the form of the demographic factors have been signed by the participants of this research. Next, an explanation was given which topics and questions were discussed during the focus group session. Key concepts such as digital environment and retail data were explained.

Topic 1: Knowledge about retail data

Following the introduction, the first topic was discussed in relation to the level of knowledge. This discussion was moderated by asking open questions and explicitly asking for experiences. Once a participant had explained his knowledge about data, follow-up questions were asked by the moderator. After a statement was given by a participant, the moderator asked for the opinion or reactions of other participants. In order to give more direction to data collection, an illustration of a Personal Health Record (PHR) was given as an example of a digital environment. An example question that was asked was as follows:

“Are any people familiar with the Personal Health Record?”

By asking this question, participants shared their experiences and explained in the group what a PHR is. Subsequently, the moderator asked what the role of data could be in this digital environment. This resulted in discussions between the participants. Besides that, participants were asked if they had any knowledge about the data collection by retail companies with an

online presence. By asking for experiences of the participants, they shared information with each other. As a result, participants with limited knowledge were able to respond to the examples that were given.

Topic 2: Need and feeling of control

The second topic is introduced with an explanatory video about the PHR to provide insight into how data is used in a similar digital environment where individuals have control over their medical data. Based on this video of a PHR, the moderator introduced the PCE to the participants. This presentation emphasized that the focus of a PCE was on retail data including personal information from retail companies with an online presence. As a result, participants were asked to what extent they want to have control over this type of data. Additionally, participants were asked to indicate whether they already felt in control of retail data. These same questions were asked in relation to medical data. This was done to analyze how the need for control differed from sector to sector. An example of a question that was asked in this second topic was as follows:

"Do you feel like you already have control over retail data from companies with an online presence?

Topic 3: Principles and requirements

Principles and requirements of a PCE was the third and final topic of the session. This topic was used to gather other insights related to the central research question. As discussed before, all participants had shared knowledge about retail data and the need for control over this data. Subsequently, the participants were asked to reflect on what a PCE would look like. Whereas the purpose of the session was to have a fruitful discussion, the participants were asked to think aloud. If the group struggled with this assignment, the moderator assisted them by referring to the example of a PHR. After the first round of ideas the participants were asked to formulate requirements and risks of a PCE individually to gather as many ideas as possible. By also asking for identifying the involved risks, more insights are gained into the possible drawbacks of a PCE. To provide insight into the principles and requirements, the participants were asked to write them down on post-its. These were assembled on the whiteboard to create an overview of the collected ideas and risks (Figure 3). If the participants struggled with the assignment, more information was provided based on the UTAUT2 factors and trust and privacy factors as identified in chapter 2. However, this was hardly applicable. The main questions in this topic were similar to the following questions:

“What requirements should this personal consumer environment meet?”
“What are the drawbacks/risks of this personal consumer environment?”

Figure 3. Overview of requirements (green) and drawbacks (red)

After all input had been collected and arranged, the overview with the requirements and risks or drawbacks were briefly discussed with the participants. In this way the participants were able to give elaborate on their input to the group. The moderator also stimulated the participants to discuss with each other. This was achieved by asking other participants if they agree upon each other.

Closing

When the time limit was reached, a signal was given by the moderator-assistant. This meant that the focus group session was coming to an end. At last, the participants had the final opportunity to add some ideas that might not come up during the plenary discussion or the individual assignment. After the participants had this opportunity, they were asked if they wanted additional information on this subject. If this was no longer the case, participants were thanked for their time and effort. As a thank you there was a gift from moderator and moderator-assistant to end the focus group session.

3.5 Participants

Whereas this research focuses on Dutch consumers, the sessions of the focus group were conducted in Dutch. A sample of 30 participants has been selected to participate in 6 heterogeneous focus groups, with 5 participants in each group. The heterogeneous groups are characterized by differences in the following factors: age, gender and level of education. Because variation was used in the demographic factors of the focus group, discussions arose where opinions often diverged. Participants were triggered to take other perspectives as well. To be more specific about the demographic factors, an overview was drawn based on the total sample. Of all 30 participants, 10 were male and 20 were female. The average age of the participants was 32 years (SD=13.8) with the youngest 17 years and the oldest 60 years. The participants in the focus groups also varied strongly in their level of education. Most participants

had a completed Higher Professional Education (11 out of 30) or Secondary Vocational Education (7 out of 30). The total overview of the 30 participants of the differences in the demographic factors per focus group are visually represented in Appendix D.

In order to select participants to participate in a focus group, two requirements had to be met. First of all the participants must be at least 16 years old because of the privacy regulation. Secondly, the participants were not allowed to be employees of a marketing agency. This is to prevent a biased view which might influence the results of this research. To recruit participants, convenience sampling and snowball sampling has been applied. This means that the researcher has asked individuals from his own network to participate in this research. These participants were also asked to recruit other participants from their network. Finally this resulted in a pool of 30 participants. Based on availability and the available information of demographic factors, the selection of focus groups was made. In the first instance, the aim was to combine different ages in one group (Table 3).

Table 3
Focus group distribution

Demographic factor: Age							
		Group 1 (n=5)	Group 2 (n=5)	Group 3 (n=5)	Group 4 (n=5)	Group 5 (n=5)	Group 6 (n=5)
Age	Avarage (SD)	33 (12.8)	32.4 (15.4)	26.6 (7.7)	39.2 (14.9)	29.2 (12.2)	35.4 (19.9)
	Median (Min, Max)	31 (19, 49)	33 (17, 53)	26 (18, 39)	44 (22, 58)	24 (23, 51)	23 (20, 60)

3.6 Data processing and analysis

After all data from the focus group sessions was collected, the recorded audio was transcribed verbatim. Next, discussed personal information such as name, job or a location were anonymized. After a re-check, the transcriptions were ready to be coded. In this case, the coding process was started according to the guidelines of Boeije (2009). In this process, all analyses were carried out on the total sample and not on an individual level.

First of all, the transcriptions were read in detail and a start was made with the orientation on coding, which was followed by three processes: open coding, axial coding and selective coding. The texts were segmented based on independence, completeness and relevance of the information. This was done by marking the segmented quotes in the software program: ATLAS.ti. For each document, the text elements varied between 104 and 154 quotations. Besides the marked quotes, comments were made for possible clarification. Next, the participants were tagged and the demographic factors per participant were linked to this. Based on these tags, it is possible to discover connections with the factors.

As a first step of orienting encoding, there is open coding. This means that the marked quotes have been read again and given descriptive labels. An example label given to a highlighted

quote was as follows: "*needs to have control over retail data*". Subsequently, all six sessions were read carefully and a first attempt was made to label the highlighted quotes.

The second step in orienting on coding is axial coding. After creating a long list of descriptive labels in ATLAS.ti, the codes were compared with each other. Codes that looked similar or had been used minimally were merged with other codes where necessary. Next, the main categories were created based on the script of the focus group session and the related sub-questions. This is shown in Table 4. Codes that were related to each other were given an overarching category. Finally, this process was repeated several times and re-analysed per session to create matching labels and categories for the final codebook (Appendix F). In this process, both open coding and axial coding were initially only applied to the first three of the six focus group sessions.

Table 4
Resulted categories from the codebook

Main categories		
		Related to
Categorie 1	Consumer knowledge about retail data	Research question 2
Categorie 2	Level of control	Research question 1
Categorie 3	Principles and requirements of a PCE	Research question 3 & 4
Categorie 4	Risks of a PCE	Additional result
Categorie 5	Consumer attitude toward data	Additional result

Based on the first three coded transcripts of the focus group session, the reliability of the codebook was measured. The purpose of this measurement was to avoid that the codebook had to be adjusted at the end of the analysis. Consequently, a second encoder performed a coding round. A random session was chosen for analysis. A conscious choice was made to analyze non-separate paragraphs of different transcripts of the focus group sessions. This because it was difficult to interpret these single paragraphs without context. The second coder was shown the full transcript of session two with the highlighted quotes without codes. This allowed the second coder to analyze the entire context with the compiled codebook. The results of the first coding by both coders were then analysed using Cohen's Kappa to test the reliability. As can be seen in Table 5, this resulted in Kappa 0.84. Since the Kappa value is above 0.75, this means that the author's coding is valid (Cicchetti, 1994). Because there were some consistent differences in the codes of the transcript, these have been changed and discussed (Appendix E). However, this did not affect the final codebook shown in Appendix F. Subsequently, the last three focus group sessions were coded based on this definitive codebook.

Table 5
Intercoder relationship with Cohen's Kappa

Symmetric Measures		
		Value
Measure of Agreement	Kappa	0.836
	N of Valid Cases	121

The third step in this process was selective coding. This means that based on the final codes it was investigated whether there were any links between the different categories. This is done by filtering in ATLAS.ti, within quotation manager, two random combined categories. In addition to reading, this created an overview of which categories were often presented together. In the next chapter, the connections that were addressed in this way are supported by quotes from the focus group sessions.

In addition to examining the links between the main categories, further research was carried out into the relationships between the codes and demographic factors. This was done based on a correlation analysis (Appendix G). The reason that the focus was placed on age, is because most of the correlations were visible in this area and is also one of the moderators of UTAUT2. Because there was only information from 30 participants, no significance can be stated. However, it does provide insight into possible relationships of this qualitative research. Other demographic factors were not included because they were out of scope.

4 Results

This chapter presents the results and findings. This is divided into five sections corresponding to the five different categories in the codebook. Sections are ordered according to the relationships between the different categories (Figure 4). Because the combination or parts of the categories contribute to answering the central research question and sub-questions, these will be answered in chapter 5. In all categories, the results and findings are discussed using the focus group sessions as a whole. In addition, the relationships between the categories will be explained under the related section. Quotations will be used to illustrate the results. The corresponding numbers of the quotations can be found in Appendix H. Finally, an additional section will be presented on the effect of demographic factors.

Figure 4. Relationships between the categories

4.1 Category 1: Consumer knowledge about data

The first topic discussed during the focus group sessions was related to knowledge. Specifically, the knowledge of a digital environment, data collection and legislation were discussed. To get everyone in the focus group familiar with the concept of a digital environment, a similar existing environment, the Personal Health Record (PHR), was introduced. Most participants were already familiar with a PHR because they worked with it in the health sector. Other participants had read something about the goal of a PHR. Participants who were not familiar with this digital environment became knowledgeable through the other participants and the introduction video that was shown during the focus group sessions. Because the information about a PHR came from different sources and backgrounds of participants, the knowledge and description of a PHR varied. As a result, knowledge about a digital environment differed from session to session.

Regarding the level of knowledge on data collection, different possibilities were mentioned to explain data collection. These were related to medical data or retail data. Participants who were familiar with a PHR knew how medical data is processed in this environment. However, the technique behind a PHR was unknown or difficult to grasp for many participants. To explain how data was processed in a PHR, examples were mentioned as: 'through your general practitioner, doctor or insurance company'.

Results based on the translation of medical data into retail data, different explanations were mentioned to explain the collection of data. Many participants were able to give examples of how retail companies with an online presence obtain data from a consumer. However, there was a lack of knowledge about the different types and sensitivities of retail data. The explanation of how retail data was collected was mixed. Most examples were related to the following topics:

online search behaviour, online click behaviour or related to smart devices. An example of data collection from this perspective was as follows:

> [1] *"But of course you also have Google Home that listens with us. But also Siri who listens. Maybe there are companies behind these systems that know what I'm talking about and use this information as well. " (Session 1, participant 1, male, 49 years old)*

Related to the examples of online search behaviour and online click behaviour, the subject 'cookie statements' came up several times. This to explain how retail companies collect data with their online presence. As a result, many participants had knowledge about the presence and purpose of cookie statements. However, there was little knowledge about how participants could delete their personal retail data.

Following this result, the GDPR was discussed in all sessions. This was done in order to find out to what extent the participants had knowledge about retail data and their rights as consumers. However, most participants had no knowledge about the content and effect of the GDPR. Especially because this was often too complex. However, there were a few participants who had knowledge about consumer rights. A reaction demonstrating this knowledge was as follows:

> [2] *"As a consumer you have the right to oblivion. You can ask retail companies to remove all your data. " (Session 3, participant 11, male, 26 years old)*

Based on the knowledge that was discussed about a PHR, data collection and the legislation, insight was gained into the current knowledge of the participants about retail data. Also by discussing this knowledge, a representation of a digital environment was formed by the participants.

Knowledge in relation to control

Related to the knowledge of retail data and data collection, the analysis of the focus groups resulted in a relationship between the category knowledge and control (Figure 5). This is demonstrated by the participants who had both knowledge about the subject as well as the need to have control over the data collected from retail companies with an online presence. They had more insight into the possibilities of the collected data. As a result, these participants already took action themselves. This is evident from the following quotes from the same participant:

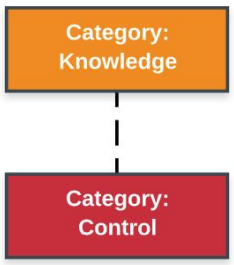


Figure 5. Relations between two categories

> [3.1] *"Yes, of course we have the GDPR. The right to be forgotten as an individual. This is the part that is now possible and important for consumers." (Session 4, participant 18, female, 22 years old)*

[3.2] *"Sometimes I just delete all the cookies on my phone or laptop. But I keep doing that all the time. Well, that's not what I want." (Session 4, participant 18, female, 22 years old)*

For a detailed representation of the relationships between the codes of the category knowledge and control, an overview is provided in Appendix I.

4.2 Category 2: Level of control

The second topic discussed during the focus group sessions related to the degree of need for control over data collection. Based on the example of a PHR, the majority of participants indicated their need for control over their retail data. This need for control was based on a large number of participants who currently do not experience control over their retail data. The need for control was remarkably greater in comparison to the need to control the medical data of participants. Since the trust in the medical sector was higher compared to the trust in the retail sector. A reaction that demonstrates a strong need for participants to have control over their retail data is as follows:

[4] *"Yes, I think a lot of people would like that [Having control over retail data]. For example, if it's just a little easier to read what's in the cookie statements. This already helps to get control of your privacy." (Session 1, participant 3, female, 30 years old)*

Few participants did not feel the need to have control over their retail data. The involved risks of the distribution and use of retail data by retailers had not yet been experienced by these participants. However, these participants did not feel in control of their retail data either. This result corresponds to the few participants who had not considered the question of having control over their retail data.

In addition to the need for control that has been addressed, the need for control is also related to the perception of data by participants. This study indicated that most participants experience a difference between retail data and medical data. As a result, these differences influence the extent to which participants experience control over their data. A few participants experienced both types of data as important to have control over, as demonstrated by the following reaction:

[5] *"Yes, but medical data could also be used for commercial purposes. If you have diabetes, for example, and you need a pump, that is also commercial related." (Session 2, participant 8, female, 17 years old)*

Except that there is a need for control over retail data, most participants experience no control over the retail data collected by retail companies with an online presence. Even the small group of participants who take steps to protect their retail data confirms even if they experience no control. This is illustrated by the following example:

[6] *"But you just don't get any feedback about the use of your data. It's that simple. All you know is that they've collected it, and luckily you can erase your entire history of data". (Session 6, participant 30, male, 60 years old)*

Control in relation to attitude

Related to the experience of control and the need for control, the analyses of the focus groups resulted in a relationship with the attitude of the participants (Figure 6). This research indicates that many participants want control over their retail data. This need for control was often associated with the argumentation of fear and distrust from the participants. Fear and distrust were focused on the approach of retail companies with retail data. This relationship was confirmed by the following quotes from the same participant:

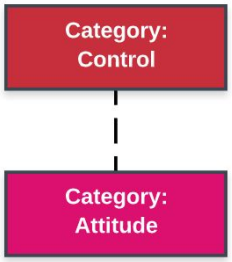


Figure 6. Relations between two categories

[7.1] *"You know what it is, things change when other organizations want to get involved, too. Then I want to keep control." (Session 2, participant 10, male, 53 years old)*

[7.2] *"This is all information that can be used against you. It's scary that everyone gets to see that or do something with it." (Session 2, participant 10, male, 53 years old)*

However, a small group had no need to control their retail data. They also expressed themselves in a different way. Nevertheless, these participants were mainly irritated towards the use of retail data by retail companies with an online presence. This relationship was confirmed by the following quotes from the same participant:

[8.1] *No, but it's more if you look somewhere, that the result is that you get personal offers every time. I don't want that. I just don't want to get anything." (Session 5, participant 21, female, 24 years old)*

[8.2] *Well, it's a lot of annoyance, but I just don't need that control." (Session 5, participant 21, female, 24 years old)*

For a detailed representation of the relationships between the codes of the category control and attitude, an overview is provided in Appendix I.

4.3 Category 3: Consumer attitude towards data

In addition to the results on the sub-questions of this study, further results were discussed that have an influence on the central main question. The attitude towards the use of data of the participants was also discussed. The participants in this study had a remarkable attitude towards the degree of control, the use of retail data and the development of a Personal Consumer Environment (PCE).

Few participants were particularly curious about the possibilities of a PCE. Especially the participants who had experience or knowledge about the use of retail data. Moreover, much distrust was expressed regarding the collection of medical and retail data. Only a few participants were emphatically distrustful about the collection of medical data. These participants were afraid that medical data would be used for other activities, as the following reaction illustrates:

> [9] *"And I think your medical records could also affect getting a job or a mortgage." (Session 1, participant 2, female, 23 years old)*

More participants were distrustful about the collection of retail data with an online presence. There was dissatisfaction with the collection and selling of consumer-related retail data. Participants acknowledge their lack of control. Furthermore, distrust of retail companies is increasing since retail data is unreadable for them, as described below:

> [10] *"You just don't know who has all this data and what they're going to do with it in the end. That's much more abstract than a medical record. So I trust that a lot less". (Session 4, participant 20, male, 26 years old)*

As well as distrust in retail companies, participants were also concerned about the approach of retail companies to their retail data. This was often described as 'scary'. This attitude often arose at the end of a session, when participants became more aware of the possibilities to collect data. This information was often received from other participants who shared their experiences. A related reaction at the end of the session is as follows:

> [11] *"I don't have anything to add now, but I suppose I'll think about it tonight and turn off the cookies. Well, I don't know". (Session 1, participant 3, female, 30 years old)*

Although the majority of participants confirm their distrust or fear of the collection of retail data, a few participants had a different attitude towards it. Remarkably, these participants were more likely to see the trust and positive side of retail companies controlling their data, as illustrated below:

> [12] *"They often know exactly what I like to buy. If I get a nice offer [from a retail company], and it saves me money". (Session 4, participant 17, female, 44 years old)*

Finally, the 'irritation' attitude was very noticeable in relation to the use of retail data. Some participants were particularly annoyed by the use of the collected retail data. This manifested itself in the delivery of irrelevant personal offers. The need to have control over these retail data varied widely. Some participants wanted to have control and some did not. A reaction in which the irritation was expressed is as follows:

[13] *"I think it looks like stalking. I find it very annoying. When I look at something once, you immediately see commercials about it everywhere". (Session 5, participant 21, female, 24 years old)*

Attitude in relation to risks of a PCE

Related to the attitude of participants towards the use of retail data, the analysis of the focus groups resulted in a relationship between the risks of a PCE and the attitude toward the collection of retail data (Figure 7). Detailed explanations of the risks of a PCE will be discussed in section 4.5.

As discussed earlier, many participants felt a strong distrust of the use of retail data from retail companies with an online presence. As a result, participants recognized risks in the leakage or misuse of this data. The risk of misuse or leaking data was supported by the negative information that was shared by the media. A reaction supporting this link between attitude and the risks of a PCE was illustrated by the reaction of participant 1:

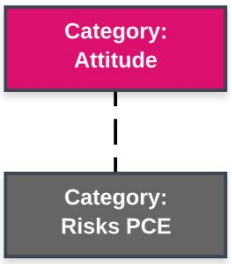


Figure 7. Relations between two categories

[14.1] *"I think quite a few people are suspicious about the use of retail data right now. This is because you often hear that there is a data leak somewhere or that our data is public anyway." (Session 1, participant 1, male, 49 years old)*

[14.2] *"If a PCE leaks its data, they [other organizations] may also see data about you that you did not want to share." (Session 1, participant 1, male, 49 years old)*

In addition, few participants expressed irritation at the use of retail data by retailers with an online presence. This behaviour was related to the risk of privacy fatigue. Because participants were irritated about how retail data was collected, the less active they were in protecting their privacy. A reaction in which this relationship is explained by the same participants is illustrated in the following quotes:

[15.1] *"I find it very annoying when I am constantly receiving banners with advertisements or websites that I have clicked on. You get to see this information again." (Session 3, participant 13, female, 26 years old)*

[15.2] *"But it's also the laziness of a person, you like it that you don't have to think about data use. I don't do anything about the protection of my privacy." (Session 3, participant 13, female, 26 years old)*

For a detailed representation of the relationships between the codes of the category attitude and risks of PCE, are illustrated in Appendix I.

4.4 Category 4: Principles and requirements of a PCE

The last topic discussed during the focus group sessions were the principles and requirements of a PCE. A selection of the factors that were discussed by the participants within the focus groups is given below. The factors that were coded most often during the analysis are discussed first. Together, this resulted in thirteen principles and requirements. In addition to these thirteen factors, another paragraph will follow to address a sub-question of this study. This last paragraph discusses the comparison with the UTAUT2 factors.

1. Effort Expectancy

The first factor that was discussed frequently in all six focus groups was: Effort Expectancy. This factor was also often discussed by the participants at the beginning of the discussions. Effort Expectancy was identified by the participants as an obvious factor. However, the participants were often disappointed that this was not the case. The reason this was often mentioned was because the subject of a PCE was sometimes difficult. In addition, the participants nowadays do not know how to control their retail data. For this reason, it was essential for participants that user-friendliness came first. This was expressed in the following way:

> [16] *"Cause I'm not a computer expert. It should be simpler for me." (Session 2, participant 10, male, 53 years old)*

2. Price Value of a PCE

The next factor that was discussed more than once in five of the six focus groups was related to costs and benefits. Based on the UTAUT2 model, also named as Price Value. According to multiple participants, it was repeatedly stated that a PCE should not cost the consumer any money. Instead, the participants confirmed that sharing their retail data should deliver something. What the retail data of the consumer should deliver was unknown. This means that participants are willing to share their retail data with retail companies with an online presence, as long as they get something in return. However, one focus group came to a different conclusion regarding the costs and benefits. From these participants it was expected that if they would have to pay for a PCE, they would expect a certain quality or reliability. The reactions from which it became clear that Price Value affects the intention to use were as follows:

> [17] *"Yeah, or you'd better use your personal data yourself. That you can do something with your own data and that you can see this in a digital environment." (Session 4, participant 20, female, 26 years old)*

[18] *"I think we as consumers get far too little in return for what a company gets in terms of information. So what we give to help companies. We hardly ever get anything in return." (Session 6, participant 30, male, 60 years old)*

3. Safety of a PCE

A third factor that was addressed in all focus groups but less often than Effort Expectancy and Price Value was: Safety. For many participants, safety was an important and unmistakable requirement for the development of a PCE. The participants often associated this factor with trust in retail companies. Participants mentioned the example of the Government as a safe environment. The example of the Government was mentioned to indicate the extent to which safety plays an important role for the participants. A reaction from a participant stating that safety plays an important role in the use of a PCE was as follows:

[19] *"Well, a safe environment. Well secured. That's just very important to me." (Session 4, participant 20, female, 26 years old)*

4. Performance Expectancy

Subsequently, Performance Expectancy was often discussed during the focus group sessions. This factor was discussed in order to raise the issue that a PCE should work as expected. A PCE must meet the expectations of the consumer. There was a lot of overlap between the participants in the expectations that a digital environment should deliver. In general, the participants wanted to be able to remove and change retail data by themselves. Control had to be in the hands of the consumer. This means that control and performance expectations are strongly related to each other. The following quotes illustrate this need:

[20] *"I really think it has to come from retail. I have this in my profile. Albert Heijn or Lidl were able to pick it up from the profile and they only read from there what I want and don't want." (Session 2, participant 9, female, 41 years old)*

[21] *"So you should not only be able to modify it but also be able to delete it. That it is different from what is possible now." (Session 4, participant 18, female, 22 years old)*

5. Single point of access

In the fifth factor, priority was given to centralising a digital environment that participants can access at any time. Availability and preferences regarding the use of retail data had to be centralised. The main focus here is not on technology but on functionality. Participants do not want to switch between different websites or different environments of retail companies. According to the participants, by centralizing the preferences of retail data, this offered the possibility to have more control over this retail data. The reactions that indicated that this factor is a requirement for a PCE were illustrated as follows:

[22] *"For me, it would really be a requirement to have all the different retail companies connected to one digital environment." (Session 4, participant 19, female, 46 years old)*

[23] *"I would like to have an application where all my preferences are stored for retail companies." (Session 5, participant 23, female, 23 years old)*

6. Awareness of data collection

A requirement that was mainly addressed in the first and fourth focus groups concerned awareness of the collection of retail data from consumers. When identifying principles and requirements, it emerged strongly that many participants were not yet aware of the possibilities of using retail data. As a result, many participants indicated that creating awareness had a strong influence on the intention to use a PCE. Repeating the negative consequences of not protecting retail data, giving triggers to protect your data or sometimes scaring the consumer of the consequences, was mentioned by some participants as an example to create awareness. This requirement was reflected, for example, in the expression of participant 4:

[24] *"Yes, I think if you highlight the collection of data, you'll wake people up. This could also make people anxious." (Session 1, participant 4, female, 43 years old)*

7. Trust in a PCE

One factor that was addressed three out of five during the focus group sessions, related to trust in retail companies. Trust was also a determining factor for the use of a PCE. Participants confirmed that trust in the organization that was going to develop a PCE had to be trusted. In addition, techniques were identified that, according to the participants, contributed to the trust and use of a PCE. Examples such as: a fingerprint scanner or two-factor verification were mentioned as trusted tools. A reaction indicating that trust is an important factor in the use of a PCE was as follows:

[25] *"When I look at the data from the Personal Health Record, I assume that the professionals will handle it with the greatest care. I want to feel the same way about a digital environment with other data." (Session 6, participant 27, female, 23 years old)*

8. Level of consumer control

The eighth factor discussed as often as trust is the degree of control in a PCE for a consumer. The requirement of control was explicitly addressed in order to argue that control should only concern the consumer. They want to have the choice of what to do with retail data before it is used by retail companies or related agencies. How much control or at what level of control can differ per consumer. The need for this requirement from the participants was explained by the following example:

[26] *"That all companies drop the information in your Cloud. And after that, companies will only be able to retrieve the information from your Cloud if you have given your permission." (Session 2, participant 6, male, 21 years old)*

[27] *"Then blockchain. You will encrypt the information you want to store on the platform and send it to everyone and then everyone will have information. This way everyone can check if the information is still correct and if it has not been changed." (Session 3, participant 11, male, 26 years old)*

9. Accessibility of a PCE

One factor that was mainly addressed in the first few focus groups was the accessibility of using a PCE. This factor is coded separately from user-friendliness. With accessibility, the focus was mainly on the influence of differences in age and knowledge. According to the participants, these differences could influence the accessibility of a PCE. This was explicitly mentioned because mixed focus groups were used in which demographic factors vary. Below, two responses were quoted in which the importance of accessibility was highlighted:

[28] *"For example, if you are 16 years old or younger, your parents can decide that for you. And when you're an adult, you can decide for yourself what you want to share and what you don't." (Session 2, participant 6, male, 21 years old)*

[29] *"It should not depend on whether someone has more or less knowledge of it or is better able to use a computer. Everyone should have access to their data and be able to manage this data." (Session 4, participant 20, female, 26 years old)*

10. Facilitating Conditions

The tenth factor in the set of principles and requirements, related to the resources needed to contribute to the intention to use a PCE. The participants indicated that their intention to use a PCE would increase if appropriate tools were provided to better support the technique behind a PCE. During the sessions, different facilitating examples were mentioned that ultimately stimulated their use of a PCE and also created awareness. An example of facilitation tools is illustrated below:

[30] *"Yes of those 30/40 second movies that explain to you very briefly how it all works." (Session 3, participant 15, male, 18 years old)*

11. Time investment

A factor that was discussed less during the focus groups was time investment. Time investment was determinant for the use of a PCE. Time investment meant that the amount of time needed to control your retail data should be limited. According to the participants, at this moment it takes too much time and actions to manage retail data. This means that time is needed to make

efficient use of the consumer's attention. Examples in which this factor was addressed were the actions related to the acceptance of cookie statements. The need to make efficient use of the consumer's time was illustrated, for example, by the following reaction:

> [31] *"Imagine that you suddenly have to read all cookie statements for a digital environment, then things could get complicated. Because we hardly ever read them because it takes too much time. This way nobody would use it." (Session 3, participant 15, male, 18 years old)*

12. Personalisation of a PCE

One of the less-mentioned factors was related to the personalisation of a PCE. Although this was a factor that was not initiated as a requirement for all participants, certain participants wanted a PCE to be personalized. This was to ensure increased accessibility and user-friendliness. As an example, the intention to use would increase when the design of a PCE takes into account the level of entry of a consumer. A citation highlighting this need was as follows:

> [32] *"More like it's really made for you. It has to be an environment that is the same for everyone, but the information that comes in has to be really personal to you." (Session 2, participant 7, female, 18 years old)*

13. Social Influence to use a PCE

The social influence factor was the weakest topic during the sessions. However, this factor was discussed in three groups. The participants emphasized that people can support each other or help each other with the use and control of retail data. An explanation for this was that the control over your own data can still be complex. In addition, it emerged that individuals are also linked to each other as soon as they use the same devices. An example of an idea that was suggested in which Social Influence emerged strongly was as follows:

> [33] *"The younger generation could help the elderly generation to make decisions. Like which data you want to protect and share." (Session 2, participant 6, male, 21 years old)*

Comparison with UTAUT2

In order to understand whether the factors of a digital environment were additional or different from the UTAUT2 model, a representation is made in Table 6. The UTAUT2 model contains seven predictors that can support the acceptance of a new technology. Although technology is an important element in the acceptance of a PCE, factors such as *Hedonic Motivation* and *Habit* have not been addressed according to the participants of all focus groups. The *Habit* factor was not addressed as a principle or requirement because a certain imagination might have been expected from the participants. Because a PCE does not yet exist, it can be difficult for the participants to predict that the use of a PCE can become a habit. Because a similar digital environment as a PHR was also not used regularly, *Habit* was not discussed. As well as *Habit*,

Hedonic Motivation was not discussed by the participants, because a PCE is a functional digital environment to control retail data. The focus here is not on having fun, but on creating control and ownership for the consumer.

Table 6
Comparison of factors based on UTAUT2

Requirements	Presented during the sessions	Remarks
Factors of UTAUT 2		
Performance Expectancy	✓	
Effort Expectancy	✓	
Social Influence	✓	
Facilitating Conditions	✓	
Hedonic Motivation	-	Not addressed
Price Value	✓	Focus on the costs and benefits
Habit	-	Not addressed

4.5 Category 5: Risks and drawbacks of a PCE

As well as the principes en requirements of a PCE, the risks and drawbacks were discussed during the focus group sessions. A selection of the drawbacks that were discussed by the participants is given below. The factors that were labelled most often during the analysis are discussed first. According to the participants, this resulted in an overview of risks and drawbacks that has to be taken into account for the development of a PCE. The last paragraph will discuss the relations between the drawbacks and the requirements of a PCE.

Privacy fatigue

The first factor that was discussed as a risk for the intention to use a PCE is privacy fatigue. In five of the six focus groups privacy fatigue was mentioned frequently. This manifested itself specifically in the form of cookie statements. Participants indicated that in most situations they immediately accept the cookies out of convenience. Reactions such as frustration and fatigue were particularly noticeable when controlling their retail data. An example of these reactions was illustrated by participant 20:

> [34] *"I don't usually make a conscious choice. They don't really matter to me. You've accepted it so much that all your data is being used now." (Session 4, participant 20, female, 26 years old)*

In explaining this behaviour, it was confirmed that a large proportion of participants were not active in protecting their privacy in online environments. When participants are not open to more active protection of their privacy, the intention to use a PCE could be less. However, there were a

few participants where privacy fatigue occurred. These participants made conscious choices to protect their privacy in online environments. A reaction in which this emerged was as follows:

> [35] *"Yeah, the next thing you should do is clean it up at the end of the evening. Throw away all the cookies. So do I." (Session 6, participant 30, male, 60 years old)*

Risk of data leak

Apart from privacy fatigue, many concerns were expressed about the possible leakage of retail data related to a PCE. This risk was also discussed in all focus groups. When retail data was leaked, the participants' fear was that all this information would end up in the public domain. A lot of fear and uncertainty was expressed. According to the participants, these concerns were based on frequent data leaks being reported in the news. The risk of a data leak particularly exists when all retail data is collected in one central place, unless there is good security. A quote from a participant where this risk was highlighted was as follows:

> [36] *"This is because you often hear that there is a data leak somewhere or that our data is somewhere on the street." (Session 1, participant 1, male, 49 years old)*

Risk of abuse

A factor that was discussed as often as data leakage was the risk of misuse of retail data. This risk focused on the misuse of the collected retail data by retail companies or other organisations that could introduce a PCE. Participants in the focus group sessions realized that retail data has a lot of value for themselves and for companies. Concerns about the misuse of this data were related to the purpose of use. In other words, participants were concerned that retail data could be used for the wrong purposes. The following reaction shows that many participants are still sceptical about the use and control of retail data:

> [37] *"It's also on a personal database. Even if you've deleted it, they still have your information. They're not going to delete it just like that." (Session 1, participant 2, female, 23 years old)*

Risk of product introduction

A subsequent factor mentioned as a disadvantage or risk of a PCE was the risk of not seeing the benefit of this digital environment. This risk is not directly related to the design of a PCE, but to the introduction of a PCE because it will be a new type of product. The reason that this can be a risk or disadvantage for a digital environment is that a PCE would not yet be able to fully meet the needs of the consumer. This means that there is a risk that there are consumers who do not yet see the added value of using a PCE. This can be inferred from the fact that these consumers might not yet face the problem of the misuse or use of their retail data. Another possibility that confirms this risk is that added value is not recognised because there are consumers who accept

that they have no control over their retail data that is collected. A reaction naming this risk was as follows:

> [38] *"It's not like your cell phone's going to explode. Nothing's going to happen if I just press "accept". You just don't feel any drawbacks yet." (Session 4, participant 19, female, 46 years old)*

Risk of awareness

A factor that was less discussed according to the participants in the sessions was the risk of awareness. Although awareness was mentioned as a principle or requirement for a PCE, according to a number of participants, awareness also had drawbacks for a PCE. These participants explained that they could also imagine that a certain group of consumers might be afraid of the awareness of retail data collection by retail companies. By creating more awareness, this could cause a group of individuals to try to shut themselves off from the possibilities of collecting data. However, a few participants could identify this risk for a PCE. The demand for awareness seems to be greater.

Risk of personalisation

The last factor that was least discussed, but agreed upon within one focus group, was the risk of personalisation. The reason that personalisation was seen as a risk or disadvantage was related to the consequences of using a PCE. According to the participants, personalisation can also go too far, because consumers are more specific about their needs. This is because consumers confirm what they find important or are interested in. A reaction in which it emerged that personalisation could also be a risk was as follows:

> [39] *"Suppose you have access in a digital environment. Here you indicate which companies you explicitly find interesting. This might allow you to live your own bubble of advertising not knowing what else is available." (Session 2, participant 6, male, 21 years old)*

Risks of a PCE in relation to the requirements

Related to the risks of a PCE, the analysis of the focus groups resulted in a relationship with the principles and the requirements of a PCE (Figure 8).
This relationship has been addressed, among other factors, with the risk of data leakage or misuse of retail data. According to many participants from the focus group sessions, it was confirmed that creating a safe digital environment that can be trusted is key. By highlighting these requirements, the risk of data leak or misuse of retail data decreases according to the participants. This is illustrated by the following expressions of the same participant:

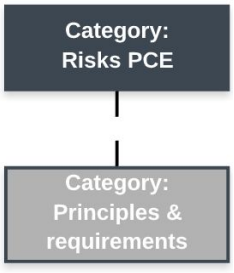


Figure 8. Relations between two categories

[40] *“Yes, I recognise hacking data as a major risk. Imagine if someone could look into my digital environment without permission and then use this information. They could do anything with it.” (Session 4, participant 19, female, 49 years old)*

[41] *“Well, a safe environment. Well secured. That's just very important to me.” (Session 4, participant 19, female, 49 years old)*

For a detailed representation of the relationships between the codes of the category knowledge and control, an overview is provided in Appendix I.

4.6 Age in relation to a PCE usage

In the last part of the results, attention is focused on a demographic factor: age. Because this research aims to vary the demographic factors, additional research has been done into the influence of age. Other demographic factors were not included because they were out of scope. Based on a correlation analysis, five relatively strong correlations between age and the factors that may influence the acceptance of a PCE were identified. All five possible correlations were above 0.4. Because there was only information from 30 participants, no significance can be stated. However, it does provide insight into possible relationships of this qualitative research. An overview of all remarkable correlations between age and the factors is given in Appendix G. Figure 9 demonstrates two relatively strong correlations between age in relation to privacy behaviour and the risk of awareness. The correlations of the codes A3, K1 and K4 were not included, because they related to the attitude, knowledge and description of a PHR, which deviated from the scope of this study.

The first factor from the category 'risks of a PCE' has been linked to privacy behaviour in the correlation analysis. Namely, the higher the age, the more clearly it is explained how the participants handle the protection of their privacy. This could be related to the fact that this target group also experienced how not explicit use was made of the consumer's personal data. Besides, they have expressed how they explicitly protect their privacy or consciously do nothing with it. The second and last factor that also comes from 'risks of a PCE' is the risk of awareness. This means that the higher their age, the more they are concerned about the awareness of data collection through a PCE. This can be explained by the fact that the older generation does not yet know what all the possibilities are for collecting data from retail companies.

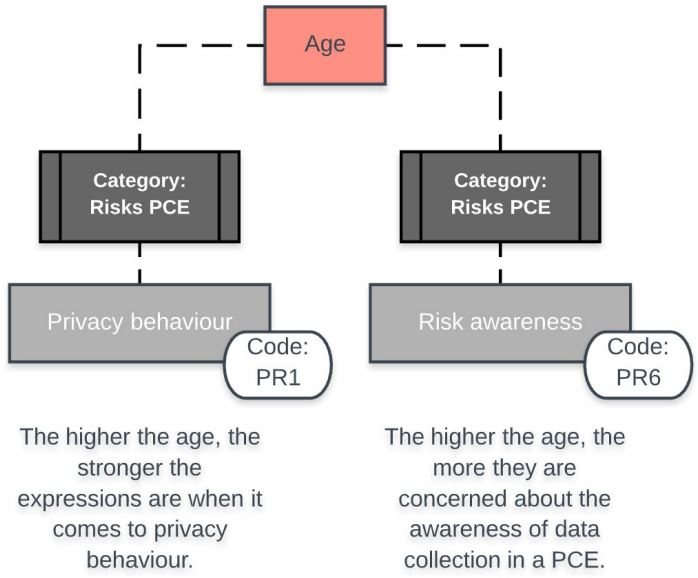


Figure 9. Connections between factors and age

Based on these results in this chapter, insight has been gained into which main categories were addressed in the analysis of the focus group sessions. These categories were further described by using the codes that were related to these categories. In order to link these results to the sub-questions and the central research question of this study, the conclusion is given in the next chapter.

5 Discussion

This section discusses the results. First, the sub-questions of this research are answered. Secondly, the practical and theoretical implications are discussed. Additionally, future recommendations are given. Finally, the limitations of this research are discussed and a conclusion is drawn.

5.1 Discussion of results

The central research question of this study was: "What are the critical principles and requirements of a Personal Consumer Environment (PCE) in retail that are expected to contribute to consumer acceptance? To answer this central research question, the sub-questions of this study will be answered first. The combination of these questions has contributed to the complete picture of the answer.

Sub-question 1: *To what extent do consumers experience a feeling of control over their retail data?*

As this study has identified, consumers currently do not feel in control of the data collected by retail companies with an online presence. Although the participants in this study do not experience a feeling of control, it can be confirmed that the need to have control over this retail data does exist. This also affects the small group of participants who have minimal control over their retail data. These participants also do not experience enough control over their retail data. The fact that many participants have no feeling of control over their retail data can be explained by the research of Morey et al. (2015). This research confirms that most companies want to keep control over their own data. Because companies keep control over retail data themselves, it is impossible for consumers to experience the feeling of control. As a result, consumer needs are misinterpreted (Turow, Hennessy, & Draper, 2015).

To support the specific need for more control over retail data, the example of a PHR was also discussed during this study. This is to gain insight into whether the need for control differs between a PHR and a PCE. Also to make a representation of the need. In this study it can be concluded that the need to have control over retail is higher than the need to have control over medical data. However, according to participants, the sensitivity of medical data is higher. This strong need for control is also reflected in previous studies. The study by Shore and Steinman (2015) confirms that when it comes to privacy and data protection mechanisms, consumers want to have control. Unfortunately, the processing of all the information involved is often far too complex for the average individual (Whittington & Hoofnagle, 2012). In addition, there is an exception for a few participants who consider control over medical data and retail data to be equally important.

Apart from the fact that exploratory research into a PCE has shown that the need for control is high, there have also been participants who have not explicitly thought about it. Participants confirmed that they were not aware of the consequences and effect of the collected retail data. According to these participants, the development of a PCE can provide tools that will increase their control over this retail data, if awareness is created.

Based on previous studies (Turow, Hennessy, & Draper, 2015; Whittington & Hoofnagle, 2012) it is also confirmed that individuals are aware of commercial monitoring in general. At the same time, it is confirmed that individuals have a vague understanding of the interpretation of data collection, which affects an individual's attitude. This is also reflected in this exploratory research into the principles and requirements of a PCE.

Sub-question 2: *What do consumers currently know about data collection in the context of retail companies with an online presence?*

The major finding of this research has shown that participants had knowledge of online data collection. Some participants had knowledge about the GDPR and their rights as consumers. However, in most situations participants had no knowledge about the next steps in creating control over their retail data. In confirmation of this result, research by Jensen, Potts, and Jensen (2005) shows that a large proportion of people claim to have knowledge about data collection. However, when this knowledge needs to be converted into actions, such as protecting your privacy, the knowledge is far less. As a result, it can be concluded that the current consumer knowledge about data collection at the retail level is superficial, but creates enough distrust. The distrust manifested in fear and irritation among participants, which can also be confirmed by the research of Solove and Citron (2018).

Also, concerning a PCE, this research has gained insight into consumers' knowledge of retail data. Participants were able to identify various ways in which data could be collected by retail companies with an online presence. In addition to the literature containing information on the different levels and sensitivity of the data, this study has shown that consumers do experience a significant difference between the data collected in the medical sector and the data from retail companies. Confirming this result, recent research by Milne, Pettinico, Hajjat, and Markos (2016) revealed that the general sensitivity of consumers concerning the information of different clusters differs but strongly emerges.

Sub-question 3: *To what extent do factors of UTAUT2 influence the intention to use a Personal Consumer Environment?*

This study has shown that some factors, based on UTAUT2, will contribute to the acceptance of a PCE. In this context, technology and the use of the internet are important drivers. The results showed that Performance Expectancy, Effort Expectancy, Social Influence, Facilitating Conditions

and Price Value are determining factors for the acceptance of a PCE. As had already been recognized by the previous model of UTAUT, Performance Expectancy, Effort Expectancy, Social Influence, Facilitating Conditions have a positive influence on the acceptance of a new technology (Venkatesh et al., 2003). In recent research, it has been further confirmed that Social Influence, in particular, is a positive predictor (Aswani, Ilavarasan, Kar, & Vijayan, 2018). Furthermore, this exploratory study confirms that the additional factor of UTAUT2, Price Value, is a strong predictor of the intention to use a PCE. Recent research by Blakesley and Yallop (2019) has already confirmed that Price Value is a strong predictor. The study by Blakesley and Yallop (2019) confirms that consumers were extrinsically motivated to share retail data if there was a financial reward or benefit in return. The demographic factor age has also been addressed in this research as a possible predictor for the acceptance of a PCE, based on the correlation analysis. However, the Hedonic Motivation factor was, as expected, not addressed as a determining factor for a PCE. The Habit factor was also not addressed because many participants do not yet make habits to protect their privacy.

Sub-question 4: *What is the effect of trust and privacy on the consumers' intention to use a Personal Consumer Environment?*

Finally, this study has shown that trust and privacy are important factors in the acceptance to use a PCE. According to many participants it was confirmed that trust is one of the important key factors in using a PCE. Not only trust in a product, but also trust in the organization. Previous studies (Gu, Lee & Suh, 2009; Mukherjee & Nath, 2007; Pavlou, 2003) also confirmed that trust influences the intention to use a technology.

Furthermore, as a result of this research, the topic of privacy was addressed as a determining factor for the acceptance of a PCE. Many participants were unaware of the effect of retail collection on their privacy. Various risks with regard to data collection were identified. Therefore, the protection of privacy determines the use of retail data by retail companies. Research by Raschke, Krishen, and Kachroo (2014) also shows that consumers are concerned about the privacy of information collected where this information is used improperly or where it is misrepresented.

Lastly, regarding the subject of privacy, privacy fatigue was pronounced in the discussion about a PCE. Privacy fatigue can be a risk for the use of a PCE. Because the consumer needs to understand that he must protect his data. Previously, privacy concerns have been shown to have a significant impact on the tendency to protect personal information from various online contexts (Dinev and Hart, 2006; Taddicken, 2013).

Central research question: *What are the principles and requirements of a Personal Consumer Environment (PCE) in retail that are expected to contribute to consumer acceptance?*

As the answers above have made clear, it can be concluded that there is a strong need for control over retail data. The majority of consumers have basic knowledge about the collection and types of retail data. Based on these insights, needs and knowledge have been identified in this study for principles and requirements. As a result of this exploratory study, it can be concluded that a total of thirteen principles and requirements may influence the intention to use a PCE. Within these thirteen factors, the factors of UTAUT2 play an important role, with the exception of Habit and Hedonic Motivation. In addition, the factors trust and privacy were discussed in all focus groups in order to be addressed as requirements. Finally, based on the additional results of this research, it can be confirmed that the participant's attitude towards retail data can also influence the intention to use a PCE.

5.2 Implications

5.2.1 Theoretical implications

This research has addressed several requirements that have contributed to the further development of theories on the acceptance of a new digital environment. By investigating the knowledge and needs of consumers, this has provided new insights.

First of all, this research has contributed to the literature by gaining insight into the extent to which the new requirements of a PCE deviate from or complement the current acceptance models, such as UTAUT2. For example, this research confirmed that all predictors of UTAUT 2, except Habit and Hedonic Motivation, influence the intention to use a new digital environment in the context of retail data. It can also be confirmed that this is certainly true among consumers, where UTAUT2 emphasizes on compared to other adoption models. Furthermore, the demographic factor 'age' plays an important role in the results of this research related to controlling the data.

Secondly, this research has provided new potential relationships between the categories discussed in the analysis of the focus groups. The qualitative approach of this research gave the participants the opportunity to illustrate the principles and requirements. In the process, the need for control had a strong influence on the consumer's attitude towards this data management. Subsequently, the consumer's attitude can indicate the extent to which risks or drawbacks have been identified. The risks and drawbacks can be used to fulfill the principles and requirements. This means that a risk can be limited when they are interpreted as a requirement for a PCE.

Thirdly, this research has contributed to the understanding of trust and privacy, in addition to confirming the current factors derived from the acceptance models. As the literature has already shown, factors such as trust and privacy are essential when collecting retail data from consumers. This means that these additional factors are unmistakable for the acceptance of a new digital environment in this context. Especially privacy fatigue, which is emerging in this period of digital

landscapes, is a factor on which more literature can be developed to respond to this problem. This research has, for example, provided insight into the initial starting points for the literature.

Fourthly, this research has gained new insights into the use of results from a different context. By taking the medical sector as an example to gain insight into the factors of a digital environment, it has provided insight into the extent to which consumers experience differences in confidence and degree of control in the medical and retail sectors. Furthermore, additional literature has been collected that the confidence of the medical sector is higher among consumers, but the need for control of his or her data is much lower. This can provide a starting point for the literature to further investigate the degree of control and trust among individuals in different sectors.

Finally, one of the most important additions is that the literature can be complemented with knowledge about the need and degree of consumer control over retail data. As discussed earlier in chapter two, there is hardly any scientific literature on this new need and knowledge of the consumer about data collection. This research provides a framework for gaining insight into the changing world of digital footprints from a consumer perspective. In the process, a boundary is crossed where research has been done from the perspective of the consumer rather than from the perspective of the retail companies.

5.2.2 Practical implications

In addition to the theoretical implications, this study also presents some practical implications that can be translated to situations within the field of work.

The most important translation that can be made into practice is that the principles and requirements function as a basis for developing a new product or service in the market. The needs of the consumer can be central to this. As an example, it can be developed in an application form in which the consumer manages his retail data. The principles and requirements can be reflected in the functionality and reliability of this environment. Another possibility is that it can become a plug-in on the websites of retail companies where the consumer takes decisions, insights and actions on the spot to manage the data of the consumer. An example concept in which many of these factors could be addressed, to regain consumer confidence in retail companies, is shown in Appendix J.

Secondly, this research can give retail companies or partners insight into how they can regain consumer confidence and commitment in general. This can be done by placing control with the consumer and being transparent about the data that is collected about the consumer. It can also have a positive effect on consumers if the factors discussed within a PCE are taken into account.

Thirdly, which is closely related to the suggestion above, is that this research can provide new insights for companies that want to keep up with the new and emerging trends. Some articles

suggest ideas that correspond to changing the role in responsibility of marketers and consumers. This research can provide guidance and confirmation to companies as to what the effects and needs are for consumers.

Fourthly, this research can provide companies with insight into consumer attitudes towards data collection. These behaviours, such as curiosity or irritation, can be used to be more efficient as an organisation by setting marketing goals. These goals can contribute by stimulating or limiting this behaviour. Since the subject 'cookie statements' has already been discussed several times, attention can be focused on the design of these statements. For example, by sharpening the documentation and explaining what they are intended for. However, because the attitude of the consumer was an additional result and was not the core of this research, follow-up research is recommended.

Finally, apart from the results, the design of this research method can be used to obtain a better understanding of consumers. This research has confirmed that focus group sessions have a positive effect on consumers, where strong insight can be generated for an exploratory study. The framework of these sessions could be used for additional research within consumer-centric organisations. Furthermore, this framework can contribute to gaining insight into the consumer's way of thinking. However, the timing and questions will have to be refined depending on the subject of the research.

5.3 Future research

Based on the theoretical and practical implications, several recommendations can be formulated for follow-up research into the need for consumer control in the field of retail data. As a result, a number of aspects have become clear that can contribute to strengthening this research, separately and linked to the limitations.

The most important first steps that can be taken after this research is to recommend a quantitative approach for further research. Emphasis should be placed on validating the thirteen different principles and requirements. Basis of this research, a first step has been taken to focus on consumer needs. The design of research that could fit in well with the verification of the principles and requirements is card sorting. The reason card sorting is recommended is that it can provide a concise list that can be used as an additional confirmation for a PCE. As well as focus groups, this offers the opportunity for explanation and substantiation

A second recommendation for future research is that further analysis can be provided into consumers' attitudes towards the collection of retail data and the risks of controlling retail data. This is because these two categories (attitude and risks) were an additional result of this research. Because it has generated remarkably first insights, further research is recommended to explore this in more depth.

The third recommendation that follows is that further research can be done into the relationships between the different categories and codes. Based on this research, the arguments during the focus group sessions were analysed in a detailed representation of codes (Appendix I). By making these connections visible in, for example, the UTAUT2 model, an experiment can be set up as a result. In this way, insight can be gained into the extent to which the UTAUT2 model can be optimised based on a new digital environment with a focus on the digital footprint of the consumer.

The fourth recommendation for future research is that prototypes of a PCE can be developed based on the results obtained so far. As with the practical implications, these principles and requirements could be translated into an end product or service. By developing and testing a product or service in follow-up research, the imagination of an as yet unknown PCE can be better defined for the participants. In addition to the introduction video of a PHR, these concepts can also provide a better insight into what the research wants to focus on.

Finally, this study recommends that the focus group sessions should also be held with international consumers. Because this research was specifically tested with Dutch consumers, it cannot be guaranteed that the principles and requirements are the same for other international customers. The same structure and format could be used to generate insight into the extent to which these principles and requirements deviate from the needs of Dutch consumers. Again, instead of the qualitative method, it is possible to use the quantitative method in which a larger group of participants participate in an experiment or a card sorting method.

5.4 Limitations

This study includes some limitations that need to be addressed in future research. Some of these limitations relate to the research method. Other limitations are related to the result and the population.

The first important limitation of this research is related to the imagination of the participants. Employing this research an attempt is made to gain insight into a relatively new and not yet existing digital environment in which consumers have control over their own retail data. The participants were expected to imagine what was important to them for a PCE. For some participants, it was difficult to imagine what could be important to them and what the risks might be. This was because some participants asked for examples in order to participate more actively in the sessions.

The limitation of imagination corresponds to the research design in which an example context of the medical sector was used. Only a few other contexts in which a similar digital environment has been developed in which the degree of control between an individual and an organization have been reversed. Despite the differences between need and knowledge have been discussed in the retail and medical sector, it is essential to test the results from other sectors.

The third limitation concerns the research method. For this research, focus groups were deliberately chosen, because it is an effective method for collecting qualitative data within a new subject. Participants question each other, contradict each other and give arguments for their points of view. However, certain participants may have a strong power of persuasion, allowing others to keep their opinions more in the background. In this study, it has sometimes happened that one participant had a clear point of view, as a result of which other participants adopted this point of view. There is a chance, however, that these other participants would not have taken this position themselves if the same question had been asked separately.

Finally, the research was only conducted among Dutch consumers. This is because the customers of Adwise, retail companies, largely sell to Dutch consumers. A limitation of this study is that the external validity is lower because the extent to which conclusions were drawn cannot be generalized for all customers with whom Adwise cooperates. This is because Adwise to a small extent also has a portfolio of international retail companies with associated international customers. It cannot be determined whether the same principles and requirements for this international target group could affect the acceptance of a PCE. For this reason, other countries may also have different rules and laws regarding data collection.

5.5 Conclusion

The central research question of this study was: “What are the principles and requirements of a Personal Consumer Environment (PCE) in retail that are expected to contribute to consumer acceptance?” Based on the results, this research has gained insight into the knowledge and need for consumer control of retail data from retailers with an online presence. Based on these insights, this resulted in thirteen principles and requirements for the acceptance of a Personal Consumer Environment (PCE) in which consumers have control over their retail data. In addition to these results, relationships between categories and factors of this research have become visible. These results are useful for understanding the consumer's needs and mindset. Furthermore, the risks involved in controlling retail data have also been identified. These risks must also be considered in the development of a PCE. To conclude, this means that a first step has been taken to put the consumer at the centre of the emerging topic of digital consumer footprints.

References

Acquisti, A., Friedman, A., & Telang, R. (2006). Is there a cost to privacy breaches? An event study. *ICIS 2006 Proceedings*, 94.

Aswani, R., Ilavarasan, P. V., Kar, A. K., & Vijayan, S. (2018). Adoption of public WiFi using UTAUT2: An exploration in an emerging economy. *Procedia Computer Science*, *132*, 297–306. https://doi.org/10.1016/j.procs.2018.05.180

Autoriteit Persoonsgegevens. (2018). Medische gegevens gebruiken en delen. Retrieved September 16, 2019, from https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/gezondheid/medische-gegevens-gebruiken-en-delen

Blakesley, I. R., & Yallop, A. C. (2019). What do you know about me? Digital privacy and online data sharing in the UK insurance sector. *Journal of Information, Communication and Ethics in Society*, *ahead-of*(ahead-of-print). https://doi.org/10.1108/jices-04-2019-0046

Boeije, H. (2009). *Analysis in Qualitative Research* (1st ed.). Thousand Oaks, Californië: Sage Publications Ltd.

Caligtan, C. A., & Dykes, P. C. (2011). Electronic health records and personal health records. *Seminars in Oncology Nursing*, *27*(3), 218–228. https://doi.org/10.1016/j.soncn.2011.04.007

Cattaneo, L. B., & Chapman, A. R. (2010). The process of empowerment: A model for use in research and practice. *American Psychologist*, *65*(7), 646–659. https://doi.org/10.1037/a0018854

Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*, *81*, 42–51. https://doi.org/10.1016/j.chb.2017.12.001

Christl, W. (2017). *Corporate surveillance in everyday life: How companies collect, combine, analyze, trade, and use personal data on billions*. Retrieved from https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf

Cicchetti, D. V. (1994). Guidelines, criteria, and rules of thumb for evaluating normed and standardized assessment instruments in psychology. *Psychological Assessment*, *6*(4), 284–290. https://doi.org/10.1037/1040-3590.6.4.284

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science*, *35*(8), 982–1003. https://doi.org/10.1287/mnsc.35.8.982

Delgado-Ballester, E., & Luis Munuera-Alemán, J. (2001). Brand trust in the context of consumer loyalty. *European Journal of Marketing*, *35*(11/12), 1238–1258. https://doi.org/10.1108/eum0000000006475

Dinev, T., & Hart, P. (2005). Internet privacy concerns and social awareness as determinants of intention to transact. *International Journal of Electronic Commerce*, *10*(2), 7–29. https://doi.org/10.2753/JEC1086-4415100201

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, *17*(1), 61–80. https://doi.org/10.1287/isre.1060.0080

European Commission. (2015). *Data protection* (Special Eurobarometer 431). Retrieved from http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_sum_en.pdf

Fishbein, M., & Ajzen, I. (1977). Belief, attitude, intention, and behavior: An introduction to theory and research. *Journal of Business Venturing*, *5*, 177–189.

Fulmer, C. A., & Gelfand, M. J. (2012). At what level (and in whom) we trust. *Journal of Management*, *38*(4), 1167–1230. https://doi.org/10.1177/0149206312439327

Gallino, S., & Moreno, A. (2014). Integration of online and offline channels in retail: The impact of sharing reliable inventory availability information. *Management Science*, *60*(6), 1434–1451. https://doi.org/10.1287/mnsc.2014.1951

Girardin, F., Calabrese, F., Fiore, F., Ratti, C., & Blat, J. (2008). Digital footprinting: Uncovering tourists with user-generated content. *IEEE Pervasive Computing*, *7*(4), 36–43. https://doi.org/10.1109/MPRV.2008.71

Grabner-Kraeuter, S. (2002). The role of consumers' trust in online-shopping. *Journal of Business Ethics*, *39*(1/2), 43–50. https://doi.org/10.1023/a:1016323815802

Graeff, T. R., & Harmon, S. (2002). Collecting and using personal data: consumers' awareness and concerns. *Journal of Consumer Marketing*, *19*(4), 302–318. https://doi.org/10.1108/07363760210433627

Groot, A. (2014, March 14). Business: Privacy is de nieuwe USP - Emerce. Retrieved June 1, 2019, from https://www.emerce.nl/nieuws/privacy-nieuwe-usp

Gu, J. C., Lee, S. C., & Suh, Y. H. (2009). Determinants of behavioral intention to mobile banking. *Expert Systems with Applications*, *36*(9), 11605–11616. https://doi.org/10.1016/j.eswa.2009.03.024

Heerink, M., Kröse, B., Evers, V., & Wielinga, B. (2010). Assessing acceptance of assistive social agent technology by older adults: The almere model. *International Journal of Social Robotics*, *2*(4), 361–375. https://doi.org/10.1007/s12369-010-0068-5

Higgins, E. T. (2006). Value from hedonic experience and engagement. *Psychological Review*, *113*(3), 439–460. https://doi.org/10.1037/0033-295x.113.3.439

Jain, P., Gyanchandani, M., & Khare, N. (2016). Big data privacy: A technological perspective and review. *Journal of Big Data*, *3*(1). https://doi.org/10.1186/s40537-016-0059-y

Janssen, M., & Kuk, G. (2016). The challenges and limits of big data algorithms in technocratic governance. *Government Information Quarterly*, *33*(3), 371–377. https://doi.org/10.1016/j.giq.2016.08.011

Janssen, M., & van den Hoven, J. (2015). Big and open linked data (BOLD) in government: A challenge to transparency and privacy? *Government Information Quarterly*, *32*(4), 363–368. https://doi.org/10.1016/j.giq.2015.11.007

Jensen, C., Potts, C., & Jensen, C. (2005). Privacy practices of Internet users: Self-reports versus observed behavior. *International Journal of Human-Computer Studies*, *63*(1–2), 203–227. https://doi.org/10.1016/j.ijhcs.2005.04.019

Kamleitner B., Mitchell VW. (2018) *Can Consumers Experience Ownership for Their Personal Data? From Issues of Scope and Invisibility to Agents Handling Our Digital Blueprints.* In: Peck J., Shu S. (eds) Psychological Ownership and Consumer Behavior. Springer, Cham

Keith, M. J., Maynes, C., Lowry, P. B., & Babb, J. (2014, December). Privacy fatigue: The effect of privacy control complexity on consumer electronic information disclosure. In *International Conference on Information Systems (ICIS 2014), Auckland, New Zealand, December* (pp. 14-17).

King, N. J., & Forder, J. (2016). Data analytics and consumer profiling: Finding appropriate privacy principles for discovered data. *Computer Law & Security Review*, *32*(5), 696–714. https://doi.org/10.1016/j.clsr.2016.05.002

Koufaris, M., & Hampton-Sosa, W. (2004). The development of initial trust in an online company by new customers. *Information & Management*, *41*(3), 377–397. https://doi.org/10.1016/j.im.2003.08.004

Labrecque, L. I., vor dem Esche, J., Mathwick, C., Novak, T. P., & Hofacker, C. F. (2013). Consumer power: Evolution in the digital age. *Journal of Interactive Marketing*, *27*(4), 257–269. https://doi.org/10.1016/j.intmar.2013.09.002

Levav, J., Heitmann, M., Herrmann, A., & Iyengar, S. S. (2010). Order in product customization decisions: Evidence from field experiments. *Journal of Political Economy*, *118*(2), 274–299. https://doi.org/10.1086/652463

Logue, M. D., & Effken, J. A. (2012). Modeling factors that influence personal health records adoption. *CIN: Computers, Informatics, Nursing*, *30*(7), 1. https://doi.org/10.1097/NXN.0b013e3182510717

Matz, S. C., & Netzer, O. (2017). Using big data as a window into consumers' psychology. *Current Opinion in Behavioral Sciences*, *18*, 7–12. https://doi.org/10.1016/j.cobeha.2017.05.009

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review*, *20*(3), 709–734. https://doi.org/10.5465/amr.1995.9508080335

Milne, G. R., Pettinico, G., Hajjat, F. M., & Markos, E. (2016). Information sensitivity typology: Mapping the degree and type of risk consumers perceive in personal data sharing. *Journal of Consumer Affairs*, *51*(1), 133–161. https://doi.org/10.1111/joca.12111

Morey, T., Forbath, T., & Schoop, A. (2015). Customer data: Designing for transparency and trust. *Harvard Business Review*, *93*(5), 96–105.

Morgan, R. M., & Hunt, S. D. (1994). The commitment-trust theory of relationship marketing. *Journal of Marketing*, *58*(3), 20–38. https://doi.org/10.1177/002224299405800302

Mukherjee, A., & Nath, P. (2007). Role of electronic trust in online retailing. *European Journal of Marketing*, *41*(9/10), 1173–1202. https://doi.org/10.1108/03090560710773390

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, *41*(1), 100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

NOS. (2018, November 24). Duizenden klachten en tips in eerste halfjaar nieuwe privacywet. Retrieved June 11, 2019, from https://nos.nl/artikel/2260557-duizenden-klachten-en-tips-in-eerste-halfjaar-nieuwe-privacywet.html

Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce*, *7*(3), 101–134. https://doi.org/10.1080/10864415.2003.11044275

Pearson, S. (2013). Privacy, security and trust in cloud computing. In *Privacy and security for cloud computing* (pp. 3-42). Springer, London.

Pierce, J. L., Kostova, T., & Dirks, K. T. (2003). The state of psychological ownership: Integrating and extending a century of research. *Review of General Psychology*, *7*(1), 84–107.

Raschke, R. L., Krishen, A. S., & Kachroo, P. (2014). Understanding the components of information privacy threats for location-based services. *Journal of Information Systems*, *28*(1), 227–242. https://doi.org/10.2308/isys-50696

Schermer, B., Hagenauw, D., & Falot, N. (2018). Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming. *Ministerie van Justitie En Veiligheid*, 9–98.

Senor, I. C., Aleman, J. L. F., & Toval, A. (2012). Personal health records: New means to safely handle health data? *Institute of Electrical and Electronics Engineers [IEEE] Computer Society*, *45*(11), 27–33. https://doi.org/10.1109/MC.2012.285

Shankar, V. (2019). Big data and analytics in retailing. *NIM Marketing Intelligence Review*, *11*(1), 36–40. https://doi.org/10.2478/nimmir-2019-0006

Shore , J., & Steinman, J. (2015). Did you really agree to that? The evolution of Facebook's privacy policy. *Technology Science*, *2015081102*. Retrieved from https://techscience.org/a/2015081102/download.pdf

Showell, C. (2017). Barriers to the use of personal health records by patients: a structured review. *PeerJ*, *5*, e3268.

Solove, D. J., & Citron, D. K. (2018). Risk and anxiety: A theory of data breach harms. *SSRN Electronic Journal*, *96*(737), 738–785. https://doi.org/10.2139/ssrn.2885638

Taddicken, M. (2013). The 'privacy paradox' in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *Journal of Computer-Mediated Communication*, *19*(2), 248–273. https://doi.org/10.1111/jcc4.12052

Tang, P. C., Ash, J. S., Bates, D. W., Overhage, J. M., & Sands, D. Z. (2006). Personal health records: definitions, benefits, and strategies for overcoming barriers to adoption. *Journal of the American Medical Informatics Association*, *13*(2), 121–126. https://doi.org/10.1197/jamia.M2025

Turner, M., Kitchenham, B., Brereton, P., Charters, S., & Budgen, D. (2010). Does the technology acceptance model predict actual use? A systematic literature review. *Information and Software Technology*, *52*(5), 463–479. https://doi.org/10.1016/j.infsof.2009.11.005

Turow, J., & Hennessy, M. (2015). The tradeoff Fallacy: How marketers are misrepresenting American consumers and opening them up to exploitation. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2820060

van Ooijen, I., & Vrabec, H. U. (2018). Does the GDPR enhance consumers' control over personal data? An analysis from a behavioural perspective. *Journal of Consumer Policy*, *42*(1), 91–107. https://doi.org/10.1007/s10603-018-9399-7

Vance, B., Tomblin, B., Studney, J., & Coustasse, A. (2015). Benefits and barriers for adoption of Personal Health Records. *Business and Health Administration Association Annual Conference*, 1–16.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, *27*(3), 425. https://doi.org/10.2307/30036540

Venkatesh, V., Thong, J. Y., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *MIS Quarterly*, *36*(1), 157–178.

Vroom, V. H. (1964). *Work and Motivation*. New York, United States: John Wiley & Sons, Inc.

Warburg, B. (2016, November 15). How the blockchain will radically transform the economy [YouTube]. Retrieved June 1, 2019, from https://www.ted.com/talks/bettina_warburg_how_the_blockchain_will_radically_transform_the_economy

Whittington, J., & Hoofnagle, C. J. (2012). Unpacking Privacy's Price. *North Carolina Law Review*, *90*(5), 1328–1368.

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems*, *12*(12), 1.

Yao, W., Chu, C. H., & Li, Z. (2010). The use of RFID in healthcare: Benefits and barriers. *IEEE International Conference on RFID-Technology and Applications*, 128–134. https://doi.org/10.1109/RFID-TA.2010.5529874

Zhang, S., Zhao, L., Lu, Y., & Yang, J. (2016). Do you get tired of socializing? An empirical explanation of discontinuous usage behaviour in social network services. *Information & Management*, *53*(7), 904–914. https://doi.org/10.1016/j.im.2016.03.006

Appendices

Appendix A: Pre-test schedule (NL)

Time	Script	Materiaal	Thema

10 min.	Aanvangst
	- Korte introductie wie ik ben
	- Kort voorstelrondje van de groep
	- Context beschrijving
	  - We zijn hier omdat (...)
	- Doel van het onderzoek
	  - Het doel van dit onderzoek is om principes en richtlijnen in kaart te brengen middels een focusgroep sessie.
	  - Hierbij ligt de focus op een digitale omgeving waarbij je controle hebt over je eigen gegevens.
	- Geïnformeerde toestemming
	  - De resultaten van dit onderzoek zullen geheel anoniem zijn.
	  - Papieren tekenen
		✓ Beeldscherm
		✓ Koffie/thee
		✓ Toestemmings formulier
			Introductie

Feedback onderdeel aanvangst: Papieren voor geïnformeerde toestemming klaarleggen, geeft een duidelijk beeld waar ik mensen wil hebben zitten. Papieren lezen en onderteken kan langer duren dan gepland.			

5 min.	Introductie focusgroep
	- Uitleg focusgroep
	  - Een focusgroep is opgezet om met elkaar in discussie te gaan. Hierbij zijn jullie 1 van de meerdere focusgroepen. In totaal zullen er 5 sessies plaats vinden.
	- Uitleg type vragen/topics
	  - Daarbij gaan we het hebben over jullie kennis en hoe een digitale omgeving eruit zou kunnen zien.
	- Vervolgstappen
	  - Na deze focusgroep sessie zal de
		✓ Beeldscherm
		✓ Camera
			Onderzoek

	data worden geanalyseerd en zullen de principes en richtlijnen in kaart worden gebracht. - Tijdsindicatie geven - De sessie zal ongeveer een 1 uur en 15 minuten duren. Zodra het einde naderd, zal ik hier een signaal voor worden gegeven.		
Feedback onderdeel introductie: Lukt binnen de tijd. Tevens vermelden dat vanaf dit moment een camera wordt aangezet.			
10 min.	Start focus group - Topic 1 Om te beginnen, starten we met het eerste topic: kennisniveau - Zijn er mensen bekend met het elektronisch patiëntendossier? - Wat weten jullie over het elektronisch patiëntendossier? - Weten jullie hoe de data wordt verzameld in een elektronisch patiëntendossier? - Weten jullie hoe bedrijven/winkels data verzamelen?	✓ Beeldscherm ✓ Camera	Topic 1: Kennisniveau
Feedback onderdeel kennisniveau: Onderwerp werd goed opgepakt door de groep. Eerste discussies kwamen hier op gang. Voldoende tijd voor dit onderdeel.			
10 min	Start focus group - Topic 2 ➡ *Start video over Elektronisch patiëntendossier (EPD)* *(Bruggetje: EPD > PCO)* - Hoe belangrijk vind je dat je controle hebt over deze gegevens (van de video)? - Hoe belangrijk vind je het om controle te hebben over andere gegevens? (Die bijvoorbeeld	✓ Beeldscherm ✓ Camera ✓ Video: https://www.youtube.com/watch?v=0LmGW4ig2Ys	Topic 2: Behoefte

	winkels verzamelen) - Heb je het gevoel dat je al controle hebt over deze gegevens? - Ervaar je een verschil tussen gegevens die afkomstig zijn van o.a ziekenhuizen en winkels?		
Feedback onderdeel behoefte: Video gaf herkenning en een duidelijk beeld bij de deelnemers. Echter, was er meer tijd nodig voor dit onderdeel om ervoor te zorgen dat iedereen de kennis kan vergaren. + 5 min voor dit onderdeel was er nodig.			
20 min	Start focus group - Topic 3 We hebben het zojuist gehad over het elektronisch patiëntendossier. Met dit onderzoek focus ik mij op een soortgelijke digitale omgeving waarin jij als consument controle kan hebt over je eigen gegevens, afkomstig van winkels. - Hoe zou zoiets eruit moeten zien? - Aan welke eisen zou deze digitale omgeving moeten voldoen? - Wat zijn de nadelen of risico's van deze omgeving *Wanneer vragen moeilijk te beantwoorden zijn, kan er richting worden gegevens middels de volgende factoren:* (UTAUT factoren) - Prestatieverwachting - Gebruiksgemak - Sociale omgeving - Faciliterende middelen/ benodigde middelen - Plezier - Kosten - Gewoonte patroon (Aanvullende factoren)	✓ Beeldscherm ✓ Camera ✓ Post-its (rood) ✓ Post-its (groen) ✓ Pennen	Topic 3: Principes en richtlijnen

	- Privacy (algemeen) - Vertrouwen - Risico's - Privacy moeheid		
Feedback onderdeel principes en richtlijnen: Door de kennis die hiervoor gedeeld is, kwam dit onderwerp snel op gang. Er was weinig sturing nodig om de factoren in kaart te brengen. + 5 min nodig voor toelichting van de opgeschreven factoren op de post-its. Input van een UX/CRO specialist middels de vraag '*Als je kijkt naar het overzicht, zou je hier nog iets aan willen toevoegen ?*' werkte goed. Er kwam nog een aantal punten binnen. Deze vraag aanvullen bij het schema.			
10 min.	Beëindiging - Signaal einde - Dankwoord		Afsluiting
Feedback onderdeel beëindiging: het afronden verliep erg snel en soepel. Hier was niet meer dan 5 minuten voor nodig. - 5 min voor dit onderdeel.			
15 min.	*Eventuele uitloop*	*Eventuele uitloop*	*Eventuele uitloop*

Algemene feedback/ punten waarop gelet moet worden:

- Duidelijk aangeven wie het gesprek zal gaan leiden.
- Aangeven dat er geen verkeerde antwoorden gegeven kunnen worden.
- Wanneer het voor sommige deelnemers moeilijk is om principes en richtlijnen in kaart te brengen, kunnen er koppels worden gemaakt.
- Eindigen met een slot vraag: *Ik zal gebruik maken van een PCO als het voldoet aan/rekening gehouden wordt met …*
- Een positie achter de deelnemer nemen wanneer het gaat om een dominant iemand. Hierdoor kan er beter contact worden gemaakt met de andere deelnemers.

Appendix B.1: Focus group schedule (NL)

Tijd	Script	Materiaal	Thema

10 min.	Aanvangst
	- Korte introductie wie ik ben
	- Kort voorstelrondje van de groep
	- Context beschrijving
	  - We zijn hier omdat (...)
	- Doel van het onderzoek
	  - Het doel van dit onderzoek is om principes en richtlijnen in kaart te brengen middels een focusgroep sessie.
	  - Hierbij ligt de focus op een digitale omgeving waarbij je controle hebt over je eigen gegevens.
	- Geïnformeerde toestemming
	  - De resultaten van dit onderzoek zullen geheel anoniem zijn.
	  - Papieren tekenen
		✓ Beeldscherm
		✓ Koffie/thee
		✓ Toestemmings formulier
			Introductie

5 min.	Introductie focusgroep
	- Uitleg focusgroep
	  - Een focusgroep is opgezet om met elkaar in discussie te gaan. Hierbij zijn jullie 1 van de meerdere focusgroepen. In totaal zullen er 5 sessies plaats vinden.
	- Uitleg type vragen/topics
	  - Daarbij gaan we het hebben over jullie kennis en hoe een digitale omgeving eruit zou kunnen zien.
	- Vervolgstappen
	  - Na deze focusgroep sessie zal de data worden geanalyseerd en zullen de principes en richtlijnen in kaart worden gebracht.
		✓ Beeldscherm
		✓ Camera
			Onderzoek

	- Tijdsindicatie geven - De sessie zal ongeveer een 1 uur en 15 minuten duren. Zodra het einde naderd, zal ik hier een signaal voor worden gegeven.		
10 min.	Start focus group - Topic 1 Om te beginnen, starten we met het eerste topic: kennisniveau - Zijn er mensen bekend met het elektronisch patiëntendossier? - Wat weten jullie over het elektronisch patiëntendossier? - Weten jullie hoe de data wordt verzameld in een elektronisch patiëntendossier? - Weten jullie hoe bedrijven/winkels data verzamelen?	✓ Beeldscherm ✓ Camera	Topic 1: Kennisniveau

15 min.	Start focus group - Topic 2
	➜ *Start video over Elektronisch patiëntendossier (EPD)*
	
	(Bruggetje: EPD > PCO)
	
	- Hoe belangrijk vind je dat je controle hebt over deze gegevens (van de video)? *(score van 1 tot 10)*
	  - Hoe belangrijk vind je het om controle te hebben over andere gegevens? (Die bijvoorbeeld winkels verzamelen)
	  (score van 1 tot 10)
	
	- Heb je het gevoel dat je al controle hebt over deze gegevens?
	- Ervaar je een verschil tussen gegevens die afkomstig zijn van o.a ziekenhuizen
		✓ Beeldscherm
		✓ Camera
		✓ Video: https://www.youtube.com/watch?v=0LmGW4ig2Ys
			Topic 2: Behoefte

	en winkels?		
25 min.	Start focusgroep - Topic 3 We hebben het zojuist gehad over het elektronisch patiëntendossier. Met dit onderzoek focus ik mij op een soortgelijke digitale omgeving waarin jij als consument controle kan hebt over je eigen gegevens, afkomstig van winkels. - Hoe zou zoiets eruit moeten zien? - Aan welke eisen zou deze digitale omgeving moeten voldoen? (Groen) - Wat zijn de nadelen/risico's van deze omgeving? (Rood) *Wanneer vragen moeilijk te beantwoorden zijn, kan er richting worden gegevens middels de volgende factoren:* (UTAUT factoren) - Prestatieverwachting - Gebruiksgemak - Sociale omgeving - Faciliterende middelen/ benodigde middelen - Plezier - Kosten - Gewoonte patroon (Aanvullende factoren) - Privacy (algemeen) - Vertrouwen - Risico's - Privacy moeheid **Slot vraag:** Zoals jullie zien hebben we een overzicht gemaakt op het bord van principes en richtlijnen. Hebben jullie het gevoel dat we nog iets missen?	✓ Beeldscherm ✓ Camera ✓ Post-its (rood) ✓ Post-its (groen) ✓ Pennen	Topic 3: Principes en richtlijnen

5 min.	Beëindiging - Signaal einde - Dankwoord		Afsluiting
15 min.	*Eventuele uitloop*	*Eventuele uitloop*	*Eventuele uitloop*

Algemene feedback/ punten waarop gelet moet worden:

- Duidelijk aangeven wie het gesprek zal gaan leiden.
- Aangeven dat er geen verkeerde antwoorden gegeven kunnen worden.
- Wanneer het voor sommige deelnemers moeilijk is om principes en richtlijnen in kaart te brengen, kunnen er koppels worden gemaakt.
- Slot vraag: *Ik zal gebruik maken van een PCO als er rekening gehouden wordt met …*
- Een positie achter de deelnemer nemen wanneer het gaat om een dominant iemand. Hierdoor kan er beter contact worden gemaakt met de andere deelnemers.

Appendix B.2: Focus group schedule (EN)

Time	Script	Material	Topic

10 min.	Start
	- Brief introduction to who I am
	- Short introduction round of the group
	- Context description
	  - We're here because (...)
	- Purpose of the investigation
	  - The aim of this research is to map out principles and requirements by means of a focus group session.
	  - The focus is on a digital environment where you have control over your own data.
	- Informed consent
	  - The results of this research will be completely anonymous.
	  - Drawing papers
		✓ Screen
		✓ Coffee/tea
		✓ Consent form
			Introduction

5 min.	Introduction focus group
	- Explanation focus group
	  - A focus group has been set up for discussion. Here you are one of the several focus groups. In total there will be 5 sessions.
	- Explanation type of questions/topics
	  - We are going to talk about your knowledge and what a digital environment could look like.
	- Next steps
	  - After this focus group session the data will be analysed and the principles and requirements will be identified.
	- Indicating the time
	  - The session will last about 1 hour and 15 minutes. As soon as the
		✓ Screen
		✓ Camera
			Research

	end is approaching, I will be given a signal for this.		
10 min.	Start focus group - Topic 1 To start with, we begin with the first topic: knowledge level - Are any people familiar with the personal health record ? - What do you know about the personal health record? - Do you know how the data is collected in a personal health record? - Do you know how companies/shops collect data?	✓ Screen ✓ Camera	Topic 1: Knowledge level
15 min.	Start focus group - Topic 2 ➜ *Start video about Personal Health Record (PHR)* *(Bridge: PHR > PCE)* - How important do you think that you have control over this data (from the video)? (score from 1 to 10) - How important do you think it is to have control over other data? (For example, shops) (score from 1 to 10) - Do you feel like you already have control of this data? - Do you experience a difference between data coming from hospitals and shops?	✓ Screen ✓ Camera ✓ Video: https://www.youtube.com/watch?v=0LmGW4ig2Ys	Topic 2: Need
25 min.	Start focus group - Topic 3 We just talked about the personal health record. With this research I focus on a similar digital	✓ Screen ✓ Camera ✓ Post-its (rood) ✓ Post-its (groen)	Topic 3: Principles and requirement

	environment in which you, as a consumer, can have control over your own data, originating from shops. - What would that look like? - What requirements should this digital environment meet? (Green) - What are the drawbacks/risks of this environment? (Red) *When questions are difficult to answer, it is possible to provide more direction through the following factors:* (UTAUT factoren) - Performance expectancy - Effort Expectancy - Social Influence - Facilitating Conditions - Hedonic Motivation - Price Value - Habit (Additional factors) - Privacy (algemeen) - Trust - Risk - Privacy fatigue **Final question:** As you can see we have made an overview on the board of principles and requirements. Do you feel that we are missing something?	✓ Pencils	s
5 min.	Ending - End of signal - Acknowledgements		Closing
15 min.	*Space for additional time*	*Space for additional time*	*Space for additional time*

General feedback/ points to watch out for:

- Clearly indicate who will lead the conversation.
- Indicate that no wrong answers can be given.
- When it is difficult for some participants to identify principles and requirements, teams can be created.
- Final question: *I will make use of a PCE if …*
- Take a position behind the participant when it comes to a dominant person. This makes it easier to make contact with the other participants.

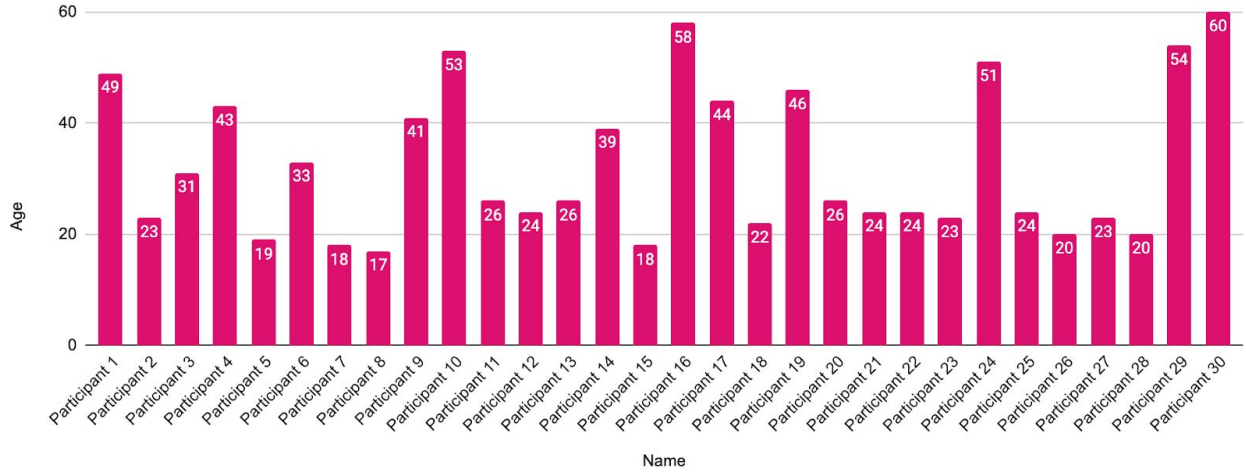
Appendix C: Survey demographic factors (NL)

Focus group: demografische vragen

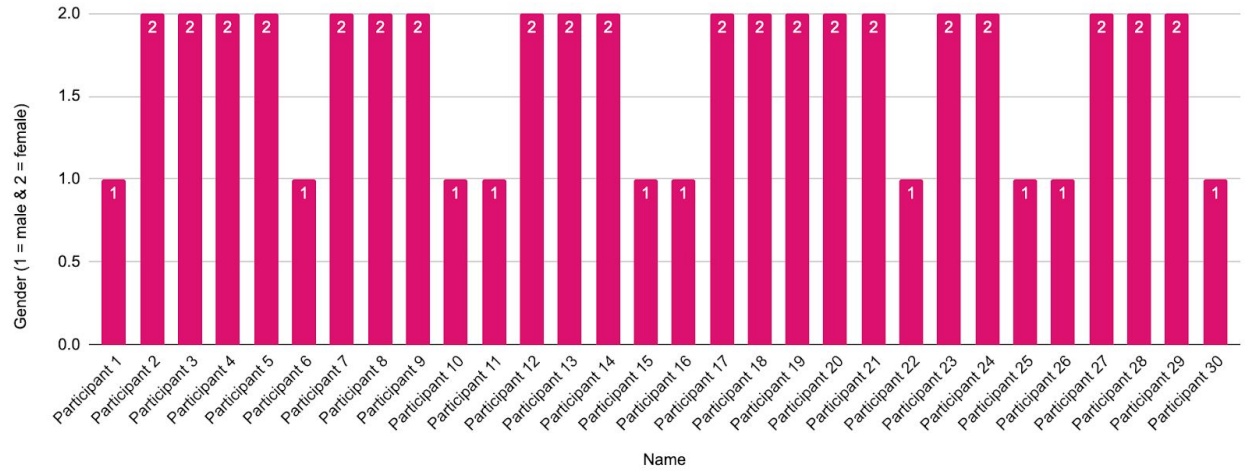
1. Wat is uw leeftijd?
   .....
2. Wat is uw geslacht?
   - Man
   - Vrouw
   - Zeg ik liever niet
3. Wat is uw hoogst genoten opleiding?
   - VMBO/MAVO
   - HAVO
   - VWO
   - HBO
   - WO
   - Zeg ik liever niet

Appendix D: Overview demographic factors

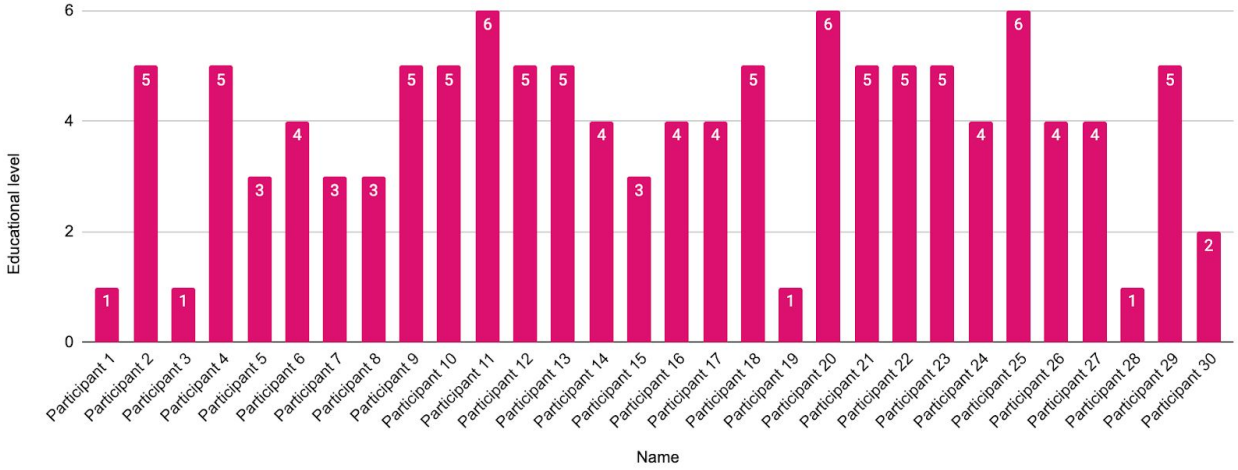
Demographic factor: Age



Demographic factor: Gender



Demographic factor: Education level



- 1 = Pre-vocational secondary education
- 2 = Senior general secondary education
- 3 = Pre-university education
- 4 = Secondary vocational education
- 5 = Higher professional education
- 6 = University education

Appendix E: Reliability analysis

Reliability analysis of a focus group session

Date: 26/11/2019
Sessie: 2

Citation	Encoder 1	Encoder 2	After consultation
1	K4	K4	-
2	K4	K1	K4
3	K2	K2	-
4	K2	K2	-
5	K2	K2	-
6	K1	K4	K4
7	K1	K1	-
8	K1	K1	-
9	K1	K1	-
10	K4	K4	-
11	K1	K1	-
12	K2	K2	-
13	K2	K2	-
14	K2	K2	-
15	K2	K2	-
16	K2	K2	-
17	K2	K2	-
18.1	K2	K2	-
18.2	A7	-	A7
19	K2	K2	-
20	A7	A7	-
21	A7	A7	-
22	K2	K2	-
23	PR2	PR1	PR2
24	PR2	PR2	-
25	PR3	PR3	-
26.1	PR1	PR3	PR3
26.2	R9	R9	-
27	R9	R9	-
28.1	PR1	-	Delete
28.2	PR3	PR3	-
28.3	P9	P9	-
29	L1	L1	-
30	L1	L1	-
31	L1	L1	-
32	A3	A3	-
33	L3	L6	L3
34	L3	L3	-
35	L1	L1	-
36	L2	L2	-
37	L2	L2	-
38	L2	L2	-
39	L4	L4	-
40	L2	L2	-
41	L2	L2	-
42	K3	K2	K2
43	K3	K3	-
44	A2	A2	-
45	K3	K3	-
46	K3	K3	-
47	K3	K3	-
48	K3	K3	-
49	L7	L6	-
50	L7	L7	-
51	L8	L8	-
52	A4	A4	-
53	L1	L7	L7
54	L5	L8	L8
55	L5	L5	-
56	K2	K2	-
57	A6	A6	-
58	R10	R10	-
59	R10	R10	-

Citation	Encoder 1	Encoder 2	After consultation
60	R10	R10	-
61	R10	R10	-
62	R2	R2	-
63.1	R2	R2	-
63.2	R3	R3	-
64	R10	R10	-
65	R2	R2	-
66	R8	R8	-
67	R8	R8	-
68	R8	R8	-
69	R8	R8	-
70.1	R1	R3	R1
70.2	R13	R13	-
71.1	R1	R1	-
71.2	R13	R13	-
72	R11	R11	-
73	R15	R15	-
74	R15	R15	-
75	R15	R15	-
76.1	R13	-	R13
76.2	R15	R15	-
77	R1	R1	-
78	R2	R2	-
79	R4	R4	-
80	R6	R6	-
81	R9	R1	R1
82	R15	R15	-
83	K5	K5	-
84	R11	R11	-
85	R11	R11	-
86	K2	K2	-
87	K2	K2	-
88	R3	R3	-
89	R14	R14	-
90	R14	R14	-
91	R14	R14	-
92	R14	R14	-
93	R7	R7	-
94	R7	R7	-
95	R8	R8	-
96	PR8	PR8	-
97	PR8	PR8	-
98	PR8	PR8	-
99	K2	K2	-
100	A7	A7	-
101	R3	R3	-
102	R9	PR3	PR3
103	A2	A2	-
104	R2	R2	-
105	R10	R2	R10
106.1	A6	A6	-
106.2	R8	R8	-
107	PR4	PR4	-
108	A6	A6	-
109	A6	A2	A2
110	A4	A2	A2
111	R8	R8	-
112	A6	A7	-

Appendix F.1: Codebook (NL)

Code	Naam	Beschrijving	Voorbeelden
Houding			
A1.	Nieuwsgierig gegevens verzamelen	Benieuwd hoe gegevens verzameld worden.	“Ik ben best wel nieuwsgierig.”
A2.	Wantrouwen gegevens verzamelen	Geen vertrouwen op de manier waarop gegevens verzameld worden.	“Ik zou niet zo veel vertrouwen erin hebben. Je weet het niet.”
A3.	Wantrouwen medische gegevens verzamelen	Geen vertrouwen op de manier waarop medische gegevens verzameld worden.	“Maar misschien weet hij veel meer dan wat in mijn dossier genoteerd staat.”
A4.	Wantrouwen retail gegevens verzamelen	Geen vertrouwen op de manier waarop retail gegevens verzameld worden.	“Gaan ze straks dan ook andere trucjes bedenken om er omheen te zeilen?”
A5.	Vertrouwen gegevens verzamelen	Het vertrouwen dat gegevens op de juiste manier verzameld worden.	“Het zal dan denk ik wel gewoon kloppen.”
A6.	Angst gebruik retail gegevens	Een angstig gevoel bij het idee dat retail gegevens gebruikt worden.	“Ze weten gewoon alles van je. Waar je bent, je pinpas. Ze weten echt alles.”
A7.	Bewustwording gegevens verzamelen	Gedachtegang over het verzamelen van gegevens.	“Ik was gewoon niet bewust dat alles wordt bekeken en in de gaten wordt gehouden.”
A8.	Irritatie gebruik retail gegevens	Gevoel van irritatie bij het gebruik van retail	“Ik vind het heel erg irritant. Als ik 1 keer ergens op kijk,

		gegevens.	zie je gelijk overal reclame erover.”

Kennis			
K1.	Data verzameling medische gegevens	Omschrijving hoe medische gegevens verzameld worden.	“Ik denk dat dat via een zorgverzekeraar gaat of via je huisarts.”
K2.	Data verzameling retail gegevens	Omschrijving hoe gegevens van bedrijven verzameld worden.	“Ik moet dan vooral denken aan de cookies om gegevens te verzamelen.”
K3.	Wetgeving	Omschrijving wat de regels zijn omtrent de wetgeving.	“Heel veel is er niet veranderd met de AVG. Hij is voornamelijk aangescherpt.”
K4.	Omschrijving elektronisch patiëntendossier	Omschrijving wat het elektronisch patiëntendossier inhoud.	“Volgens mij kan je informatie ophalen van een ander ziekenhuis.”
K5.	Omschrijving digitale omgeving	Omschrijving wat een digitale omgeving inhoud.	“Je mag zelf bepalen welke bedrijven je belangrijk vindt en zij mogen weten wat je leuk vindt.”

Mate van controle			
L1.	Wil controle medische gegevens	Mate waarin iemand controle wil over zijn medische gegevens.	“Ik vind dat dat heel belangrijk is die controle. Maar ik denk geen 10.”
L2.	Wil controle retail gegevens	Mate waarin iemand controle wil over de gegevens die bedrijven verzamelen.	“Wat je niet wil dat ze het mogen weten, mogen ze ook niet opslaan. Jij moet die controle hebben.”
L3.	Wil geen controle	Mate waarin iemand	“Als alleen de arts er naar

	medische gegevens	geen controle wil over zijn medische gegevens.	kan kijken, dan hoef ik die controle niet.”
L4.	Wil geen controle retail gegevens	Mate waarin iemand geen controle wil over gegevens die bedrijven verzamelen.	“Als ze mijn gegevens gebruiken om het assortiment te verbeteren, dan vind ik dat niet erg.”
L5.	Wil controle op alle gegevens	Mate waarin iemand controle wil over alle gegevens die over hem/haar verzameld worden.	“Ik vind alle soort gegevens wel privacygevoelig om dat zelf te beheren.”
L6.	Wil geen controle op gegevens	Mate waarin iemand geen controle wil over alle gegevens die over hem/maar verzameld worden.	“Ik vraag me af of ik perse meer grip zou willen hebben. Op cookies heb ik grip, maar ook daarin denk ik ‘ik snap het allemaal niet’ dus ik accepteer het maar.”
L7.	L7. Ervaren verschil in data	Ervaren het gevoel dat er een verschil zit in waarde van medische gegevens en gegevens die bedrijven verzamelen.	“Ik vind medisch wel belangrijker. Dat is meer privacy.”
L8	L8. Ervaren geen verschil in data	Ervaren geen gevoel dat er een verschil zit in waarde van medische gegevens en gegevens die bedrijven verzamelen.	“Ja maar medische gegevens zouden ook voor commerciële doeleinden kunnen worden gebruikt.”
L9.	L9. Niet nagedacht over controle gegevens	Niet bewust nagedacht over het hebben van grip op gegevens die over hem/haar verzameld worden.	“Ik heb er nog nooit over nagedacht. Ik wist niet eens dat ik een medisch dossier had.”

L10.	L10. Heeft geen controle op gegevens	Mate waarin iemand geen grip heeft over de verzamelde gegevens van hem/haar.	“Nee. Als ik schoenen heb gekocht, dan zie ik ze overal weer terug komen.”
L11.	Heeft controle op gegevens	Mate waarin iemand grip heeft over de verzamelde gegevens van hem/haar.	“Af en toe delete ik alle cookies die op mijn telefoon of laptop staan. Maar ja dat blijf ik constant doen.”

Privacy & Risico			
PR1.	Privacy gedrag	De mate waarin iemand gedrag vertoond dat gerelateerd is aan privacy.	“Volgens mij kijkt niemand ernaar. Ik druk gewoon op accepteren.”
PR2.1.	Privacy moeheid - aanwezig	De mate waarin iemand moe wordt over het nadenken over privacy.	“Het is meestal gemakzucht. Dan hoef ik even niet na te denken.”
PR2.2.	Privacy moeheid - afwezig	De mate waarin iemand niet moe wordt over het nadenken over privacy.	“Ik probeer de cookies wel altijd weg te klikken. En als dat niet werkt, dan vraag ik mezelf af hoe graag ik op die website wil zijn.”
PR3.	Risico - datalek	De mate waarin iemand het risico inziet van het lekken van verzamelde gegevens.	“Je hoort best vaak dat er een datalek is en dat al onze gegevens op straat liggen.”
PR4.	Risico - misbruik	De mate waarin iemand het risico inziet van het misbruiken van verzamelde gegevens.	“Ik ben alsnog bang dat je gegevens ergens voor worden gebruikt.”
PR5.	Risco - nut niet inzien	De mate waarin iemand het risico inziet van het het geen waarde	“Ik denk dat er ook mensen zijn die het prima vinden dat hun gegevens verzameld

		hebben van een digitale omgeving.	worden.”
PR6.	Risico - bewustwording	De mate waarin iemand het risico inziet van het bewust maken van gegevens verzamelen.	“Ik denk dat als je het onder de aandacht brengt dat veel mensen er over na gaan denken en angstig worden.”
PR7.	Personalisatie	De mate waarin iemand het risico inziet van een overkill aan personalisatie.	“Je hebt aangegeven wat je leuk vindt, waardoor je straks heel veel reclame krijgt.”

Richtlijnen			
R1.	Prestatieverwachting	Eis dat een digitale omgeving moet doen wat hij zou moeten doen. Verwijderen en aanpassingen van verzamelde gegevens.	“Het moet gewoon werken. Je gegevens moeten aanpasbaar en verwijderbaar zijn.”
R2.	Gebruikersgemak	Eis dat een digitale omgeving gebruiksvriendelijk is.	“Het moet gewoon gemakkelijk en gebruiksvriendelijk zijn en alles op één plek.”
R3.	Faciliterende omstandigheden	De mate waarin een individu ervaart dat objectieve factoren van invloed zijn om het gebruik te vergemakkelijken.	“Je moet wel meldingen krijgen om je erop te attenderen.”
R4.	Sociale omgeving	De mate waarin een individu ervaart dat het gebruik van anderen invloed heeft op het gebruik van een digitale omgeving.	“Ik denk dat de druk van je sociale omgeving daarbij wel kan helpen.”

R5.	Betrouwbaar	Eis dat een digitale omgeving betrouwbaar moet zijn.	“Ja, vertrouwen vind ik hierin heel erg belangrijk.”
R6.	Bewustwording	Eis dat een digitale omgeving bijdraagt aan de bewustwording van het verzamelen van gegevens.	“Ik denk dat het belangrijk is dat er herhaald wordt dat je overal gevolgd wordt.”
R7.	Kosten en baten	Eis dat een digitale omgeving iets moet opleveren voor de consument.	“Het moet ons uiteindelijk wel gewoon iets opleveren.”
R8.	Veiligheid	Eis dat een digitale omgeving veilig is in gebruik.	“Als je zorgt dat het veilig is, dan ga je risico’s inperken.”
R9.	Tijdsduur	Eis dat het gebruik van een digitale omgeving efficiënt in gebruik is.	“Ja dat kost ook gewoon heel veel tijd.”
R10.	Toegankelijkheid	Eis dat een digitale omgeving toegankelijk is voor verschillende doelgroepen.	“Het moet voor ons goed zijn, maar eigenlijk voor iedereen. Dus ook voor oudere mensen zoals ik.”
R11.	Persoonlijk	Eis dat een digitale omgeving aansluit bij je persoonlijkheden.	“Ik zou zelf graag een persoonlijke pagina willen.”
R12.	Centraal	Eis dat een digitale omgeving een centrale omgeving is voor dataverzameling.	“Ik zou graag willen dat het ergens centraal geregistreerd wordt.”
R13.	Controle	Eis dat een digitale omgeving de consument controle zal gaan geven.	“Dat je het gewoon zelf kan bepalen. Dat je iets meer keuzes hebt.”

Demografische factoren*			
D1.	Deelnemer	-	“Deelnemer 1”
D2.	Geslacht	-	“Vrouw”
D3.	Leeftijd	-	“23”
D4.	Opleidingsniveau	-	“HBO”

* Ingevuld middels een korte enquête omtrent de demografische factoren voorgaan aan de focusgroepsessie.

Appendix F.2: Codebook (EN)

Code	Naam	Beschrijving	Voorbeelden
Attitude			
A1.	Curious data collection	Wondering how data is collected.	"I'm kind of curious."
A2.	Distrust data collection	No trust in the way data is collected.	"I wouldn't have so much trust in it. You don't know."
A3.	Distrust in collecting medical data	No trust in the way medical data is collected.	"But maybe he knows a lot more than what's in my file."
A4.	Distrust retail data collection	No trust in the way retail data is collected.	"Are they going to come up with other tricks to hide behind words?"
A5.	Trust data collection	The confidence that data is collected correctly.	"I guess it'll just be right then."
A6.	Fear use retail data	A fearful feeling with the idea that retail data is being used.	"They just know everything about you. Where you are, your ATM card. They really know everything."
A7.	Awareness data collection	Thought about data collection.	"I just wasn't aware that everything was being watched and monitored."
A8.	Irritation use retail data	Feeling irritated when using retail data.	"I find it very irritating. When I look at something once, you immediately see commercials."

Knowledge			
K1.	Data collection medical data	Description of how medical data is collected.	"I think it's via a health insurance company or your family doctor."
K2.	Data collection retail data	Description of how data is collected from companies.	"I'm thinking about the cookies to collect data."
K3.	Legislation	Description of the rules of the legislation.	"A lot hasn't changed with the GDPR. It's mostly refined."
K4.	Description personal health record	Description of the contents of the personal health record.	"I think you can get information from another hospital."
K5.	Description digital environment	Description of what a digital environment contains.	"You get to decide which companies you care about and they get to know what you like."

Level of control			
L1.	Want control medical data	Degree to which someone wants control of their medical data.	“Ik vind dat dat heel belangrijk is die controle. Maar ik denk geen 10.”
L2.	Want control retail data	Degree to which someone wants control over the data that companies collect.	“Wat je niet wil dat ze het mogen weten, mogen ze ook niet opslaan. Jij moet die controle hebben.”
L3.	Does not want control of medical data	Degree to which someone doesn't want control of their medical data.	“Als alleen de arts er naar kan kijken, dan hoef ik die controle niet.”
L4.	Does not want control of retail data	Degree to which someone does not want	"If they use my information to improve the assortment, I

		control over data that companies collect.	don't mind."
L5.	Wants control of all data	Degree to which a person wants control over all data collected about him/her.	"I do find any kind of data sensitive to manage on my own."
L6.	Does not want control of all data	Degree to which a person does not want control over all the data that is collected about him/her.	"I wonder if I'd really like to have more control. I have a grip on cookies, but I think 'I don't get it all' so I accept it".
L7.	Experienced difference in data	Experience the feeling that there is a difference in value between medical data and data collected by companies.	"I think medical is more important. That's more privacy."
L8	Experienced no difference in data	Experience no sense of difference between the value of medical data and data collected by companies.	"Yes, but medical data could also be used for commercial purposes."
L9.	Not thought about control data	Not consciously thinking about having control over data that is collected about him/her.	"I've never thought about it. I didn't even know I had a medical record."
L10.	Has no control over data	Degree to which a person has no control over the data collected from him/her.	"No. If I bought shoes, I'll see them come back anywhere."
L11.	Has control over data	Degree to which a person has control over the data collected from him/her.	"Sometimes I delete all cookies that are on my phone or laptop. But I keep doing that all the time."

Privacy & Risk			
PR1.	Privacy behaviour	The extent to which a person engages in behaviour related to privacy.	"I don't think anyone's looking at it. I'm just pressing accept."
PR2.1.	Privacy fatigue - present	The degree to which someone gets tired of thinking about privacy.	"It's usually laziness. Then I don't have to think for a moment."
PR2.2.	Privacy fatigue - absent	The degree to which someone doesn't get tired of thinking about privacy.	"I always try to click away the cookies. And if that doesn't work, I ask myself how much I want to be on that website."
PR3.	Risk - data leaks	The extent to which someone understands the risk of leaking collected data.	"You hear quite often that there's a data leak and all our records are on the street."
PR4.	Risk - Abuse	The extent to which a person understands the risk of misuse of collected data.	"I'm still afraid your data will be used for something."
PR5.	Risk - don't see the point	The degree to which someone understands the risk of not enjoying a digital environment.	"I think there are some people who are fine with their data being collected."
PR6.	Risk - awareness	The degree to which a person understands the risks of raising awareness of data collection.	"I think if you bring it to your attention that a lot of people are going to think about it and get scared."
PR7.	Personalization	The degree to which someone understands the risk of an overkill of personalization.	"You've indicated what you like, so you'll get a lot of publicity later."

Principles & Requirements			
R1.	Performance expectancy	Demands that a digital environment should do what it's supposed to do. Delete and modify collected data.	"It just has to work. Your data needs to be customizable and removable."
R2.	Effort expectancy	Demand that a digital environment is user-friendly.	"It just needs to be easy and user-friendly and all in one place."
R3.	Facilitating conditions	The extent to which an individual experiences that objective factors have an influence on facilitating use.	"You have to get reports to alert you to it."
R4.	Social influence	The extent to which an individual experiences that the use of others influences the use of a digital environment.	"I think the pressure of your social environment can help with that."
R5.	Trust	Requirement that a digital environment must be reliable.	"Yes, trust is very important to me."
R6.	Awareness	Requirement that a digital environment contributes to the awareness of data collection.	"I think it's important to repeat that you're being followed everywhere."
R7.	Price value	Requirement that a digital environment must deliver something for the consumer.	“Het moet ons uiteindelijk wel gewoon iets opleveren.”
R8.	Safety	Requirement that a digital environment is safe to use.	"If you make sure it's safe, you're going to reduce risks."

R9.	Duration	Requirement that the use of a digital environment is efficient.	"Yeah, that just takes a lot of time, too."
R10.	Accessibility	Requirement that a digital environment is accessible to different target groups.	"It should be good for us, but it should be good for everyone. Including older people like me."
R11.	Personal	Requirement that a digital environment matches your personality.	“I would like a personal page of my own."
R12.	Central	Requirement that a digital environment is a central environment for data collection.	"I would like it to be centrally registered somewhere."
R13.	Control	Requirement that a digital environment will give the consumer control.	"That you can just decide for yourself. That you have a little more choices."

Demographic factors*			
D1.	Participant	-	“Participant 1”
D2.	Gender	-	“Female”
D3.	Age	-	“23”
D4.	Education level	-	“Higher professional education”

* Completed by means of a short survey about the demographic factors preceding the focus group session.

Appendix G: Correlation analysis

Correlations

		Age	A1	A2	A3	A4	A5	A6	A7	A8	K1
Measures											
1	Age	1	0.283	0.095	.475**	0.196	0.309	0.11	0.003	0.002	.590**

** Correlation is significant at the 0.01 level (2-tailed).

* Correlation is significant at the 0.05 level (2-tailed).

Correlations

		K2	K3	K4	K5	L1	L2	L3	L4	L5	L6	L7	L8	L9
Measures														
1	Age	0.082	0.011	.429*	-0.023	-0.165	-0.04	-0.139	0.264	0.021	-0.172	-0.107	0.174	0.046

** Correlation is significant at the 0.01 level (2-tailed).

* Correlation is significant at the 0.05 level (2-tailed).

Correlations

		L10	L11	PR1	PR2.1	PR2.2	PR3	PR4	PR5	PR6	PR7	R1	R2	R3
Measures														
1	Age	0.303	0.201	.403*	-0.081	0.076	-0.012	0.009	0.02	.458*	-0.333	-0.207	0.14	0.133

** Correlation is significant at the 0.01 level (2-tailed).

* Correlation is significant at the 0.05 level (2-tailed).

Correlations

		R4	R5	R6	R7	R8	R9	R10	R11	R12	R13
Measures											
1	Age	0.102	-0.07	0.038	-0.002	-0.007	-0.055	0.024	-0.056	-0.283	0.015

** Correlation is significant at the 0.01 level (2-tailed).

* Correlation is significant at the 0.05 level (2-tailed).

- Code A3 = Distrust in collecting medical data
- Code K1 = Medical data collection
- Code K4 = Description personal health record
- Code PR1 = Privacy behaviour
- Code PR6 = Risk awareness

Appendix H: Original quotations

[1] “Maar je hebt natuurlijk ook Google Home die met ons mee luistert. Maar ook Siri die meeluistert. Misschien zitten er achter deze systemen bedrijven die weten waar ik het over heb en die deze informatie vervolgens ook nog gebruiken. " (Sessie 1, deelnemer 1, man, 49 jaar oud)

[2] “Als consument heb je recht op vergetelheid. Je kunt retailbedrijven vragen of ze al je gegevens willen verwijderen." (Sessie 3, deelnemer 11, man, 26 jaar)

[3.1] "Ja, natuurlijk hebben we de GDPR. Het recht om als individu te worden vergeten. Dit is het deel dat nu mogelijk en belangrijk is voor de consument." (Sessie 4, deelnemer 18, vrouw, 22 jaar)

[3.2] "Soms verwijder ik gewoon alle cookies op mijn telefoon of laptop. Maar dat blijf ik de hele tijd doen. Dat is niet wat ik wil." (Sessie 4, deelnemer 18, vrouwe, 22 jaar)

[4] "Ja, ik denk dat een heleboel mensen dat zouden willen [controle over de retail data]. Bijvoorbeeld, als het allemaal gewoon een beetje makkelijker is wat er achter de cookies zit. Dit helpt al om controle te krijgen over je privacy." (Sessie 1, deelnemer 3, vrouw, 30 jaar)

[5] "Ja, maar medische gegevens kunnen ook voor commerciële doeleinden worden gebruikt. Als je bijvoorbeeld diabetes hebt en je hebt een pomp nodig, dan is dat ook commercieel.” (Sessie 2, deelnemer 8, vrouw, 17 jaar)

[6] "Maar je krijgt gewoon geen feedback over het gebruik van je gegevens. Zo eenvoudig is het. Het enige wat je weet is dat ze het hebben verzameld, en gelukkig kun je je hele geschiedenis van gegevens wissen." (Sessie 6, deelnemer 30, man, 60 jaar oud)

[7.1] “Weet je wat het is, dingen veranderen als andere organisaties ook mee willen doen. Dan wil ik de controle houden." (Sessie 2, deelnemer 10, man, 53 jaar)

[7.2] "Dit is alle informatie die tegen je gebruikt kan worden. Het is eng idee dat iedereen dat te zien krijgt of er iets mee doet." (Sessie 2, deelnemer 10, man, 53 jaar)

[8.1] “Nee, maar het is telkens als je ergens naar kijkt, je elke keer weer persoonlijke aanbiedingen krijgt. Dat wil ik niet. Ik wil gewoon niets krijgen.” (Sessie 5, deelnemer 21, vrouw, 24 jaar oud)

[8.2] “Nou, het is een hoop ergernis, maar voor mij hoeft het gewoon niet die controle.” (Sessie 5, deelnemer 21, vrouw, 24 jaar oud)

[9] “En ik denk dat je medische gegevens ook van invloed kunnen zijn op het krijgen van een baan of een hypotheek.” (Sessie 1, deelnemer 2, vrouw, 23 jaar)

[10] "Je weet gewoon niet wie al deze gegevens heeft en wat ze er uiteindelijk mee gaan doen. Dat is veel abstracter dan een medisch dossier. Dus ik vertrouw dat veel minder". (Sessie 4, deelnemer 20, man, 26 jaar oud)

[11] “Ik heb nu niets toe te voegen, maar ik denk dat ik er vanavond over nadenk en de cookies uitzet. Je weet het gewoon niet". (Sessie 1, deelnemer 3, vrouw, 30 jaar oud)

[12] “Ze weten vaak precies wat ik graag koop. Als ik een mooie aanbieding krijg [van een winkelbedrijf], bespaart dat me geld." (Sessie 4, deelnemer 17, vrouw, 44 jaar).

[13] "Ik vind dat het lijkt op stalken. Dat vind ik heel het erg vervelend. Als ik een keer naar iets kijk, zie je er meteen overal spam". (Sessie 5, deelnemer 21, vrouw, 24 jaar)

[14.1] "Ik denk dat nogal wat mensen wantrouwig zijn over het gebruik van winkelgegevens op dit moment. Dit komt omdat je vaak hoort dat er ergens een datalek is of dat onze gegevens toch op straat liggen". (Sessie 1, deelnemer 1, man, 49 jaar)

[14.2] "Als een PCE zijn gegevens lekt, kunnen zij [andere organisaties] ook gegevens over je zien die je niet wilde delen." (Sessie 1, deelnemer 1, man, 49 jaar)

[15.1] "Ik vind het erg vervelend als ik voortdurend banners ontvang met advertenties of websites waar ik op heb geklikt. Je krijgt deze informatie telkens weer te zien." (Sessie 3, deelnemer 13, vrouw, 26 jaar)

[15.2] "Maar het is ook de luiheid van de mens, je vindt het prettig dat je niet hoeft na te denken over het gebruik van gegevens. Ik doe niets aan de bescherming van mijn privacy." (Sessie 3, deelnemer 13, vrouw, 26 jaar)

[16] “Omdat ik geen computerexpert ben. Het zou voor mij eenvoudiger moeten zijn.” (Sessie 2, deelnemer 10, man, 53 jaar)

[17] Ja, of je kunt beter zelf je persoonlijke gegevens gebruiken. Dat je iets met je eigen gegevens kunt doen en dat je dit in een digitale omgeving kunt zien.” (Sessie 4, deelnemer 20, vrouw, 26 jaar)

[18] "Ik denk dat we als consument veel te weinig terug krijgen voor wat een bedrijf aan informatie krijgt. Dus we geven informatie om bedrijven te helpen. We krijgen bijna nooit iets terug.” (Sessie 6, deelnemer 30, man, 60 jaar)

[19] "Nou ja, een veilige omgeving. Goed beveiligd. Dat is gewoon heel belangrijk voor mij." (Sessie 4, deelnemer 20, vrouw, 26 jaar)

[20] "Ik denk echt dat het uit de retail bedrijven moet komen. Ik heb dit in mijn profiel. Albert Heijn of Lidl hebben het uit mijn omgeving kunnen halen en ze lezen daar alleen wat ik wel en niet wil." (Sessie 2, deelnemer 9, vrouw, 41 jaar)

[21] "Dus je moet het niet alleen kunnen aanpassen, maar ook kunnen verwijderen. Dat het anders is dan wat nu mogelijk is." (Sessie 4, deelnemer 18, vrouw, 22 jaar)

[22] "Voor mij zou het echt een vereiste zijn om alle verschillende retailbedrijven in één digitale omgeving aan te hebben." (Sessie 4, deelnemer 19, vrouw, 46 jaar)

[23] "Ik wil graag een applicatie waar al mijn voorkeuren zijn opgeslagen voor retail bedrijven." (Sessie 3, deelnemer 13, vrouw, 26 jaar)

[24] "Ja, ik denk dat als je het verzamelen van gegevens benadrukt, je de mensen wakker maakt. Dit zou mensen ook angstig kunnen maken." (Sessie 1, deelnemer 4, vrouw, 43 jaar)

[25] "Als ik de gegevens uit het persoonlijke gezondheidsdossier bekijk, ga ik ervan uit dat de professionals er met de grootste zorgvuldigheid mee om zullen gaan. Ik wil hetzelfde voelen voor een digitale omgeving met andere gegevens." (Sessie 6, deelnemer 27, vrouw, 23 jaar)

[26] "Dat alle bedrijven de informatie in je Cloud zetten en daarna kunnen bedrijven de informatie alleen nog maar uit uw Cloud halen als u daar toestemming voor heeft gegeven." (Sessie 2, deelnemer 6, man, 21 jaar)

[27] "Blockchain. Je versleutelt de informatie die je wilt opslaan op het platform en stuurt deze naar iedereen en dan heeft iedereen informatie. Op deze manier kan iedereen controleren of de informatie nog steeds correct is en of deze niet is gewijzigd." (Sessie 3, deelnemer 11, man, 26 jaar)

[28] "Als je bijvoorbeeld 16 jaar of jonger bent, kunnen je ouders dat voor je beslissen. En als je volwassen bent, kun je zelf beslissen wat je wel en niet wilt delen." (Sessie 2, deelnemer 6, man, 21 jaar)

[29] "Het mag er niet van afhangen of iemand er meer of minder kennis van heeft of beter in staat is om een computer te gebruiken. Iedereen zou daar toegang moeten hebben tot zijn of haar gegevens en in staat moeten zijn deze te beheren." (Sessie 4, deelnemer 20, vrouw, 26 jaar)

[30] "Ja van die 30/40 seconden filmpjes die je heel kort uitleggen hoe het allemaal werkt." (Sessie 3, deelnemer 15, man, 18 jaar)

[31] "Stel je voor dat je ineens alle cookie statements voor een digitale omgeving moet lezen, dan zou het wel eens ingewikkeld kunnen worden. Want we lezen ze bijna nooit omdat het te veel tijd kost. Op deze manier zou niemand het gebruiken." (Sessie 3, deelnemer 15, man, 18 jaar)

[32] "Meer alsof het echt voor jou gemaakt is. Het moet een omgeving zijn die voor iedereen hetzelfde is, maar de informatie die binnenkomt moet echt persoonlijk voor je zijn." (Sessie 2, deelnemer 7, vrouw, 18 jaar)

[33] "De jongere generatie zou de ouderen kunnen helpen om beslissingen te nemen. Zoals welke gegevens je wilt beschermen en delen." (Sessie 2, deelnemer 6, man, 21 jaar)

[34] "Ik maak meestal geen bewuste keuze. Het maakt me niet echt uit. Je hebt het geaccepteerd dat al je gegevens nu worden gebruikt." (Sessie 4, deelnemer 20, vrouw, 26 jaar)

[35] "Ja, het volgende wat je moet doen is het opruimen aan het eind van de avond. Gooi alle cookies weg. Dat doe ik ook." (Sessie 6, deelnemer 30, man, 60 jaar)

[36] "Dit komt omdat je vaak hoort dat er ergens een datalek is of dat onze gegevens ergens op straat liggen." (Sessie 1, deelnemer 1, man, 49 jaar oud)

[37] "Het staat ook op een persoonlijke database. Zelfs als je het hebt verwijderd, hebben ze nog steeds je gegevens. Ze gaan het niet zomaar verwijderen." (Sessie 1, deelnemer 2, vrouw, 23 jaar)

[38] "Het is niet zo dat je mobiele telefoon gaat ontploffen. Er gaat niets gebeuren als ik gewoon op "accepteren" druk. Je voelt gewoon nog geen nadelen." (Sessie 4, deelnemer 19, vrouw, 46 jaar)

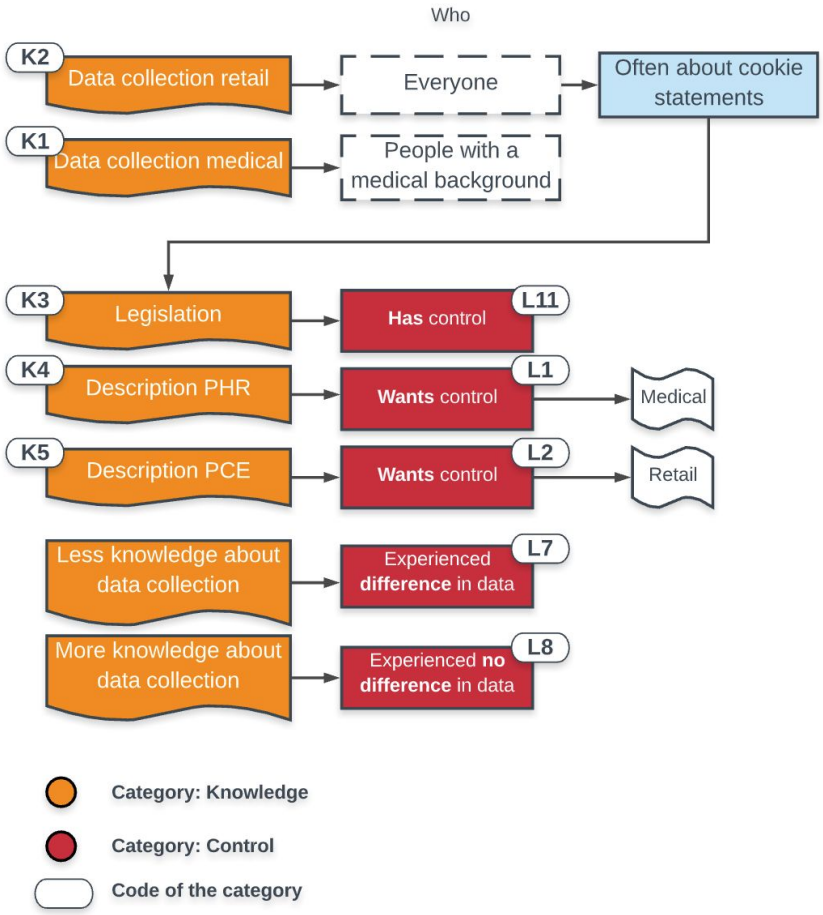
[39] "Stel dat je toegang hebt in een digitale omgeving. Hier geeft u aan welke bedrijven u expliciet interessant vindt. Zo zit je misschien in je eigen bubbel zonder te weten wat er nog meer beschikbaar is." (Sessie 2, deelnemer 6, man, 21 jaar)

[40] "Ja, ik vind dat hacken van gegevens een groot risico is. Stel je voor dat iemand zonder toestemming in mijn digitale omgeving zou kunnen kijken en dan deze informatie zou kunnen gebruiken. Ze zouden er alles mee kunnen doen." (Sessie 4, deelnemer 19, vrouw, 49 jaar)

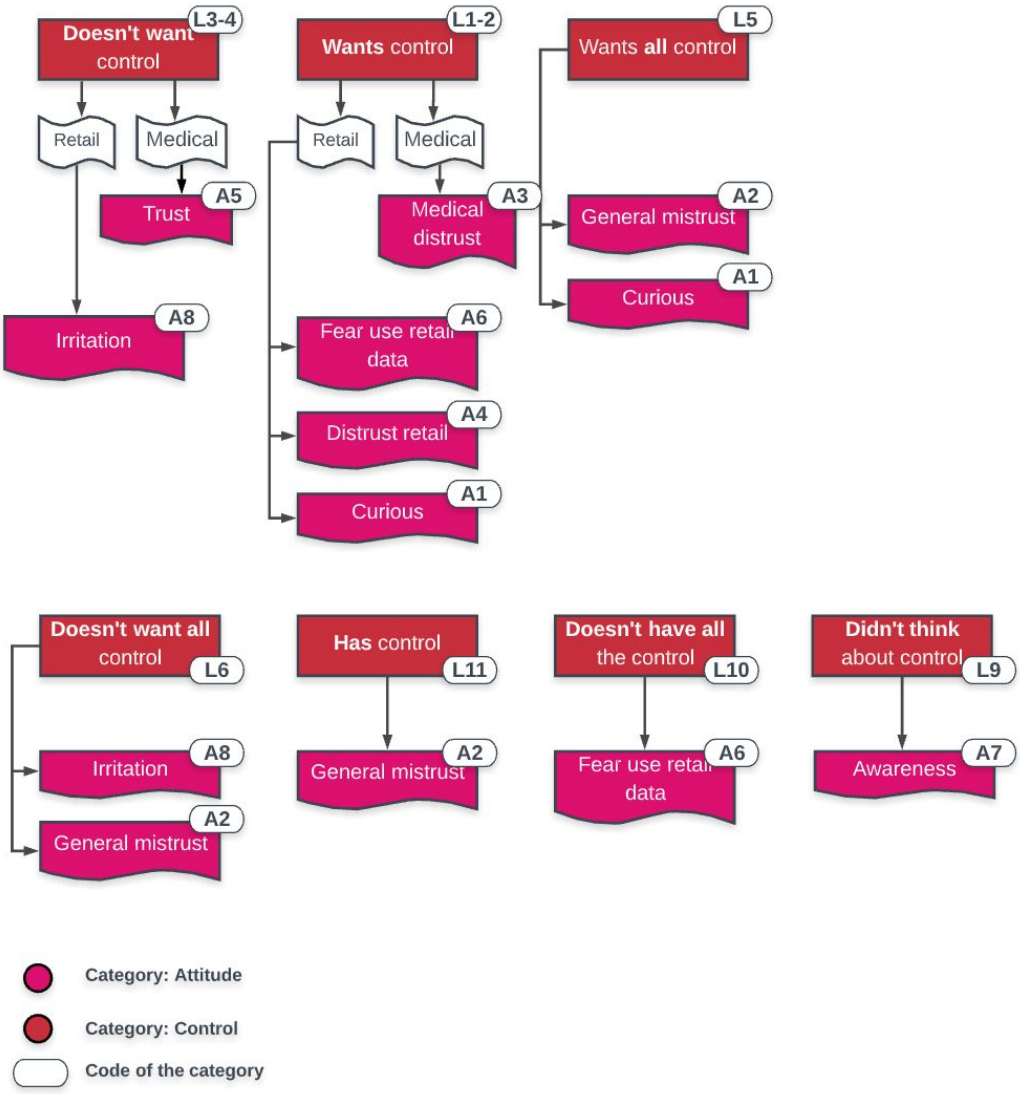
[41] "Nou, een veilige omgeving. Goed beveiligd. Dat is gewoon heel belangrijk voor mij." (Sessie 4, deelnemer 19, vrouw, 49 jaar)

Appendix I: Relationships between the codes

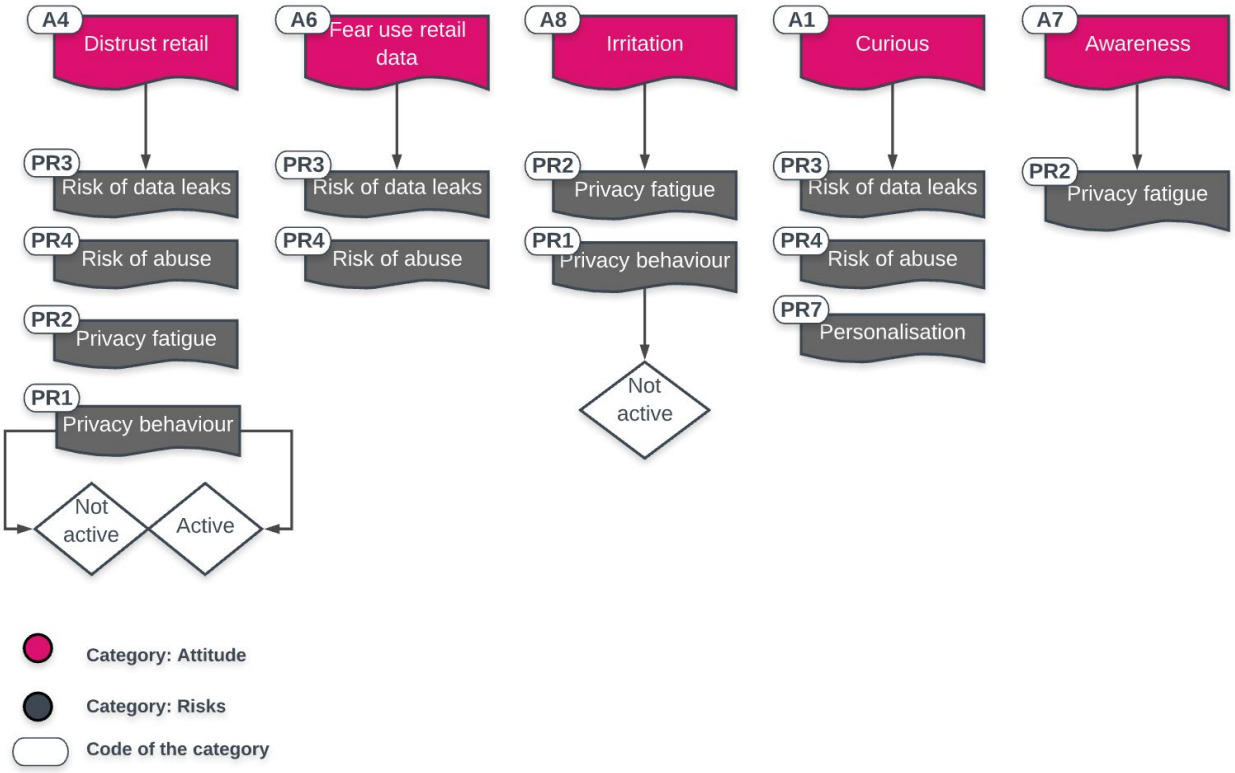
1. Relationship between the knowledge and need for control of the consumer



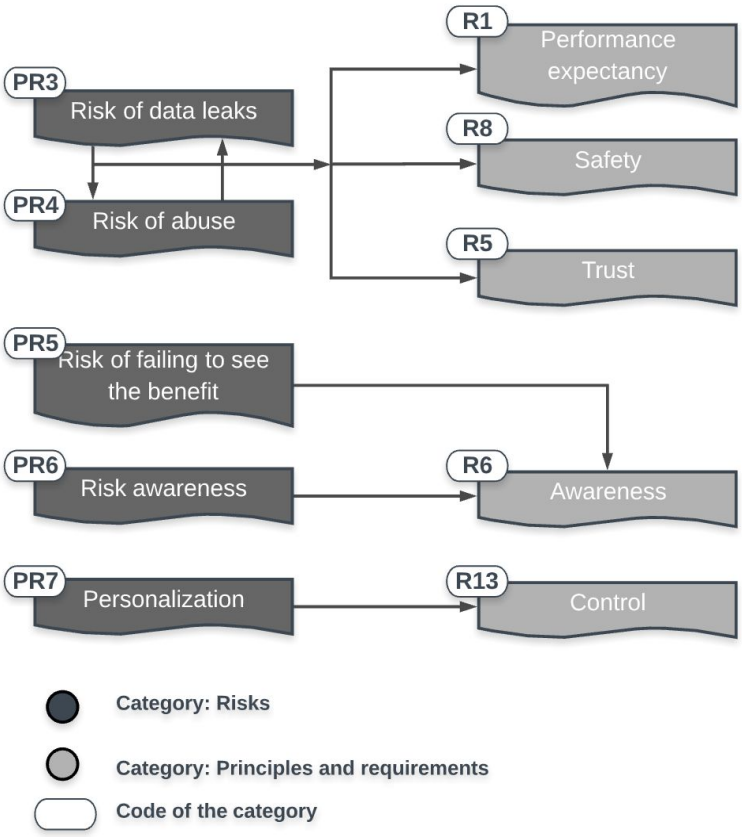
2. Relationship between the need for control and the attitude of the consumer



3. Relationship between the attitude of the consumer and the risk of collecting retail data



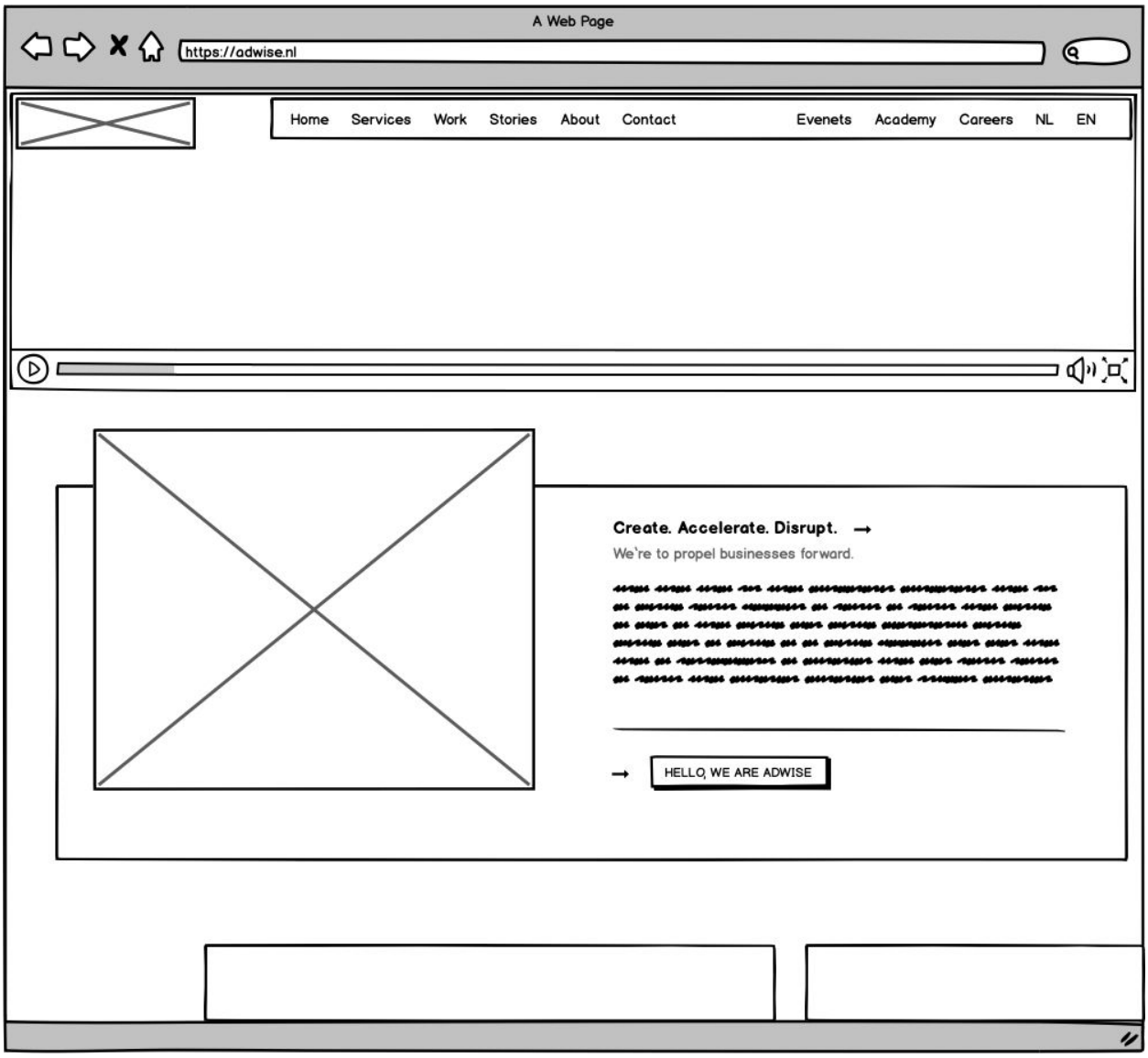
4. Relationship between the risk of retail data collection and the principles and requirements of a PCE.



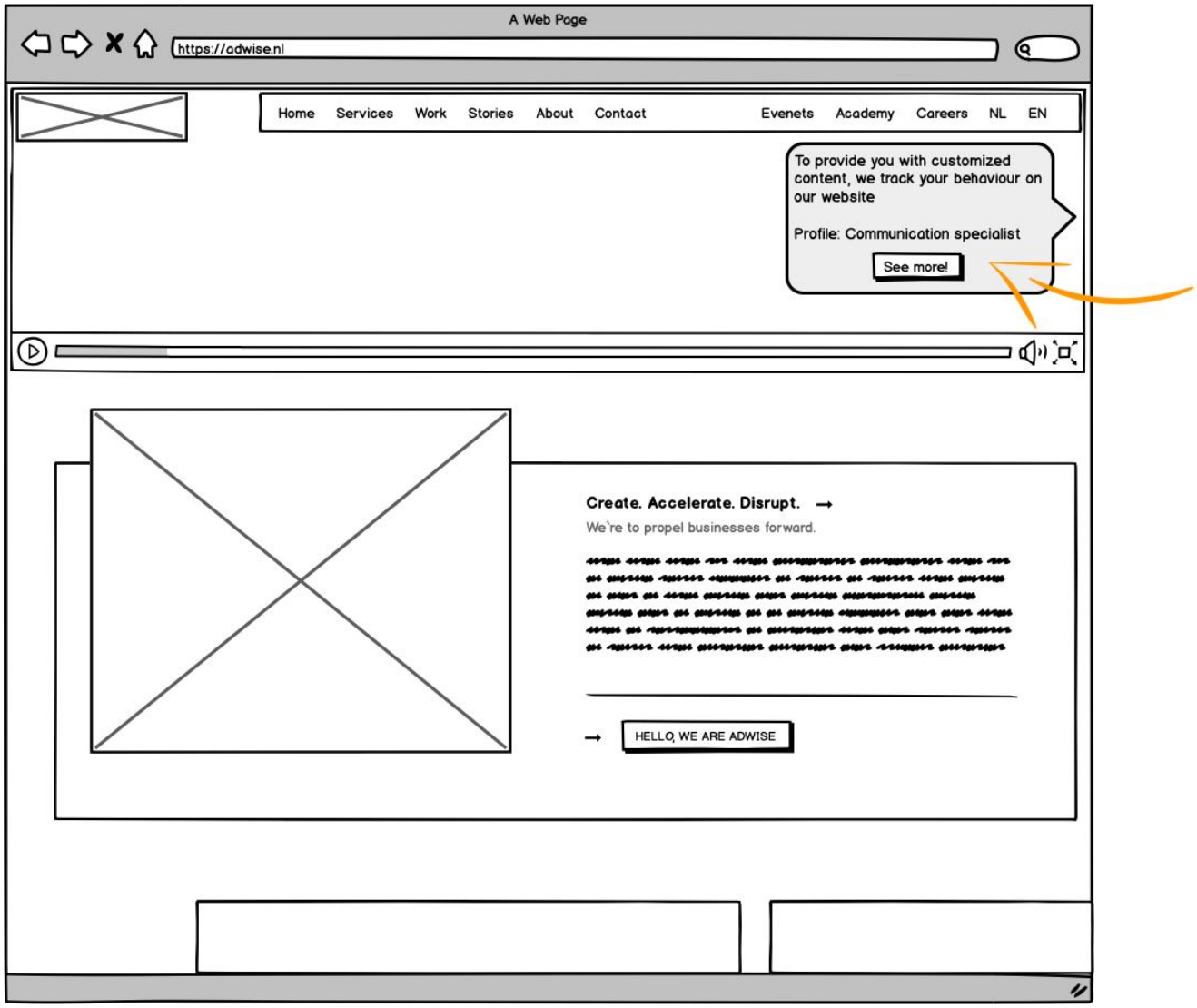
Appendix J: Concept product

Three views of a website presenting a way in which consumer confidence is central.

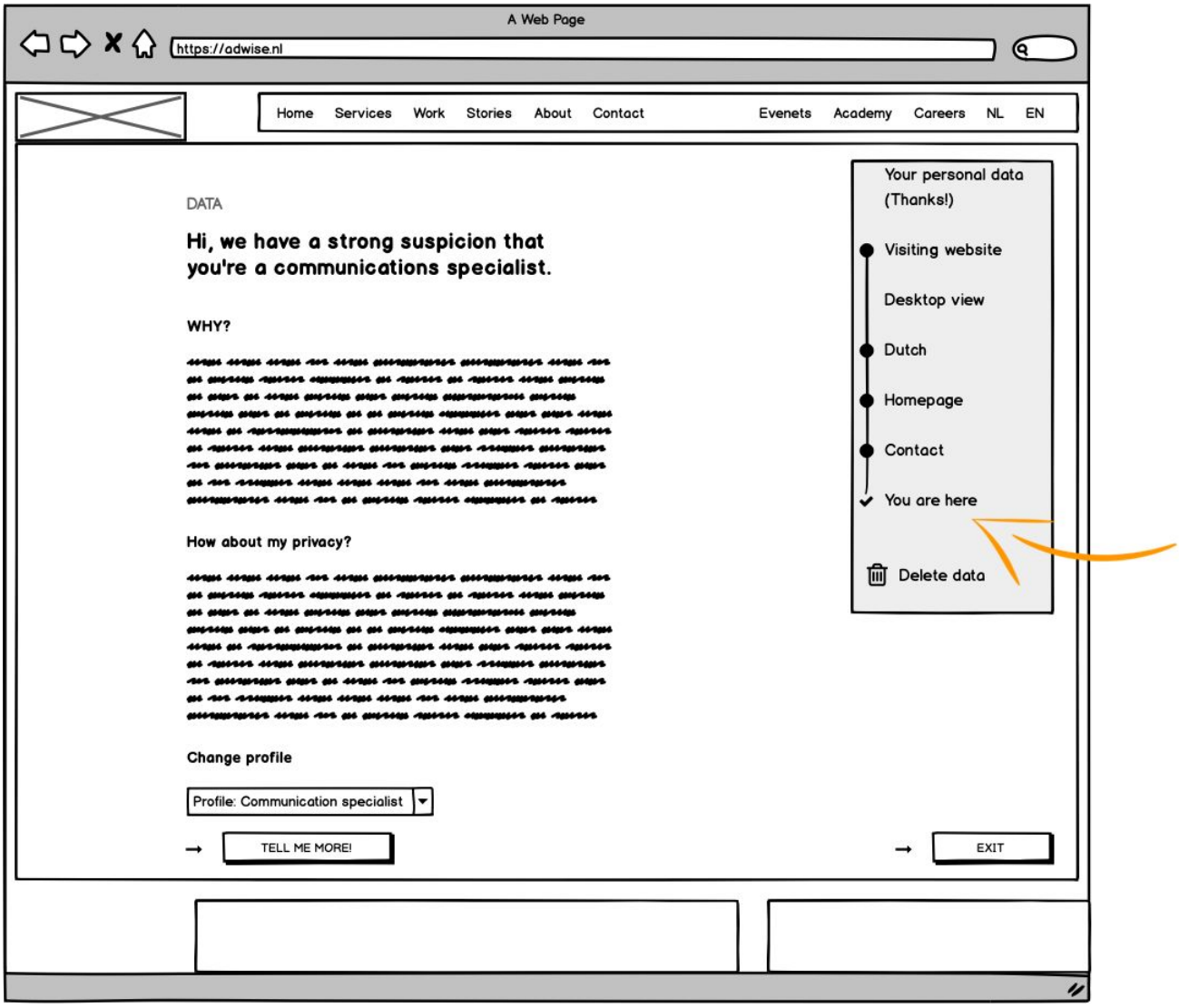
1. *HOME PAGE*



2. *HOME PAGE WITH NOTIFICATION*



3. *DETAIL PAGE (with the corresponding profile)*



Master Thesis

February 2020

Loraine Seliger