Ambient intelligence & personalization : people's perspectives on information privacy

DOI:
10.6100/IR642224

Ambient Intelligence & Personalization:

People's Perspectives on Information Privacy

Evelien van de Garde-Perik

Ambient Intelligence & Personalization:

People’s Perspectives on Information Privacy

The work described in this thesis has been carried out at the Philips Research Laboratories Eindhoven, the Netherlands and the faculty of Industrial Design of the Eindhoven University of Technology, the Netherlands.

Cover design: Paul Verspaget
Printing: Universiteitsdrukkerij Technische Universiteit Eindhoven

This thesis is printed on recycled paper.

A catalogue record is available from the Eindhoven University of Technology Library
ISBN: 978-90-386-1732-9

Ambient Intelligence & Personalization:

People's Perspectives on Information Privacy

PROEFSCHRIFT

ter verkrijging van de graad van doctor aan de
Technische Universiteit Eindhoven, op gezag van de
Rector Magnificus, prof.dr.ir. C.J. van Duijn, voor een
commissie aangewezen door het College voor
Promoties in het openbaar te verdedigen
op dinsdag 19 mei 2009 om 16.00 uur

door

Evelien Maria van de Garde-Perik

geboren te Oldenzaal

Dit proefschrift is goedgekeurd door de promotor:

prof.dr.ir. J.H. Eggen

Copromotor:
dr. P. Markopoulos

Acknowledgements

In May 2003 I started working on the research for my thesis. I did not know that so many things were about to happen in the years that would follow. Many people supported me in one way or another during this important period of my life. Thanks to all of you!

Above all, I would like to thank the following people:

Berry Eggen

For being my promotor. In the beginning of my PhD we were working together in preparing the EUSAI 2004 conference, towards the end of my PhD again we were working closely together in trying to finish my thesis. I would like to thank you for the numerous amount of times that you have read and reread (parts of) my thesis and for your suggestions for improvement. Thanks for keeping calm and understanding in times of pressure.

Panos Markopoulos

For being my co-promotor. Although we have different working styles, we successfully worked together during the course of my PhD. I appreciate the degree of freedom you gave me in my research and the faith you have shown in me. I greatly value your detailed reviews of the papers and chapters that resulted from my research.

Boris de Ruyter

For providing an industrial context to my work, and for spending a lot of precious time and effort in building the Music Recommender (several versions of it!!!) and one of the Questionnaires of chapter 3.

Pam Briggs, Huib de Ridder & Jean-Bernard Martens

For accepting to be a member of the reading committee and for carefully reading the lengthy draft of my thesis. With the help of your comments and suggestions I was able to improve (the focus of) my thesis.

Natalia Romero Herrera

For accepting to be my paranymph. We shared many things during the last couple of years: both of us being a former USI and having worked at Philips Research, we shared an office, both investigated privacy, and worked with the same supervisor. Thanks for all the support in my work and all the pleasure next to it. I hope to be your close colleague for many years to come (and I am glad it is still possible)!

Besides, during my PhD I have consulted several people for advice on which route to take; I would like to thank all of them. I am especially thankful to Wijnand IJsselsteijn for his support in the first stages of my PhD and to Jan Engel for his thoughts and advice on statistics. I appreciate the help I have received from many colleagues at Philips Research and the Eindhoven University of Technology in the form of useful discussions and suggestions for improvement after reading parts of my thesis. Thanks to all the people who participated in my studies, among which were many of my colleagues, friends and family members. Furthermore, thanks to Philips Research for funding this research.

Finally, and most importantly I would like to thank my family for being there for me. While I am grateful for the support I have received from everyone, I would like to thank some family members in particular (which I will do in Dutch).

Magda, bedankt voor het feit dat je Marlieke en (nu ook) Nic een geweldige tijd thuis hebt gegeven, terwijl ik bezig was met mijn onderzoek en proefschrift. Pap en mam, hartelijk bedankt voor het feit dat jullie altijd onvoorwaardelijk voor me hebben klaargestaan. De afgelopen tijd hebben jullie met liefde ontzettend veel taken en zorgen overgenomen. Mijn dank is groot! Ankie, wij hebben een band voor het leven. Ik ben ontzettend blij dat je met veel enthousiasme hebt geaccepteerd om mijn paranimf te zijn.

Rogier, Marlieke en Nic, ik vind het jammer dat ik zo druk ben geweest de afgelopen tijd. Ik heb jullie helaas niet de volle aandacht kunnen geven die jullie alle drie verdienen. Maar met het afronden van mijn proefschrift is er nu weer tijd om volop samen te genieten. Ik ben dolgelukkig en dankbaar dat jullie in mijn leven zijn.

Contents

1. Introduction

This thesis concerns people's perspectives on information privacy in the context of Ambient Intelligence and personalization. The concept of Ambient Intelligence will be described first, which will address the importance of privacy research. Then, existing research and design in relation to privacy will be reviewed. Based on the background provided by these sections, a description of this thesis' research problem and research approach will be provided. This chapter ends with an outline of this thesis.

1.1 AMBIENT INTELLIGENCE AND PERSONALIZATION

1.1.1 The concepts of Ambient Intelligence and personalization

“Imagine coming home after a long day of hard work. You immediately feel great the moment you enter the house. The temperature is just right, the lighting is perfect. You couldn’t have selected the music better yourself. You open your fridge and smile. It contains your favorite snack and the oven is already preheated. This is just what you needed. All you have to do is pop the dish into the oven and relax. While your food is being cooked, you receive a personal update of local news, sports scores, as well as some information about current theater shows that you may like to visit.”

The scenario above presents just one example of an Ambient Intelligence environment. Many companies see Ambient Intelligence as a vision of the future for information and communication technologies. It is a future where technology is everywhere, but where it disappears into the background. Computational and communicational intelligence will be embedded into everyday objects such as furniture, clothes, vehicles, roads, smart materials and even particles of decorative substances like paint. Ambient Intelligence will result in a smart, perceptive environment that adapts to its inhabitants (Aarts, 2003). It will enable people and objects to interact with their environment in a seamless, trustworthy and natural manner. In an environment with Ambient Intelligence, devices will operate collectively. Lighting, sound, vision, domestic appliances, and personal healthcare products operate together to improve the user experience through natural and intuitive user interfaces (Aarts, 2005). Environments will contain many different technologies that are interconnected to provide the main Ambient Intelligence functionality. Similar concepts to Ambient Intelligence are Ubiquitous Computing (Weiser, 1991) and Pervasive Computing (IBM, 1999b). The term Ambient Intelligence will be used to describe the research context of this thesis. The term Ubiquitous Computing will be used occasionally for references in accordance with the existing work.

Ambient Intelligence relies on proactive and autonomic computing. Proactive computing aims to improve both the performance and user experience by speculative or anticipatory actions. Autonomic computing aims to improve the user experience through system self-regulation (Satyanarayanan, 2002). Related to these forms of computing is personalization, which implies the adaptation of a system towards needs and interests of a user. Personalization is the tailoring of a product or system towards an individual to support his or her personal preferences and/or intentions. In the context of computation and communication technologies personalization can be described as the adaptation of content, structure and/or presentation to the characteristics of each individual user, usage behavior and/or an environment (adapted from Kobsa et al., 2001).

Personalization is already widely used. An example of personalization that is already available is the personal recommendations for books or CD’s that are provided by Amazon on the basis of previous purchases. Another example is the feature in the Microsoft Windows environment that only the most recently used programs, functions or files are instantaneously visible. In the future, personalization could happen across applications, such that web browsing history or location tracking are available and used to provide appropriate personal and localized information on various devices. It could also be that rooms become sensitive to their occupants and the activity they are engaged in and consequently that the room adapts temperature, lighting conditions and music accordingly.

User needs and preferences to which a system adapts may be specified by the user, or an Ambient Intelligence system may derive these needs by observation of user activity or logging of user interactions. Trewin (2000) makes a distinction between adaptable and adaptive systems. Adaptable systems are systems where users can alter many aspects of the interface; adaptive systems on the other hand are systems that take initiative in achieving a suitable configuration (Trewin, 2000). Adaptivity is one of the defining characteristics of Ambient Intelligence (Aarts, 2003).

In order for systems to be personalized to fit user needs, it is necessary to collect data about that user, his or her preferences and activities. In other words, there is a need for personal data. Typically, the information that is stored about the user is referred to as a user profile or a user model (Dickinson et al., 2003). Fischer (2001) defines a user model as a model that systems have of users and that resides inside a computational environment. User profiles can contain various types of information, for example information about access and use of a system, including the particular functions that were used. They can include information about the users themselves, such as name, user ID or location.

The existence of a user profile facilitates the shared use of one machine by multiple users, or the use of a variety of different machines by one specific user. The user profile can contain a user's basic requirements or preferences, which can be easily stored and recalled, and which can save the users from going through a new configuration process for every session (Trewin, 2000). Depending on the context for which the user profile is used, it can contain a variety of data about the user. On a PC a user profile can be a collection of personal documents and settings, such as 'favorites' or 'bookmarks' for frequently visited websites, desktop contents, and cookies containing personal data or information about website visits such as the contents of electronic shopping carts. A user profile in an intelligent tutoring system can contain information on a learner's knowledge with regard to the topic of interest, general cognitive abilities, as well as personal preferences. For information filtering systems (e.g., music, television, or travelling recommendations) a user profile can contain information such as general user characteristics, previous use of the information, user ratings, and assumptions based on knowledge and characteristics of similar users. For an Ambient Intelligence environment the profile may include similar types of information including records of user state or activities as they are observed by the system (e.g., information on presence, mood, activity).

There are different ways to obtain data for a user profile. Three main types of personal data retrieval can be distinguished:

- Asking the user to provide the necessary information (e.g., age, address, or credit card number);
- Logging or tracing actual use of the system (use of computer functions, watching of television channels, telephone numbers dialed, locations visited);
- Analyzing or interpreting the user's behavior (related to the system itself, or more general user information, e.g. preferences for TV shows or personality traits).

The first type of profiling is mostly referred to as explicit data collection, because the user consciously and intentionally provides data (Cranor, 2004). In the latter two cases, the user does not have to provide the necessary data explicitly. These two types of data retrieval are called implicit profiling.

In short, current developments towards Ambient Intelligence aim to provide people with a smart perceptive environment based on computational and communicational intelligence in everyday objects. The intelligent environment will react in a proactive and autonomous manner to characteristics of each individual user, behavior or situation based. Therefore, Ambient Intelligence relies on the collection and storage of data about the user, his or her preferences and activities.

1.1.2 Expected benefits of Ambient Intelligence

The characteristics underlying Ambient Intelligence are intended to bring people many benefits. For example according to Aarts (2003) Ambient Intelligence is:

- Embedded: many networked devices are integrated in the environment;
- Context-aware: these devices can recognize users and their situational context;
- Personalized: they can be tailored towards the user's needs;
- Adaptive: they can change in response to the user;
- Anticipatory: they can anticipate the user's desires without conscious meditation.

The following description of Ambient Intelligence and its benefits is provided by the Information Society Technologies Advisory Group[1] (ISTAG, 2001):

> *"Ambient Intelligence implies a seamless environment of computing, advanced networking technology and specific interfaces. It is aware of the specific characteristics of human presence and personalities, takes care of needs and is capable of responding intelligently to spoken or gestured indications of desire, and even can engage in intelligent dialogue. Ambient Intelligence should also be unobtrusive, often invisible: everywhere and yet in our consciousness – nowhere unless we need it. Interaction should be relaxing and enjoyable for the user, and not involve a steep learning curve."*

It is the ambition of researchers in this field that Ambient Intelligence will make interaction between people and their environment more natural (Aarts et al., 2002; Abowd & Mynatt, 2000) and hence provide seamless and intuitive support to people in their daily life activities (ISTAG, 2001). Interaction will be more like the way users interact with the physical world, and less like the way desktop computers are currently used. Handwriting, speech and gestures may be used as explicit or implicit input to an Ambient Intelligence environment (Abowd & Mynatt, 2000). Benefits of systems that support more natural human forms of communication and thus of Ambient Intelligence are improved learnability, general ease of use, and support of tasks without drastically changing the structure of those tasks (Abowd & Mynatt, 2000) or by allowing users to concentrate on the real task (ISTAG, 2001).

To summarize, an Ambient Intelligence environment will enable people to benefit from information and services anywhere, without conscious effort, from the user's point of view, non-intrusively, and with flexibility and adaptability.

[1] The ISTAG reflects and advises on the definition and implementation of a coherent policy for research in ICT in Europe.

1.1.3 Potential downsides of Ambient Intelligence

Besides the positive aspects mentioned before, Ambient Intelligence and personalization will definitely have some potential downsides as well. The user's physical environment will be equipped with numerous devices, all of which can store sensitive[2] or personal information about the user. The collected user information can be stored and used in order to provide personalized services to users, but it can also be copied and aggregated indefinitely with other sources of information. This may even take place without user involvement or awareness. This implicit collection of information is an essential element of scenarios relating to Ambient Intelligence (Aarts et al., 2002). Although this implies less effort for the user, it can lead to privacy issues because of a lack of awareness and control by the people concerned (Cranor, 2004; Kobsa & Schreck, 2003; Nguyen & Mynatt, 2002). Such a technological landscape can be problematic for users.

Aarts et al. (2002) mention several possible threats to people in an Ambient Intelligence environment. People might be concerned about the requirements underlying Ambient Intelligence, possible accidents, and long term risks. The requirements underlying Ambient Intelligence result in constant monitoring, as well as registering and recording user behavior for personalization. Accidents could be due to an environment in which autonomous decisions by electronics on a large scale get out of control, or lack of safety and security. Ambient Intelligence systems could be extremely vulnerable to intrusion and damage caused by outsiders, and large amounts of possibly personal information could be floating around without protection. Finally, long term risks are a consequence of the technological nature of Ambient Intelligence. In an extreme form people could be represented by digital substitutes, which could lead to alienation of people or to a blurred reality.

Abowd and Mynatt (2000) describe four main social implications related to ubiquitous computing, namely security, visibility, control and privacy. Security of data is a concern, since data may be accessed and possibly modified by anyone without appropriate security. Transportation of data over a public network increases the risk. Visibility of activities is especially important in an environment where computers are disappearing in the background; users should be informed about how they are being sensed in an 'invisible' computing environment. Users should be able to control; they should be able to stop sensing or recording, or to control the distribution and use of the information. Privacy is described by Abowd and Mynatt (2000) as appropriate and beneficial use and dissemination of information, which is particularly important since ubiquitous computing makes information more generally available.

The issues of security, privacy and control are also addressed in the ISTAG report ISTAG (2001). This report provides numerous examples of critical socio-political factors for Ambient Intelligence. Among other things the ISTAG report describes the impact of Ambient Intelligence on:

- Trust[3] and confidence: People may wonder whether there will be effective norms of trust that prevent invasive/intrusive usage of technologies.

[2] Sensitive information can be regarded as secret or confidential, and as such it is not to be divulged.

[3] In the context of this thesis trust is the degree of belief that, for a particular situation, an entity has the capacity to 'harm', but is not expected to exercise this capacity.

- Privacy: Issues may arise due to the fact there will be more open systems. There may be problems regarding ownership of data, content control, and accessibility of content. In other words, protection of users in an Ambient Intelligence landscape may be complicated. Furthermore, technological developments are outpacing regulatory adjustments. And free will and choice could be reduced as a result of Ambient Intelligence.
- Security: This is needed to protect private and confidential transactions from third party interference, to prevent exposure to viruses and hackers, and to deal with computer and network collapse.
- User control: Ambient Intelligence should be controllable by ordinary people, and allow people to decide what level of access they have on what issue and when. Perhaps different identities could be used to show different aspects of the user e.g. business related, personal, medical etc.

Similar points are raised by the Safeguards in a World of Ambient Intelligence[4] (SWAMI) consortium (Punie et al., 2005). The SWAMI consortium provides dark scenarios of Ambient Intelligence which highlight potential risks related to issues such as security, identity, trust, loss of control, victimization, and privacy. The scenarios illustrate the consequences of misuse or incompletely processing of identity-based data (i.e. information related to legal identity, identification, authentication and preferences). Victimization occurs in the scenarios when people are unfairly treated as criminals.

The SWAMI scenarios show privacy invasions in various forms such as:
- Identity theft (or identity-related crime): This may be possible in an Ambient Intelligence environment without suitable security. It may give malicious persons many opportunities to steal identity information (typically financial details e.g. credit card details) and to use it for criminal purposes.
- Disclosure of personal data: Many privacy threats are associated with disclosure of information; it could lead to spamming, or disclosure of location information may result in embarrassing situations.
- Surveillance: This is possible since every inhabitant leaves electronic traces in an Ambient Intelligence environment. These traces enable new and more comprehensive surveillance of people's physical movements, use of electronic services and communication behavior. It is possible to construct very sophisticated personal profiles and activity patterns. Surveillance may be desirable for the safety and security of society; however it causes ethical, privacy and data protection problems.
- Risks from implicit user profiling: Users may not be aware of the digital traces they leave behind, or could be deprived from having access to some services, and it results in lack of freedom in making decisions.

Garfinkel's Database Nation (2000) gives various examples of how the storage of data about people may compromise their privacy. The data stored may be used in another context, for another purpose, or by parties unknown to the person involved. Garfinkel describes how supermarket discount cards, warranty cards, and cell phone networks can be used to track individual consumer preferences and their physical movement (in case of cell phones). An example of unexpected use of such data is that of a man who slipped and injured himself in a store, and consequently sued the store. The store used

[4] SWAMI is an EU-funded research project aiming to identify social, legal, economic and ethical implications related to Ambient Intelligence.

the data from his loyalty card, which showed a history of liquor purchases, in order to undermine the credibility of his claim. Furthermore, Garfinkel describes various technologies, such as retina scans and DNA analysis that can be used to identify and track individuals. He also illustrates how medical data can be available and misused by for example potential employers and insurance companies. Garfinkel argues that privacy is not just an issue of regulation and of penalizing offenders; lack of privacy can have a profound impact on society when people feel less free, because they are being watched everywhere they go. It could be that when visions such as that of Ambient Intelligence materialize, people will no longer be able to act unobserved anywhere and anytime.

All issues mentioned in this section are directly related to users' privacy. To avoid the dark scenarios sketched out above, to preserve personal freedoms, but also to enable acceptance of Ambient Intelligence technologies, privacy concerns of people need to be understood and adequately addressed. Appropriate solutions to provide protection of people's privacy in Ambient Intelligence environments are needed.
The following section will deal with privacy from various perspectives. First of all, the notion of privacy will be discussed and a definition of privacy will be provided. Then, privacy research and existing ways to address privacy concerns will be reviewed.

1.2 REVIEW OF PRIVACY RESEARCH AND DESIGN

1.2.1 The notion of privacy

Over the ages, technological developments have often brought with them threats to privacy and have increased sensitivity of society to privacy issues. In the 19th century private and domestic life could be invaded due to inventions such as photography or printing (Warren & Brandeis, 1890). Prior to such inventions, people had to be present in order to witness an event. Through these inventions it suddenly became possible to make visual or audio recordings of a private event. These recordings could afterwards be shown or played to a larger audience in another setting. Warren and Brandeis (1890) described the right to privacy in this context as the right to be let alone.

Almost a century later, Westin (1967) claimed similarly that the right to privacy must no longer be taken for granted due several forms of surveillance (e.g. traditional surveillance by devices like spike microphones, phone taps, and parabolic microphones; psychological surveillance through personality testing; and data surveillance by monitoring information collected in databases). Westin (1967) defined privacy as the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others. In other words privacy is the ability of the individual to control the terms under which his or her personal information is acquired and used by others.

A few years later Altman (1975) dealt with privacy from a social psychology perspective. He described privacy as an interpersonal boundary process by which individuals or groups regulate their interaction with others. Altman sees privacy as selective control of access to the self or to one's group. People optimize their accessibility along a spectrum of “openness” and “closedness” depending on context. According to Altman the concept of privacy is central to understanding the relationship between the physical and social environment and the individual's behavior. Personal space and territorial behavior are mechanisms which can be used to achieve desired levels of privacy for individuals or groups (Altman, 1975). Altman describes four mechanisms that can be used in an attempt to obtain desired levels of privacy:

- Verbal (what and how things are said) and nonverbal behavior (body language that may be used for instance to convey discomfort when other people come too close);
- Personal space or the use of distance or angle of orientation from others;
- Territorial behavior or the use of areas and objects in the environment;
- Culturally based norms and practices.

The territorial mechanism is more distant from the self compared to personal space, yet both personal space and territorial behavior play an important role in privacy regulation according to Altman. They may be used to open the self to interaction with others or close the self off from such interaction.

Privacy is a complex phenomenon that is interpreted differently depending on the individual and the circumstances (Boyle & Greenberg, 2005). Privacy only becomes an issue within a public context, as one may decide to present certain parts of oneself depending on the audience and the situation involved (Goffman, 1959). Privacy is often described as a process of control over personal information (Boyle & Greenberg, 2005). In the context of this thesis, the term 'privacy' refers to a boundary control process in which individuals regulate when, how and to what extent information about them is communicated to others. The emphasis will be on information privacy, rather than interpersonal or social privacy. *Information privacy* refers to the claim by individuals that data about themselves should generally not be made available to other individuals and organizations and that, where data is possessed by another party, the individual must be able to exercise a substantial degree of control over that data and its use (Clarke, 1999, pg. 60). In this thesis the term privacy is used to denote information privacy, unless stated otherwise.

Westin's and Altman's views on privacy represent different types of privacy. According to Iachello and Hong (2007) the work by Westin refers to the management of personally identifiable information, something they call data protection. The focus is on protecting such data by regulating how, when, and for what purpose data can be collected, used and disclosed. The work by Altman, on the other hand, describes how people manage their privacy with respect to other individuals, and is called personal privacy by Iachello and Hong. The focus of this thesis is related to Westin's view on informational privacy, in contrast to Altman's view on *interpersonal privacy*.

1.2.2 Research into privacy related to Ambient Intelligence

Privacy appears to be an inherently difficult concept to study. Recently, researchers into privacy and ubiquitous computing have come to recognize the methodological difficulties for researching privacy in this domain and successive workshops at international conferences were organized on this topic (Romero et al., 2005; Patil et al., 2006).

A well-known issue in privacy research concerns the apparent discrepancy between privacy-related attitudes and behaviors, which has been reported in several different empirical investigations of privacy preferences (e.g., Acquisti & Grossklags, 2003; Berendt et al., 2005). This discrepancy means that stated preferences or attitudes towards new products are hard to use as an indication of intention to use.

There can be several explanations for this discrepancy. In general, attitudes expressed outside a specific context are not good predictors of behavior, since behavior is mediated by social and environmental factors (Ajzen & Fishbein, 2005). Furthermore, as already known from experiments by Milgram (1974), under the authority of the experimenter participants can engage in behaviors they would not normally engage in.

To deal with the difficulties of studying privacy regarding Ambient Intelligence, privacy researchers sometimes propose systematic analyses of privacy risks (Hong et al., 2004), or structured methods to guide the design of context aware and adaptive systems with respect to personal privacy (Iachello & Abowd, 2005). Several technological solutions to guarantee people's privacy have been proposed; for a relatively recent survey see Langheinrich (2005). Other researchers have focused on providing design guidance to designers of Internet-based applications (e.g., Ackerman et al., 1999; Good & Krekelberg, 2003) and Ambient Intelligence and Ubiquitous Computing applications (Bellotti & Sellen, 1993; Nguyen & Mynatt, 2002; Lederer et al., 2004; Langheinrich, 2002). There is still little known about how users of personalized systems experience disclosure of information, what motivates them, and how conscious they are of the choices they make concerning the disclosure of information and the consequences thereof.

The remainder of this section will review privacy research and design for privacy from three different perspectives. First, previous research on users' perception of privacy will be treated. Then two possible ways to manage user's privacy concerns in Ambient Intelligence environments will be discussed: legally based design guidance and technical tools for privacy protection.

1.2.3 User perception of privacy

From the discussion on the potential downsides of Ambient Intelligence in section 1.1.3, it became clear that privacy is a major issue for Ambient Intelligence. Not many studies have been performed on the user perception of privacy in Ambient Intelligence. However, there are various studies that have been performed on the perception of privacy in general or for specific applications such as e-commerce or context-sensing. Some of the relevant work in the light of this thesis will be discussed in this paragraph. Two different types of studies are distinguished: general surveys or public opinion polls and the development and validation of privacy models.

General surveys and public opinion polls on privacy

The study by Ackerman et al. (1999) presents insights on Internet users' attitudes about privacy. Their study is a web-based survey with 381 participants. They found a high level of concern about privacy in general and on the Internet in particular. Participants' reactions to scenarios about online data collection were extremely varied. Participants' comfort level to provide personal information depended on the type of information involved.

IBM (1999a) reports a multi-national survey (United States, Germany, and United Kingdom) conducted on consumer privacy and personalized marketing in four specific industries (health, finance, insurance and retail). Approximately 1000 adults from each of the three countries participated in a telephone based interview and an additional 2000 adults from the US participated in a web-based survey. In total 80% of the participants agreed with the fact that "consumers have lost all control over how personal information is collected and used by companies." And 71% felt "it is impossible to protect consumer privacy in the computer age". Based on participants' answers to some of those statements the report distinguishes participants on the basis of their level of privacy concern. Males are more likely than females to be in the “High” Privacy Concern group (28% vs. 21%) as well as consumers over age 50 (33% vs. about 20% for the other age groups). Almost all participants (94%) indicated to be “very” or “somewhat” concerned about the possible misuse of their personal information. Similarly, a high proportion of participants (92%) said they are concerned about threats to their personal privacy when they are using the Internet. Females expressed greater concern than males.

Cyber Dialogue (2000) uses a telephone based survey and an online survey to obtain opinions about privacy (2000 and 500 participants respectively). Cyber Dialogue found that the type of information influences people’s willingness to disclose in return for personalized content. Most online users are willing to share their name with a Web site (88%). Over 80% of online users are willing to supply information regarding their level of education, age, or hobbies. However they are less willing to provide sensitive information such as income (59%) or a credit card number (13%). About half of the participants (49%) feel that a Web site that shares information about them with other companies is invading their privacy. In case of behavioral information that will be used only for the purposes of providing customized content, some consumers are willing to allow the sharing of information across Web sites. Many, however, will not accept the distribution of personal information without permission or compensation. And almost one-third of online users feel that Web sites should not share any information about their customers with other companies.

Another web-based survey with 1529 participants by Harris Interactive (2002) found that a majority of participants (79%) agreed that they have lost control over how their personal information is collected and used by companies. Participants indicated to be most concerned about the threat of their personal information falling into the hands of individuals or companies who have no relationship to them. Participants indicated that selling personal information to third parties (75%) is by far their greatest concern. Also this study uncovered that willingness to disclose online depends on the type of information involved. In case of health related information, 67% of participants said they never share the information online, 36% in case of financial information, 14% in case of preferences, hobbies or interests and 5% in case of personal information such as their name or email address.

Recent studies regarding privacy related behavior on social networking sites also indicate the potential for serious privacy conflicts. Social networking sites (SNS) enable users to connect to other people, such as friends, and colleagues, or to meet new people. It enables people to send mails and instant messages, and to post personal information profiles including for example photos, video, images, and audio. Example networking sites are MySpace, Facebook or Hyves.

On social networking sites people may be tempted to give out more personal information than they would in real life. In a study by IT security firm Sophos 41% of the people gave a stranger complete access to their profiles including personal information such as email address, date of birth and phone number. By giving out such highly personal information people become more prone to identity theft (Sophos, 2007). Other risks on social networking sites are the distribution of personal information without one’s consent, for example due to other people posting photographs of you or passing on contact information from your online profile without your consent (Get Safe Online, 2007). Furthermore, employers could make use of the information in social networking sites in order to screen potential employees (OECD, 2007).

Even though social networking sites offer the possibility to adapt privacy settings to limit the availability of personal information to other people, many users choose to make their information publicly available (OECD, 2007). Some users are not even aware that this is the default setting. And others presume that only the people in their friendship network are able to see their personal details (Ofcom, 2008).

The examples described above, show there is a large body of evidence showing that people are very concerned about privacy in general and about privacy over the internet in particular. Concerns are dependent on the situation involved, e.g. the type of information influences people's willingness to disclose. People are less willing to provide sensitive information such as health or financial information, whereas they have less problems sharing information regarding their preferences or name. Other concerns relate to the possible misuse of their personal information, or the availability of data to other parties. Overall, many people feel that they have lost control over the collection and use of personal information by companies.

Development and validation of privacy models

Pedersen (1999) has developed a model for types of privacy by privacy functions. In this model the types of privacy are six different privacy behaviors (solitude, isolation, anonymity, reserve, intimacy with friends, and intimacy with family; Pedersen, 1979). Pedersen's model distinguishes five basic types of privacy functions or needs: contemplation, autonomy, rejuvenation, confiding and creativity. The model describes different ways in which people try to achieve privacy and it identifies the privacy needs that those privacy mechanisms fulfill.

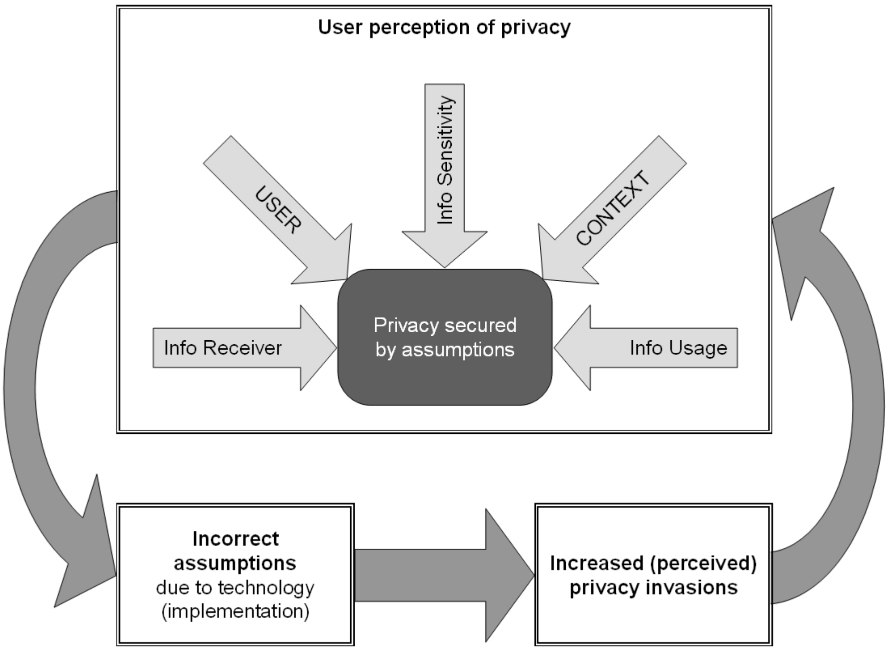
Adams and Sasse (2001) present a model of user perceptions of privacy in multimedia environments. The core of this model is the privacy invasion cycle which indicates that most invasions of privacy occur when users realize that a mismatch has occurred between their perceptions and reality. The privacy model by Adams and Sasse (2001) identifies 3 major privacy factors, which interact with each other to form the users' overall perception of privacy. These factors are the user's perception of (not necessarily actual):

- Information Sensitivity (the data being transmitted);
- Information Receiver (who receives and or manipulates their data);
- Information Usage (how their data is being used now or at a later stage).

Two other issues which are important but not specific to privacy are the User and the specific Context. They may influence the relative importance of the three privacy factors (see Figure 1.1).

The privacy model and invasion cycle by Adams and Sasse (2001) do not help to make predictions about user behavior; instead they describe the mechanism by which privacy invasions occur. Adams and Sasse (2001) did not formulate the model in an attempt to prove it; instead the model emerged by analysis of both qualitative and quantitative data collected by the authors and others. Except from expert evaluations of the model (reported in Adams, 2001), no formal validation has been attempted. The model provided by Adams and Sasse (2001) is quite different from the privacy regulation process as described by Altman (1975). The latter is much more pointed towards control by the individual, whereas in the former privacy is almost seen as something that cannot be controlled by the user (the user can only try to make accurate assumptions about the three privacy factors involved). However, both views support the influence of the individual (user) and the context involved on the perception of privacy.

Figure 1.1. Privacy invasion cycle (adapted from Adams & Sasse, 2001)


User perception of privacy
USER
Info Sensitivity
CONTEXT
Info Receiver
Privacy secured by assumptions
Info Usage
Incorrect assumptions due to technology (implementation)
Increased (perceived) privacy invasions

Dinev and Hart (2003, 2006) have evaluated two models that assess the trade-offs between the perceived personal benefits and privacy costs associated with Internet use in conducting e-commerce transactions. The 2006 study concerned a survey where participants were asked to rate various statements. It was found that the three factors most strongly related to the willingness to provide personal information were Internet privacy concerns, Internet trust, and personal Internet interest. The 2003 study was a similar survey. In this study the strongest relation was found between trust and Internet use.

The Technology Acceptance Model (TAM) by Davis et al. (1989) models how users come to accept and use a new technology by a number of influencing factors such as Perceived Usefulness and Perceived Ease of Use. Some extensions of TAM have been suggested that incorporate (privacy) risk as well. Featherman and Pavlou (2003) include various types of risk in their extension of TAM for e-services adoption. One of these risk facets is privacy risk. Featherman and Pavlou conducted a study in which participants first had to carry out a task with a demonstration website, which was then followed by a questionnaire. The model by Lui and Jamieson (2003) is an extension of TAM for an Internet-based business-to-consumer electronic commerce system and incorporates multiple dimensions of trust and risk perceptions. This model does not specifically include privacy risk, but it is covered by the general risk statement “Overall, I am concerned about experiencing some kind of loss if I transact with this system” and trust statement: “I believe the retailer is concerned about consumer privacy.” In their study participants are first provided with a scenario providing an intention to buy an item from an existing website, which was followed by a questionnaire.

Acquisti (2004) takes a different approach to modeling privacy behavior, namely one from an economic perspective. His paper shows that there are several difficulties that hinder any model of privacy related decisions based on full rationality. The paper also explains why even privacy concerned individuals do not protect their personal information. Apart from the fact that information to make good decisions is often lacking, individuals do not base their decisions on rationality. Even if there would be sufficient information, consumers are likely to trade off long-term privacy for short-term benefits. Therefore, Acquisti proposes that behavioral models based on immediate gratification bias can better explain the discrepancy between attitudes and behavior.

Chellappa and Sin (2005) develop a model to predict consumers' usage of online personalization as a result of the tradeoff between their value for personalization and their concern for privacy. Their study is based on a survey measuring participants level of agreement with various statements. They found that a consumer's intent to use personalization services is positively influenced by her trust in the vendor.

Most of the studies and models described in this section address privacy concerns related to Internet use. There is a lack of models describing the perception of privacy in more complex environments, such as those based on Ambient Intelligence. Therefore this thesis will focus on privacy perception of people in an Ambient Intelligence context, and a model for the acceptance of privacy interfaces for Ambient Intelligence technologies will be proposed and investigated.

1.2.4 Guidelines on privacy issues

A large body of work in the area of privacy and Ambient Intelligence has aimed at generating guidelines for addressing privacy issues. This work, to which this thesis also contributes, has its origins in attempts by scholars and activists in the 60's to institute a legislation framework for the management of personal information stored in databases with personal information on US citizens that were becoming widespread in the 60's.

Westin's section on "The computer and privacy" in his book "Privacy and freedom" (1967) provides the basis for the "Fair Information Practices". These Fair Information Practices were first articulated in a comprehensive manner in the United States Department of Health, Education and Welfare's report entitled *Records, Computers and the Rights of Citizens* (1973). In this report the fundamental principles of Fair Information Practice are described as follows:

1. There must be no personal-data record-keeping systems whose very existence is secret.
2. There must be a way for an individual, to find out what information about him is in a record and how it is used.
3. There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.
4. There must be a way for an individual to correct or amend a record of identifiable information about him.
5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.

The Privacy Act of 1974, which is public law, led to the installment of the Privacy Protection Study Commission. The aim of this commission was to study privacy issues and recommend future legislation. In the report of the Privacy Protection Study Commission (1977), the five existing principles (see indication in parentheses) were further refined to a total of eight principles. The principles in the report of the Privacy Protection Study Commission are:

1. *Openness Principle*: There shall be no personal-data record-keeping system whose very existence is secret and there shall be a policy of openness about an organization's personal-data record-keeping policies, practices, and systems (FIP1).
2. *Individual Access Principle*: An individual about whom information is maintained by a record-keeping organization in individually identifiable form shall have a right to see and copy that information (FIP2).
3. *Individual Participation Principle*: An individual about whom information is maintained by a record-keeping organization shall have a right to correct or amend the substance of that information (FIP4).
4. *Collection Limitation Principle*: There shall be limits on the types of information an organization may collect about an individual, as well as certain requirements with respect to the manner in which it collects such information (Addition to FIP).
5. *Use Limitation Principle*: There shall be limits on the internal uses of information about an individual within a record-keeping organization (FIP3).
6. *Disclosure Limitation Principle*: There shall be limits on the external disclosures of information about an individual a record-keeping organization may make (FIP3).
7. *Information Management Principle*: A record-keeping organization shall bear an affirmative responsibility for establishing reasonable and proper information management policies and practices which assure that its collection, maintenance, use, and dissemination of information about an individual is necessary and lawful and the information itself is current and accurate (FIP5).
8. *Accountability Principle*: A record-keeping organization shall be accountable for its personal-data record-keeping policies, practices, and systems (Addition to FIP).

The Organization of Economic Cooperation and Development (OECD) have covered the same eight principles though in a slightly different form in their OECD guidelines (OECD, 1980). The same holds for the EU Directive 95/46/EC on the protection of individuals with regard to the processing of personal data (European Parliament, 1995). The EU Directive is however much more extensive since it specifies various special occasions and exceptions. The OECD guidelines will be presented in more detail in chapter 3.

Many publications on privacy concerns in personalized environments refer to (some of) these legal guidelines. For example Langheinrich (2001) discusses some existing legal guidelines and presents his list of guidelines as areas of innovation and system design that future research in ubiquitous computing will need to focus on. Cranor (2004) refers to the OECD principles since she recognizes it as a useful framework for analyzing privacy issues related to e-commerce personalization. Lederer et al. (2002) indicate that particularly notice and consent are important to end-users concerned with the collection of personal information in a Ubiquitous Computing environment. They explain that notice and consent are the means by which a user gains feedback from and exhibits control over the privacy-sensitive aspects of a Ubiquitous Computing system. The Fair Information Practices have also informed the definition of the five characteristics of the design framework for Ubiquitous Computing systems (history, feedback, awareness, accountability, and change) by Nguyen and Mynatt (2002).

While the Fair Information Practices are used to guide design or research, hardly ever do related studies involve users in evaluating the effectiveness of such measures for the prevention of privacy concerns (except perhaps the work by Culnan & Armstrong, 1999, who studied the effect of complying with Fair Information Practices on the privacy concerns of users).

1.2.5 Technological advances to protect privacy

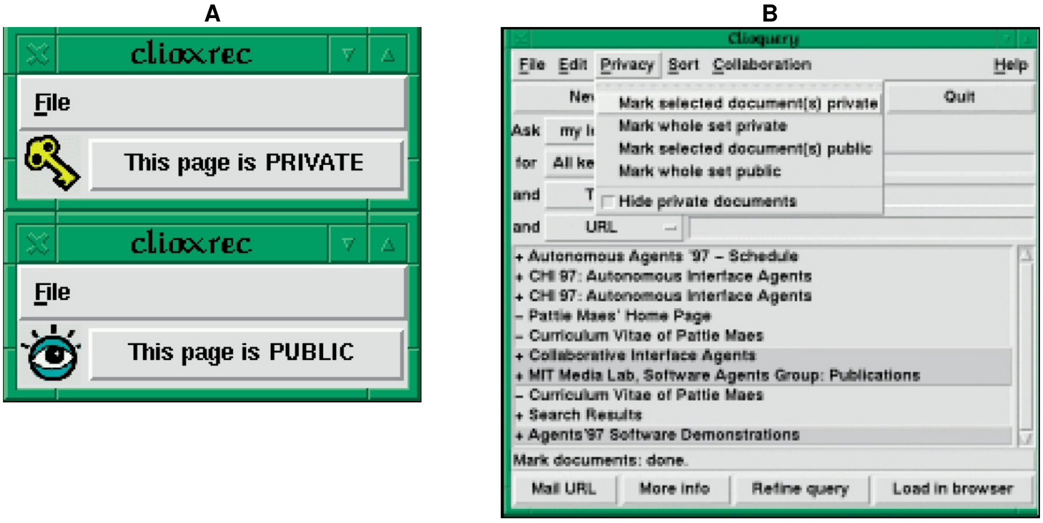
As mentioned before, the very nature of the task of managing personal information will change with Ambient Intelligence. Managing information disclosure will even become more frequent, more encompassing and more complex. For this reason, specialized technologies have been developed that aim to assist users in protecting their privacy. The remainder of this section is concerned with interaction technologies (rather than security technologies) that allow users to be aware of and control the disclosure of their personal information.

Privacy policies are known to be difficult to comprehend by users (Jensen & Potts, 2004; Milne & Culnan, 2004). The World Wide Web Consortium (W3C) developed a standard computer-readable language for website privacy policies (P3P), in an attempt to offer a solution to the difficulty of reading and understanding privacy policies. P3P 'user agents' may check for P3P policies at websites that a user visits and compare them with the users' previously specified privacy preferences. Finally they can provide feedback to the user about these policies (Cranor et al., 2006). This type of technology was an attempt by the industry to allow self-regulation of the market. Rather than introducing legislation, as suggested by for example Garfinkel (2000) and Culnan (2000), companies went for supporting a standard way to describe policies namely P3P. The argument was that if users can read and understand policies, they can adjust their internet usage behavior accordingly. Eventually companies could benefit from a competitive edge by offering more advantages to their users through this machine-readable privacy policy. An important obstacle for this approach however, is to make privacy policies understandable to the broad public since, users need to be able to specify their personal preferences with regard to privacy policies.

A P3P related example is the concept of Privacy Critics by Ackerman and Cranor (1999). Privacy Critics provide feedback to users, and do not necessarily take action on their own. Privacy Critics would help (instead of automate) the user's control over private information. Several Critics can be created by users in order to watch different phenomena. Each Critic can check on a different facet of a problem domain and user goal. Users can turn these Critics off and on, set threshold levels, and decide what aspects of privacy they want to guard. No user evaluation was performed with Privacy Critics. The user interface for defining a Privacy Critic is not presented in the paper by Ackerman and Cranor (1999).

Lau et al. (1999) developed a tool called Record Light that could indicate which website visits ought to be considered private or public by the system (see Figure 1.2A). Furthermore, a Search-and-Mark tool could be used to change previously made decisions (see Figure 1.2B). However, these settings were not taken into account for future visits to the same website, instead subsequent website visits were classified according to the actual setting of the Record Light. The tools turned out to be confusing, and laborious for users despite the fact that only one single click was required while visiting websites.

Figure 1.2. The record light and search-and-mark tool (Lau et al., 1999)



+ Autonomous Agents '97 – Schedule
+ CHI 97: Autonomous Interface Agents
+ CHI 97: Autonomous Interface Agents
– Pattie Maes' Home Page
– Curriculum Vitae of Pattie Maes
+ Collaborative Interface Agents
+ MIT Media Lab, Software Agents Group: Publications
– Curriculum Vitae of Pattie Maes
+ Search Results
+ Agents'97 Software Demonstrations

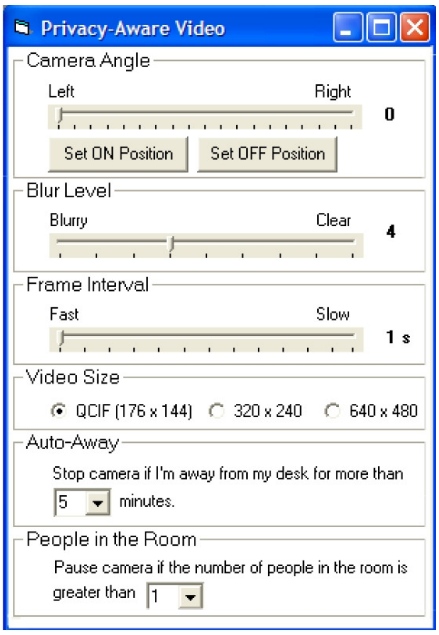
Mark documents: done.

Note: Figure A shows two record light windows. The top window is displayed when the record light is toggled to PRIVATE, the bottom when it is set to PUBLIC. Figure B shows the interface for the search-and-mark tool. The lower half of the window displays the results of a search; titles of recently browsed Web pages are prefixed by their classification into public (+) or private (-); The user is about to select a menu option that will mark the selected documents as private.

Langheinrich (2002) also developed a system based on P3P. The scope of his Privacy Awareness System (paws) is aimed to provide users of ubiquitous computing environments with what he calls a privacy-enabler, instead of a tamper-proof privacy-protector. The system is meant to help others respect one's personal privacy, to enable users to be aware of their own privacy, and to rely on social and legal norms to protect users from possible wrongdoers. This system is based on machine readable privacy policies. Users can specify their privacy preferences by using a machine readable privacy language. Data collectors also have to state in machine readable policies the details about the information collection, such as who is collecting data, what data is collected and for what purpose. Privacy proxies will handle all privacy related interactions between users and data collectors. Whenever data is (either explicitly or implicitly) collected from the user it is stored in a database together with each individual privacy policy related to it. The database takes care of following the privacy policy's promises with respect to the storage duration, usage, and recipients of information. It can also provide users with a detailed "usage log" of their personal information. Since no user interface was developed, the system was not evaluated in a user study.

Lederer, Hong, et al. (2003) propose the use of a 'faces' metaphor for the individual's privacy management. In this system privacy preferences are grouped into several 'faces' which are considered to be appropriate for different circumstances. Each face represents a number of dimensions such as what data to disclose and at what accuracy. A lab-based experiment which combined scenarios with the use of the prototype was performed. The evaluation required participants to set their preferences for a couple of instances. Later they were asked to tell what information they thought would have been disclosed in each of the instances. Furthermore, they were asked what they would have wanted to disclose in retrospect. The interface and evaluation of the 'faces' metaphor will be discussed in more detail in chapter 4.

Figure 1.3. Configuration window for Home Media Space attributes (Neustaedter & Greenberg, 2003)



Privacy-Aware Video

Camera Angle

Left Right 0

Set ON Position | Set OFF Position

Blur Level

Blurry Clear 4

Frame Interval

Fast Slow 1 s

Video Size

● QCIF (176 x 144) ○ 320 x 240 ○ 640 x 480

Auto-Away

Stop camera if I'm away from my desk for more than 5 minutes.

People in the Room

Pause camera if the number of people in the room is greater than 1

Neustaedter and Greenberg (2003) have developed a system which provides telecommuters privacy feedback and control mechanisms by audio and visual feedback, and explicit and implicit control elements. The system allows telecommuters to set their privacy preferences on the spot (see Figure 1.3). One of the authors evaluated the system. For this no formal evaluation approach was used, instead an overview of design faults that were discovered are presented in the paper by Neustaedter and Greenberg (2003).

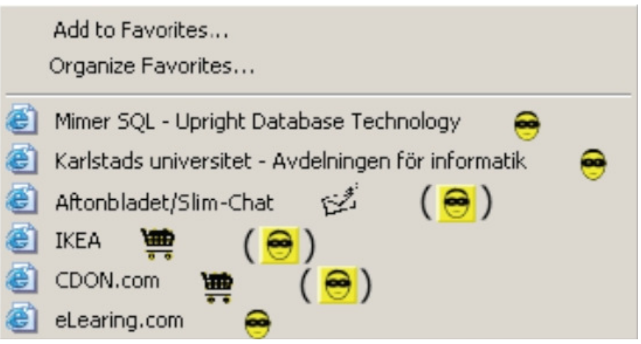
Kobsa (2003) presents a software architecture that encapsulates different personalization methods in individual components and tries to find an optimum between anticipated personalization effects and currently prevailing privacy constraints.

Privacy Bird (Cranor et al., 2006) is a P3P user agent that analyses web site policies as the user connects and downloads web pages. It compares P3P policies against a user's privacy preferences and assists the user in deciding whether to disclose data to a website. A bird icon changes shape and color to indicate whether a website is P3P-enabled, and (if that is the case) whether its privacy policy matches the user's privacy preferences.
A privacy preference specification interface for Privacy Bird allows users to select their preferred level of privacy (low, medium, high or custom). This interface is layered so that users are able to quickly configure their settings without giving up the ability to control the details. When a user selects one of the default settings, the interfaces displays the accompanying settings. This provides immediate feedback about what each of the settings does and makes it easy for users to modify the default settings. This interface will be discussed in more detail in chapter 4.
Privacy Bird is evaluated by Cranor et al. (2006) in the form of a user survey, a laboratory study, and an evaluation of 11 design criteria based on the framework for privacy by Bellotti and Sellen (1993) or Bellotti (1997). Following these criteria is meant to provide users with feedback and control over information collection, usage and

storage in various environments such as computer mediated communication, computer supported collaborative work, and ubiquitous computing. According to Bellotti and Sellen systems should be trustworthy and meaningful. They should support perceptibility, unobtrusiveness, and minimal intrusiveness. They should use appropriate timing, offer flexibility, yet require low effort on behalf of the user and have high learnability. Furthermore the framework advices low cost and failsafe systems.
In the laboratory study three approaches (Privacy Bird, Internet Explorer 6 and reading privacy policies) were compared (Cranor et al., 2006). Based on these studies Privacy Bird was found to be useful and usable. For example the use of Privacy Bird caused people to change their online behavior such as providing less information or visiting sites with better privacy policies. Participants also indicated that it was easier to find information using the Privacy Bird than by reading website privacy policies themselves. However, the biggest disadvantage of P3P based system such as Privacy Bird is its limited use due to the fact that most websites are not P3P-enabled or have technical errors in their P3P policies (Byers et al. 2003).

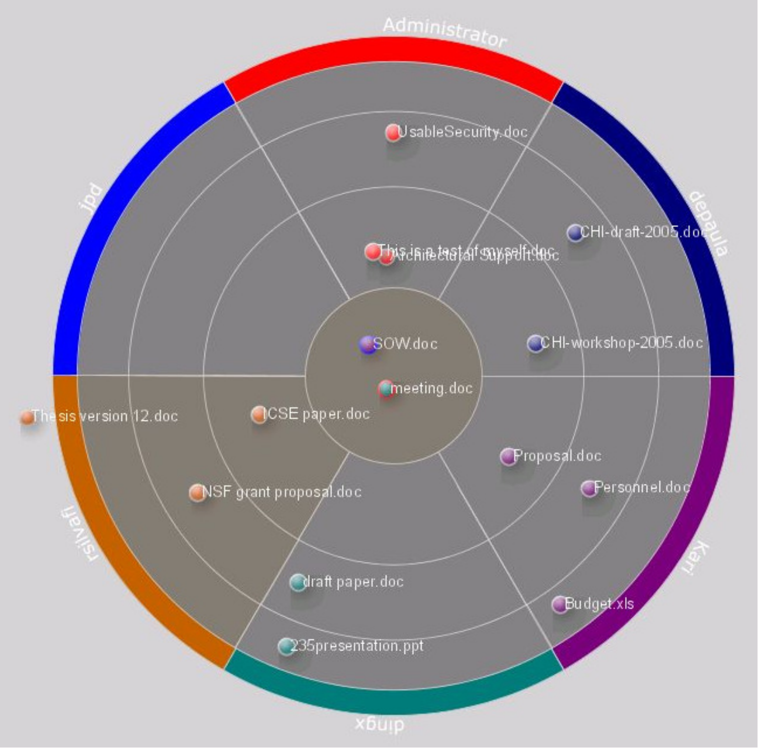
The PRIME project (Pettersson et al., 2005) proposes three different UI paradigms to allow the user to specify privacy preferences in the context of electronic communication: the Role-centred approach, the Relationship-centred approach and TownMap. The Role-centred paradigm provides user control of data disclosure via ‘roles’. The user can set and utilize different disclosure preferences for different data types by using these roles (see Figure 1.4). The user can select the role of choice when navigating online. This approach is similar to the concept of faces by Lederer, Hong, et al. (2003). In the Relationship-centred UI paradigm privacy preferences are defined in relation to each communication partner. Each communication partner can have different roles attached to them besides the default anonymous role. The usability of both tools was assessed by means of usability evaluations and questionnaires (focusing among others on interpretation of the icons, factors influencing user trust in the tool, and comprehension of users actions). The TownMap, is an attempt to make preference settings more accessible and understandable to users. Different areas represent different privacy protection concepts. There are three predefined areas with different default privacy options: the Public area (where by default a new pseudonym is used for each transaction), the Neighbourhood and Work area (both use pseudonyms in relation to specific communication partners). The idea is that the approach to use different default

Figure 1.4. Favorites list with icons for roles (Pettersson et al., 2005)


Add to Favorites...
Organize Favorites...
Mimer SQL - Upright Database Technology
Karlstads universitet - Avdelningen för informatik
Aftonbladet/Slim-Chat
IKEA
CDON.com
eLearing.com

Note: If multiple icons are displayed next to a ‘favorite’ then the user can select in which role he or she wants to visit a website. The anonymous role can be selected by clicking the masked man. The other two icons represent other roles. Clicking on the name of a favorite website implies selecting the first role listed.

Figure 1.5. The Impromptu interface (Rode et al., 2006)



Note: The circle corresponds to the shared workspace in which each section corresponds to a single user's area of the shared workspace.

'roles' for different areas within a town will make it easier for a novice to see the options available once he or she has grasped the TownMap metaphor. The TownMap was not used for a formal evaluation, except for a preference test.

Rode et al. (2006) propose and test an interface called Impromptu (see Figure 1.5) which allows users to set access rights to documents, and which reflects access and use of documents by other users. Files are represented by dots and are placed in and around a circular region. A unique color is assigned to each user's area, files and indicators of activity. The closer the files are towards the center the 'more shared' they are. Files outside the circle are not shared at all, but available to the local user only. Files in the outer region are visible but not readable or writable to others. Files towards the center provide more access rights to others such as both reading and writing.

This section has provided an overview of diverse tools that are proposed to protect users' privacy. However these tools have not been extensively tested by users. In some cases the technical feasibility of the tools has been assessed, but not their efficiency in reducing privacy concerns of users. This omission shall be addressed in more detail in chapter 4 of this thesis.

1.3 RESEARCH SCOPE OF THESIS

1.3.1 Research problem

Personalized systems and Ambient Intelligence environments may store and aggregate large amounts of personal data. The use of personal and sensitive data for adaptation, as well as permanent storage and possible transfer of profile data to other applications might be problematic due to the lack of control experienced by the user. These points are stressed frequently when Ambient Intelligence is discussed (see also section 1.1.3).

Studying privacy issues related to personalization and Ambient Intelligence is therefore of great importance for the adoption of these technologies by consumers. Research is needed in order to find solutions for the potential privacy problems (addressed in section 1.1.3). Such solutions will be crucial to the deployment and acceptance of Ambient Intelligence. The difficulties of finding solutions acceptable to end-users relate to:

- The volume of information that may be collected. Information was previously collected manually, but with Ambient Intelligence there will be a continuous stream of data collection from any location.
- The personal nature of this information. Information may be collected anytime, anywhere and even without the user's awareness, and may include detailed recording of user behavior. Even information that may at first not seem very personal or sensitive could become so anyway due to aggregation of multiple sources of information, or due to availability of the information in a different context.
- The general availability of the information stored in various interconnected locations. Previously information was stored into separate databases (few and far apart), but Ambient Intelligence provides the ability to integrate data repositories and easily access them through the internet. With this comes the risk of data being available to unintended parties. Overall, the distribution and use of personal data become much easier.
- User control. Ambient Intelligence may give people the impression of limited freedom and choice. People do not want to be controlled by a system, but instead want to be able to decide for themselves. For example users may want to balance the need for sharing privacy sensitive information (for instance with other people or appliances) and the need for keeping this information secret.
- The invisibility of data collection and consequently the difficulties for users to conceptualize what information is collected and how this information may be used or abused. Information may be collected anytime, anywhere and even without the user's awareness. Information may for example be accessible in another context, by unintended parties, or for unintended purposes.

The differences between an off-line and Ambient Intelligence environment make privacy a pressing concern, and can change the nature of the task of managing one's own information. Perhaps in the 70's the decision to disclose information may have been performed with a frequency of a year, and by sending in a signed written form. Now it becomes a daily, or even more frequent, decision because of the amount of traces that are left behind. The use of various cards with personal identifiers in shops or while travelling, the use of electronic forms of communication such as e-mail or instant messaging, the use of internet and mobile telephony involve the disclosure of information almost continuously. Being able to manage the disclosure of personal information and thus to control one's privacy is of major importance in such an environment.

However, as mentioned before, despite the key role of privacy for the acceptance of personalization and Ambient Intelligence technologies, few empirical studies have been conducted to fully understand the phenomenon and to support the development of appropriate solutions. This thesis focuses on the privacy concerns of users that are due to adaptation or personalization in the context of Ambient Intelligence. The aim of this thesis is to suggest potential solutions to provide protection of people's privacy in Ambient Intelligence environments. One way to obtain this could be by reducing or omitting these privacy concerns. That the problems of privacy in Ambient Intelligence or personalization relate to the management of personal information is manifested already in the domain of personalization for web applications. Therefore, in this thesis, empirical studies are either concerned with Ambient Intelligent scenarios or with actual use of personalized web applications.

The methodological problems concerning privacy research addressed before occur in many studies of privacy in the domain of computer-mediated communications, Internet use and Ambient Intelligence. Relying solely on either self-reported attitudes or behavior will not provide a complete and realistic picture. Studies of privacy restricted to laboratory experimentation or surveying opinions lack external validity in the absence of actual risk and a realistic context of use. Field observations of the actual use of a system can disguise many of the privacy concerns people may have despite demonstrated risk-taking behavior and do not offer sufficient controls for the privacy risks and the benefits of the disclosure. Therefore, there is a need for a method of investigation that provides a thorough understanding of both the factors causing people's privacy concerns and their behavior. A better understanding of the factors and situations that evoke privacy concerns is important primarily to be able to reduce user concerns and enhance trust. Another important focus of privacy research is on the consequences of user concerns. Understanding the attitudinal and behavioral reactions that result from privacy concerns is important in order to be able to judge the importance of dealing with privacy concerns.

The aim of this PhD project is three-fold. First of all, it aims to provide knowledge about the user perception of privacy in personalized or Ambient Intelligence environments. This obtained insight is used to support the second aim of this thesis: to provide design guidance through user evaluations for interaction solutions for the management of personal information disclosure. Finally, though not an initial aim of this thesis, the research for this thesis provides insight into appropriate methodology for research into both of these areas.

This thesis addresses the following four research questions in the context of personalization and Ambient Intelligence:

1. What are people's information privacy concerns?
2. What influences people's information disclosure behavior?
3. How to communicate privacy consequences?
4. How to design privacy interfaces?

The approaches used to address these research questions will be discussed next.

1.3.2 Research approach

This thesis provides guidance on how to design privacy interfaces that allow users to specify their preferences with regard to disclosure of personal information in the context of Ambient Intelligence and personalization. An important first step is to study user attitudes and behaviors, and later to evaluate how people react to different privacy interfaces in order to find out which approach works best to design a privacy interface. For this reason, surveys and observations of behavior are conducted as well as evaluations of different design concepts. This thesis will describe field experiments where participants used a personalized service making privacy choices, interviews and questionnaires surveying user attitudes in relation to privacy guidelines, and an evaluation study of user interfaces for privacy management. The different approaches applied in the context of this thesis will be discussed below.

In this thesis different approaches were used in order to obtain a rich view on people's privacy concerns in an Ambient Intelligence environment. Methodological triangulation is applied; which involves the use of two or more methods of data collection within the same study. Both within- and between-method triangulation (Denzin, 1970) is used; multiple scales are used to measure privacy attitudes in questionnaires and different methodologies are used to study users' perception of privacy.

Both laboratory and field studies were performed. Field studies may provide a more natural setting for use. In contrast, laboratory studies require participants to come to a specific place that is less familiar to them. Laboratory studies are more suitable for short studies and allow more control over the way people participate in the study, e.g. timing, possibilities to interact with the experimenter. Studies of privacy which are restricted to laboratory experimentation or surveying opinions might lack ecological validity in the absence of actual risk and because they are conducted outside a realistic context of use.

Especially with the topic of privacy it is important to move beyond surveys and interviews, due to the discrepancy between reported attitudes and actual behaviors as mentioned before. Hence, in this thesis participants were provided with applications that were actually used in order to obtain a realistic experience, and to be able to judge consequences with regard to privacy. Since presence of the experimenter may influence's people's behavior, in this thesis the experimenter was never present while participants were using the applications.

All studies consisted partly of surveys, with a combination of open and closed questions. Closed questions cost less time for the participant to answer and are suitable when there is some knowledge about the type of answers one can expect (Emans, 1990), or when there is a clear idea about the issues one wants to address. Open questions, on the other hand, are more time-consuming, yet they are an ideal way to avoid influencing participants (e.g. there is no answering category pointing them to privacy issues, so they have to come up with this topic themselves).

In some of the surveys pairwise comparison was used. This technique requires participants to compare two alternatives at the same time, instead of evaluating them consecutively. The advantage of pairwise comparison is that participants consciously have to compare two alternatives (with regard to a certain aspect). In contrast, when alternatives are evaluated individually no conscious comparison is made, which could lead to unnecessary ties in participants' judgments.

Interviews were also conducted in the context of this thesis, since interviews allow a deeper level of understanding to arise. In interviews it is possible to ask for immediate clarification or further explanation of an answer that is given by a participant. The interviews in this thesis were conducted in a semi-structured way. This technique allows the interviewer to make sure that all necessary topics are addressed, yet the order of topics is not fixed in semi-structured interviews. In this way interviews approach the spontaneity of a natural conversation (Black & Champion, 1976) and may feel less as an interrogation. Consequently, it may be perceived as more pleasurable.

There were some other considerations in setting up the studies of this thesis. For privacy it is important to provide a context of use, since privacy perception is known to be context dependent (Consolvo et al., 2005; Lederer, Mankoff, et al., 2003; Sheehan, 2002; Adams & Sasse, 2001). In some of the studies in this thesis scenarios were used to provide participants with such a context. Since the aim of the surveys was to learn about people's privacy concerns and related behaviors it was important not to inform people about this topic, in order not to influence their perception of the manipulation. Within-subject designs were chosen in order to be able to compare different situations for one single participant.

1.3.3 Thesis outline and study motivations

Chapters 2, 3 and 4 present the empirical studies that were conducted in the context of this thesis. Table 1.1 shows an overview of the research questions that are addressed by the studies of these chapters. The contents of these chapters and the motivation for the studies performed will be discussed in more detail in the sections below.

Table 1.1. Overview of research questions addressed in each of the chapters

	Research question	Chapter
1.	What are people's information privacy concerns?	2, 3, 4
2.	What influences people's information disclosure behavior?	2, 4
3.	How to communicate privacy consequences?	3
4.	How to design privacy interfaces?	4

Study about privacy attitudes and behavior (chapter 2)

The first study, described in chapter 2, concerns an experimental field study. Due to the afore-mentioned complexity of privacy perception it was felt that a more realistic approach was needed than mere surveying of people's opinions. Therefore, an approach was chosen in which both actual privacy behavior and the underlying attitudes of users could be investigated.

For the purpose of this study a music recommender service was created. Participants' disclosure behavior in relation to this system was observed, further examined and combined with insights into underlying motivations based on questionnaires and interviews. Participants were free to use the experimental service at a time and place of their own convenience. They were able to listen to recommended music based on their personality traits or preferences for music genres. These two sources for music recommendations were used for their assumed difference in sensitivity (personality traits were assumed to be more sensitive than preferences for music genres) in order to create situations where different forms of privacy behavior may be appropriate.

In principle participants could use the service as any other music service. However, every day some events occurred on account of the experiment. Such events were rating the quality of the previous playlist, and answering a question about the disclosure and use of personal information. Besides providing music, the service took care of these experimental events as well. Then, after using the music service, participants were asked to answer a survey. With some participants an interview was conducted in order to obtain more in depth insight in their feelings and considerations.

Studies about privacy guidelines (chapter 3)

As described before in section 1.2.4, there exists a large body of work in the area of privacy and Ambient Intelligence regarding guidelines to address privacy concerns. However, few studies involve the user in evaluating the effectiveness of such measures to reduce or prevent privacy concerns. The studies about privacy guidelines, described in chapter 3, address this issue.

In total four studies regarding privacy guidelines were conducted. All of these studies took the form of a survey. First, two pilot studies were performed in order to assess people's understanding of the privacy consequences of system descriptions based on privacy guidelines. Since these pilot studies showed limited understanding of these descriptions, the statements were revised to improve people's comprehension. These improved textual descriptions were used in two follow-up studies: one to investigate the relative importance of the various privacy guidelines, and another in which the comprehension of video- and text-based descriptions of privacy guidelines was compared. The first follow-up study was conducted in order to investigate whether there are possibilities to further improve people's comprehension of privacy guidelines besides revising text. The second follow-up study aimed to contribute to the evaluation of the relative effectiveness of privacy guidelines for the prevention of privacy concerns in Ambient Intelligence environments. This was done by asking participants to evaluate desirability of possible adaptations in system features.

Study about privacy preference management (chapter 4)

The studies described in chapter 2 and 3 increased the level of insight into privacy behavior, privacy attitudes and relative importance of privacy guidelines. Although these studies provided some guidance for appropriate ways to design privacy interfaces, actual use and evaluation of privacy interfaces were lacking. Therefore, in the last study, described in chapter 4, a laboratory experiment was conducted in which three privacy interfaces based on different conceptual models for privacy preference management were used and evaluated by participants. In addition, a model was evaluated in order to investigate the impact of the perception of risk, trust, usefulness and ease of use on intention to use.

Conclusions (chapter 5)

Following the empirical study chapters, chapter 5 provides a recapitulation of this thesis. Then, it will reflect on the methodology used in this thesis, followed by directions for future research. Finally, this chapter is concluded with the contributions of this thesis.

2 Evaluation of Privacy Attitudes and Behavior

This chapter[5] presents an experimental study of privacy-related attitudes and behaviors regarding a music recommender service based on two types of user modeling: personality traits versus musical preferences. The study aimed to address the following questions:

- *What are people's information privacy concerns?*
- *What influences people's information disclosure behavior?*

Contrary to prior expectations and the attitudes reported by participants, personality traits were frequently disclosed to the system and even to other users, which indicates that embedded modeling of user personality does not represent an acceptance barrier.

Discrepancies between privacy attitudes and behaviors have been reported before in the context of e-commerce applications, but the corresponding studies could not exclude several conflicting hypotheses, such as participants expressing attitudes outside the context of specific privacy dilemmas, knowledge of participation in research and contact with researchers, which may have mitigated perceived privacy risks. It can be argued that these are fundamental problems in empirical investigations into privacy which apply to most published works relating to privacy and user modeling. Measures to control these factors in the current study are discussed and methodological suggestions for future research are presented.

[5] This chapter is based on the following publication: Garde-Perik, E. van de, Markopoulos, P., Ruyter, B. de, Eggen, J.H., & IJsselsteijn, W. (2008). Investigating privacy attitudes and behavior in relation to personalization. *Social Science Computer Review*, 26(1), 20-43.

2.1 INTRODUCTION

It was noted in chapter 1 how adaptive systems and personalized systems in particular rely on having appropriate and sufficient information about their users to operate optimally. This could, for example, include information about the identity of the user, earlier usage of a service, the user's preferences and dislikes, and many other types of data (Kobsa, 2001).

The collection and processing of such information can conflict with privacy concerns (Kobsa, 2002). More specifically, it has been suggested that privacy-related concerns are contingent upon:

- The kind of information collected (Adams & Sasse, 2001; Ackerman et al., 1999, Bellotti & Sellen, 1993);
- The degree of control users have over disclosure (Bellotti & Sellen, 1993; Olivero & Lunt, 2004; Günther & Spiekermann, 2005);
- The degree of accessibility (Bellotti & Sellen, 1993; Adams & Sasse, 2001);
- The way the information is used (Bellotti & Sellen, 1993; Adams & Sasse, 2001).

The methodological problems concerning privacy research addressed in chapter 1 occur in many studies of privacy in the domain of computer-mediated communications, Internet use, and Ambient Intelligence. Relying solely on either self-reported attitudes or behavior will not provide a complete picture of reality. Studies of privacy restricted to laboratory experimentation or surveying opinions lack external validity in the absence of actual risk and outside a realistic context of use. Field observations of the actual use of a system can disguise many of the privacy concerns people may have despite demonstrated risk-taking behavior and do not offer sufficient controls for the privacy risks and the benefits of the disclosure. There is a need for a method of investigation that provides a thorough understanding of both the factors causing people's privacy concerns and their behavior. A better understanding of the factors and situations that evoke privacy concerns is important primarily to be able to reduce user concerns and enhance trust. Another important focus of privacy research is on the consequences of user concerns. Understanding the attitudinal and behavioral reactions that result from privacy concerns is important in order to be able to judge the importance of dealing with privacy concerns.

This chapter presents an experimental study which was set up to provide users with realistic privacy dilemmas during the use of a personalized music recommender service. The music recommender service was created specifically for the purpose of this study in order to enable full control over the experimental conditions. Participants were presented with disclosure choices that were as realistic as possible. Logging of their behavior in these situations was combined with self-report and attitude measurements regarding privacy. The study enabled the testing of some of the assumptions regarding privacy and personalized systems and provided an opportunity to explore the motivation behind observed privacy behavior.

Two types of information were requested from participants as input to suggest music: personality traits and music preferences. The first assumption was that personality trait information would be regarded as more sensitive, resulting in a lower tendency towards disclosure compared to music preferences. Secondly, it was expected that showing profile information directly to other users would result in lower disclosure compared to use of the profile information by the system alone. Despite these expectations, it is important to realize that this study is of an explorative nature. Especially with regard to the underlying attitudes no hypotheses were formulated in advance. However, it was felt that the simultaneous investigation of attitudes and behavior with regard to disclosure of personal information is necessary to gain insight into the user's actual choices in disclosing privacy sensitive information, while taking into account the reported attitudes users claim to have in comparison to privacy-related behavior. This study is an attempt of getting a better understanding of attitudes and other influences on actual disclosure behavior.

The following section will describe the methodology used. Then, the research findings will be presented, followed by a discussion of the results in the light of other research. Finally, the conclusions of this study and implications for future work are addressed.

2.2 METHOD

This study involved participants using a music recommender service accessed through a web application over the Internet. Participants used this service from their own computers at work or at home, similar to any other Internet-based music recommender service. The system confronted the participants with privacy dilemmas relating to two types of personal information: preferences for different music genres and information about their personality.

Participants were asked to disclose this information to the recommender service and/or other users of this service. Rentfrow and Gosling (2003) have established a relationship between music preferences and personality traits which makes it feasible to recommend music based on personality traits. For example, someone who scores high in terms of the personality trait *Neuroticism* as well as *Openness to New Experiences* is likely to be interested in the 'Reflective & Complex' music dimension. Music genres that fall into this music dimension are Blues, Jazz, Folk and Classical Music (Rentfrow & Gosling, 2003).

The interest in contrasting these music preferences and personality traits comes from the relative legitimacy of these two approaches to user profiling for the purpose of recommending music. According to Iachello and Abowd (2005) an application is legitimate if the interest in using it for a specific purpose justifies the burden on individuals' rights. Music preference data are seemingly innocuous, but they are directly relevant to the Music Recommender and are commonly offered by users to systems of this kind. However, music preferences can be used for direct marketing, so they could also be considered to be somewhat sensitive by some users.

Personality traits are *more or less stable, internal characteristics of people, which make their behavior consistent from one time to another, yet different from the behavior that other people would exhibit in comparable situations* (Child, 1968). As a user modeling approach, personality traits have a lot of potential since they are domain independent and may be applied in a much wider range of contexts than music recommendation.

Conversely, a personality profile of a user can be misused and misapplied in a variety of contexts, for example by a prospective employer or a medical insurance provider. Storage of personality traits seems to have little legitimacy in the context of music recommendation, and therefore does not adhere to the principle of proportionality. This means that it does not balance the usefulness of the application and its effect on privacy (Iachello & Abowd, 2005). The difference in legitimacy between personality traits and music preferences is expected to lead to a difference in perceived sensitivity of the two types of information.

During the experimental study participants were confronted with choices regarding whether or not:

- To disclose personal information;
- Disclosure would be anonymous.

It was anticipated that personality trait information would be regarded as more sensitive, resulting in comparatively less disclosure than for music preferences. It was also anticipated that showing profile information directly to other users would result in less disclosure than if the profile information were used only by the recommender system and not shown to anyone else.

It is important to realize that this study is of an explorative nature, combining quantitative and qualitative methods. The underlying attitudes were measured in order to see whether existing instruments for assessing privacy attitudes would be good predictors of actual behavior. Furthermore, context-specific privacy preferences were surveyed and explanations for disclosure behavior considered; these were then analyzed qualitatively in order to explore the relationships between them.

2.2.1 Design

The music recommender service consisted of two separate music recommender systems: one based on music preferences and another based on personality traits. The study followed a ‘within subjects’ design whereby participants were exposed to profiling of both music preferences and personality traits. The order in which participants used the two recommender systems was counterbalanced. Participants could use the recommender systems at home or at work.

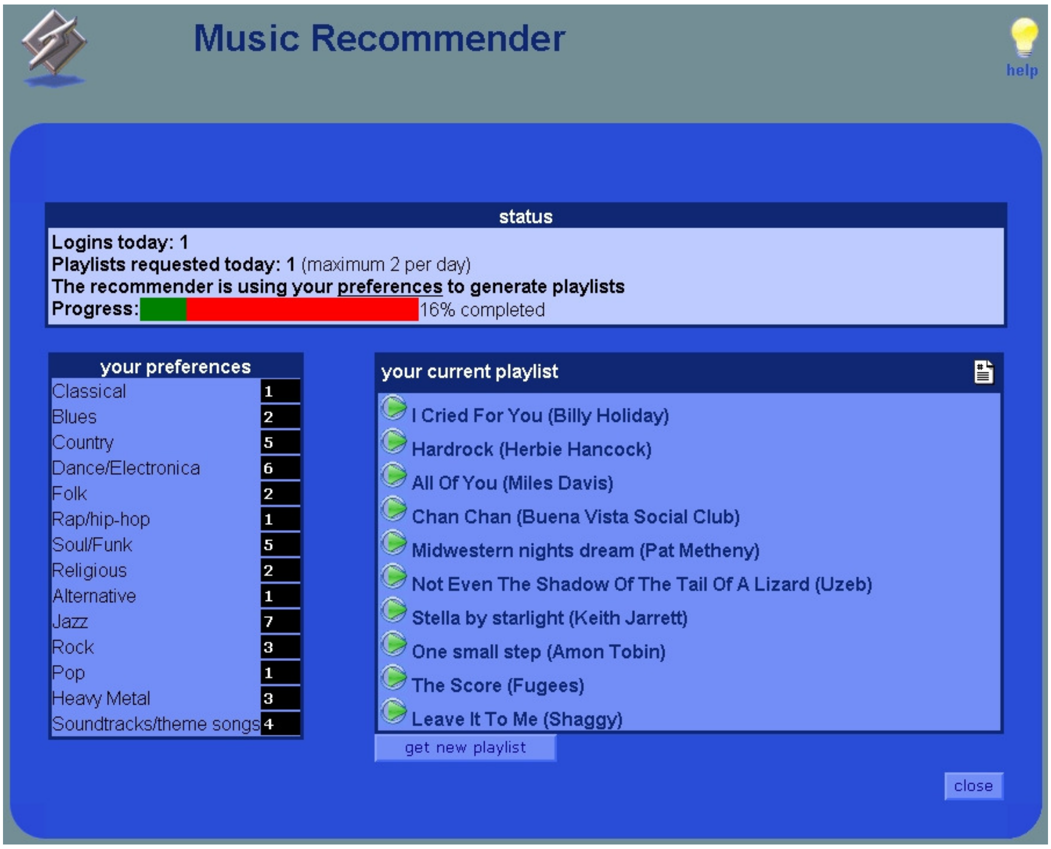
The study involved four disclosure choice moments. Two disclosures related to profile information and the other two related to personality traits. In both cases, participants were first asked to share information for comparison by the system (as in collaborative filtering, where profiles of users are compared in order to provide recommendations that are appreciated by one user to another user with a similar profile), and to then share the current profile information with other users (as in social networking sites). In each case, participants could choose between three levels of disclosure at these choice moments: no disclosure, anonymous disclosure or disclosure including identity information.

Data of both a qualitative and quantitative nature was collected: actual disclosure choices were monitored by system logs, explanations for these choices were gathered through questionnaires and interviews, and attitudes towards privacy and the use of personal information were measured by means of a questionnaire.

2.2.2 Participants

Participants were recruited by e-mail announcements via secretaries and bulletin boards within the Eindhoven University of Technology and the Philips Research Labs in Eindhoven. In view of the music collection stored in the available database, recruitment was aimed at participants in the 18 to 50 years age group. In total 48 participants took part in the study and completed the on-line questionnaire.

Figure 2.1. Screenshot of Music Recommender system based on preferences for music genres



status

Logins today: 1
Playlists requested today: 1 (maximum 2 per day)
The recommender is using your preferences to generate playlists
Progress: 16% completed

your preferences	
Classical	1
Blues	2
Country	5
Dance/Electronica	6
Folk	2
Rap/hip-hop	1
Soul/Funk	5
Religious	2
Alternative	1
Jazz	7
Rock	3
Pop	1
Heavy Metal	3
Soundtracks/theme songs	4

your current playlist

- I Cried For You (Billy Holiday)
- Hardrock (Herbie Hancock)
- All Of You (Miles Davis)
- Chan Chan (Buena Vista Social Club)
- Midwestern nights dream (Pat Metheny)
- Not Even The Shadow Of The Tail Of A Lizard (Uzeb)
- Stella by starlight (Keith Jarrett)
- One small step (Amon Tobin)
- The Score (Fugees)
- Leave It To Me (Shaggy)

As compensation for their time, participants were given a music CD selected on the basis of the songs recommended to them. This was done in order to motivate participants to be honest about their music preferences and personality traits, and served to increase the realism of both the costs and benefits of the disclosure they would make during the experiment.

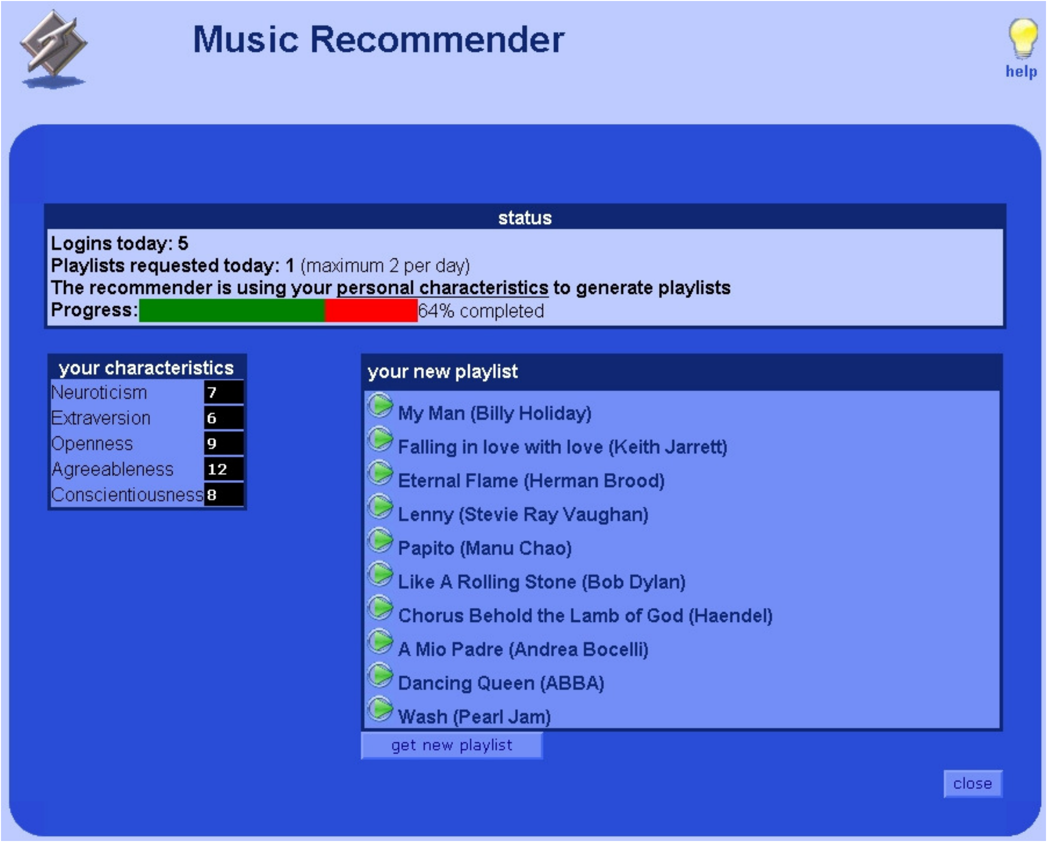
The ages of participants ranged from 17 to 49, with an average age of 26. Half of participants were 23 years old or younger. In total 21 participants were interviewed. Interviewee ages ranged from 19 to 49, with an average age of 27.

2.2.3 Apparatus and materials

The music recommendations were provided via a web-based application created for the purposes of this study. The service offered personalized playlists of songs. Streaming technology was used to make these songs available for participants to play on their computers. The experimental recommender service was built on a database of nearly 6000 songs spread evenly over 14 different music genres.

While using the personality-based recommender, participants could see a screen like the one shown in Figure 2.1. At the top of the screen a status bar shows the number of times the user has logged into the service, the number of playlists requested, the source of information on which the recommendation is based (*"The recommender is using your*

Figure 2.2. Screenshot of Music Recommender system based on personality traits



status

Logins today: 5
Playlists requested today: 1 (maximum 2 per day)
The recommender is using your personal characteristics to generate playlists
Progress: 64% completed

your characteristics	
Neuroticism	7
Extraversion	6
Openness	9
Agreeableness	12
Conscientiousness	8

your new playlist

- My Man (Billy Holiday)
- Falling in love with love (Keith Jarrett)
- Eternal Flame (Herman Brood)
- Lenny (Stevie Ray Vaughan)
- Papito (Manu Chao)
- Like A Rolling Stone (Bob Dylan)
- Chorus Behold the Lamb of God (Haendel)
- A Mio Padre (Andrea Bocelli)
- Dancing Queen (ABBA)
- Wash (Pearl Jam)

preferences to generate playlists"), and the progress within the study. On the left side of the screen an overview of the current profile information based on preferences for music genres is shown. The right side of the screen displays the current playlist. Below this playlist a button is displayed; this can be used to request a new playlist. The screen of the recommender based on personality traits is similar (see Figure 2.2), except that the status part stated: *"The recommender is using your personal characteristics to generate playlists"*. On the left side of the screen an overview of the music preference profile is shown.

2.2.4 Procedure

The procedure of the experimental study is shown schematically in Figure 2.3. Participants were sent instructions by e-mail. They were not informed in advance that the research related to privacy. Participants had to register on the Music Recommender website by providing their e-mail address. This was their business/university e-mail address, which consisted of their name and company. At the time of registration participants were assigned randomly to an experimental group (linked to a specific order in which they would experience the two recommender systems) and were sent a personal access code.

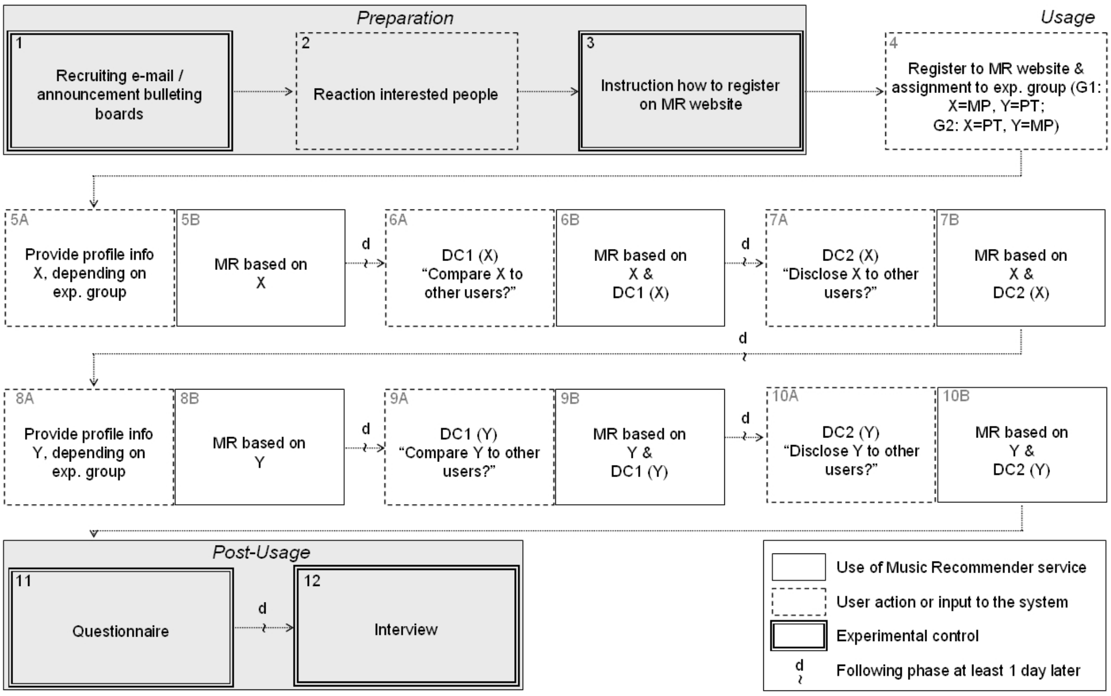
Participants were asked to access the portal site of the Music Recommender on six separate days within a period of 2-3 weeks. This time-frame was chosen first of all to ensure that participants would not rush through all phases of the study and as a consequence would not be able to distinguish between the different study phases. Secondly, the study would not last for too long and it will therefore enable participants to remember disclosure choices or underlying concerns afterwards. They were asked to listen to at least one playlist per day. If a participant had listened to a playlist the previous day, the participant was offered the next phase. The Music Recommender therefore served two purposes: it operated as a music recommender service and it also implemented the experimental procedure.

As indicated earlier, the order in which participants experienced the two recommender systems was counterbalanced. The first phase of both Music Recommender systems (boxes 5 and 8 in Figure 2.3) consisted of a default situation in which no additional disclosure of information was required (local use of the information only).

In the second phase (6A/9A in Figure 2.3), participants were asked to disclose their profile information for the purpose of collaborative filtering (for the participants this was referred to as *"comparing preferences to those of others users"* or *"comparing personality traits to those of others users"*).

In the third phase (7A/10A in Figure 2.3), participants were asked to disclose their profiles directly to other users. In this way, participants were asked to reveal an increasing amount of information.

Figure 2.3. Flowchart of phases in Music Recommender study


Preparation
1 Recruiting e-mail / announcement bulleting boards
2 Reaction interested people
3 Instruction how to register on MR website
Usage
4 Register to MR website & assignment to exp. group (G1: X=MP, Y=PT; G2: X=PT, Y=MP)
5A Provide profile info X, depending on exp. group
5B MR based on X
d
6A DC1 (X) "Compare X to other users?"
6B MR based on X & DC1 (X)
d
7A DC2 (X) "Disclose X to other users?"
7B MR based on X & DC2 (X)
d
8A Provide profile info Y, depending on exp. group
8B MR based on Y
d
9A DC1 (Y) "Compare Y to other users?"
9B MR based on Y & DC1 (Y)
d
10A DC2 (Y) "Disclose Y to other users?"
10B MR based on Y & DC2 (Y)
Post-Usage
11 Questionnaire
d
12 Interview
Use of Music Recommender service
User action or input to the system
Experimental control
d Following phase at least 1 day later

Note: MR= Music Recommender; G1/2= experimental group 1/2, MP= Music Preferences, PT= Personality Traits, DC= Disclosure Choice, X= first source for recommendations, Y= second source for recommendations.

In each of the three phases of using the two recommender systems the actual recommendation mechanism remained constant, but the percentage of recommendations that were offered according to the profile was designed to increase if users chose to disclose their profile information. This was done to ensure that the recommender performance would improve predictably when the user chose a higher level of disclosure (disclosure of profile information including identity information was considered the highest level of disclosure). This manipulation of the recommendation mechanism was not revealed to participants. Instead, participants were told in advance that the recommendations might improve as a result of their information disclosure. The intention was that without more information about the recommendation mechanism they would suppose that the data would actually be used for collaborative filtering and that improvements are due to disclosure. This was preferred over actual collaborative filtering as it could not be certain that disclosure would predictably lead to improved recommendations for the duration of this experiment.

In the first phase of both recommender systems, 80% of the recommendations were generated according to the user's profile. Depending on the choices made by the participant in the second and third phase (regarding whether to disclose and whether disclosure would be anonymous or not), the recommendation could improve, so that 90% or 100% of the recommendations were generated according to the profile. After they had used the Music Recommender, participants were asked to complete an on-line questionnaire with a combination of open and multiple-choice questions. Again, it was not revealed to the participants that the focus of the study was privacy.

Finally, 21 out of 48 participants were contacted to arrange an interview appointment after the completion of the on-line questionnaire. The individual interviews were set up in such a way as to achieve an open atmosphere in which participants would express their feelings freely. Interviewees were questioned in more detail about their choices during the study, and encouraged to give thorough explanations about the answers they had given in the on-line questionnaire.

2.2.5 Measures

Before participants could actually receive personally recommended playlists, they had to provide their first type of profile information (which depended on the experimental group they were assigned to). The second type of profile information was collected only after three days of using the first recommender system (see Figure 2.3). The profile information was collected by means of two short, validated measures: the Short Test of Music Preferences (STOMP) and the Ten Item Personality Measure (TIPI). Both measures are included in Appendix A1.

The STOMP test (Rentfrow & Gosling, 2003) inquires about the basic preference level for 14 different music genres on a scale from 1 (strongly dislike) to 7 (strongly like). It asks people to:

> *"please indicate your basic preference level for the genres listed using the scale provided".*

Example genres are 'country', 'jazz' or 'rock'. The STOMP values were used as a basis for music recommendations in the music-preference-based application.

The TIPI (Gosling et al., 2003) encompasses a personal judgment of the extent to which 10 pairs of personality traits apply on a scale from 1 (disagree strongly) to 7 (agree strongly). It gives people the following task description:

> *"Here are a number of personality traits that may or may not apply to you. Indicate (…) the extent to which you agree or disagree with that statement. You should rate the extent to which the pair of traits applies to you, even if one characteristic applies more strongly than the other."*

Examples of pairs of personality traits used in TIPI are 'reserved/quiet' or 'sympathetic/warm'. The TIPI scores were converted to the Big Five personality dimensions (i.e. Extraversion, Agreeableness, Conscientiousness, Neuroticism, and Openness to Experiences) and used as a basis for music recommendations in the personality-traits-based condition.

The Big Five personality dimensions are frequently used in personality assessments, although they are usually based on long questionnaires of sometimes more than 200 items that have to be rated. For the purpose of the personality-based Music Recommender system, it was felt that such a long questionnaire would take up too much time and effort for the participants.

The short TIPI test was created for situations where very short measures are needed or where personality is not the primary focus of interest. Both these conditions hold for this study so the TIPI was chosen as a personality inventory. Furthermore, since the length of TIPI and STOMP are quite comparable, participants were likely to have similar expectations about the use of the two types of profile information by the two different recommender systems (a 200-item questionnaire might raise the expectations of participants with regard to the accuracy of the music recommendations, and it would be likely to raise suspicion about other potential use of the information as well).

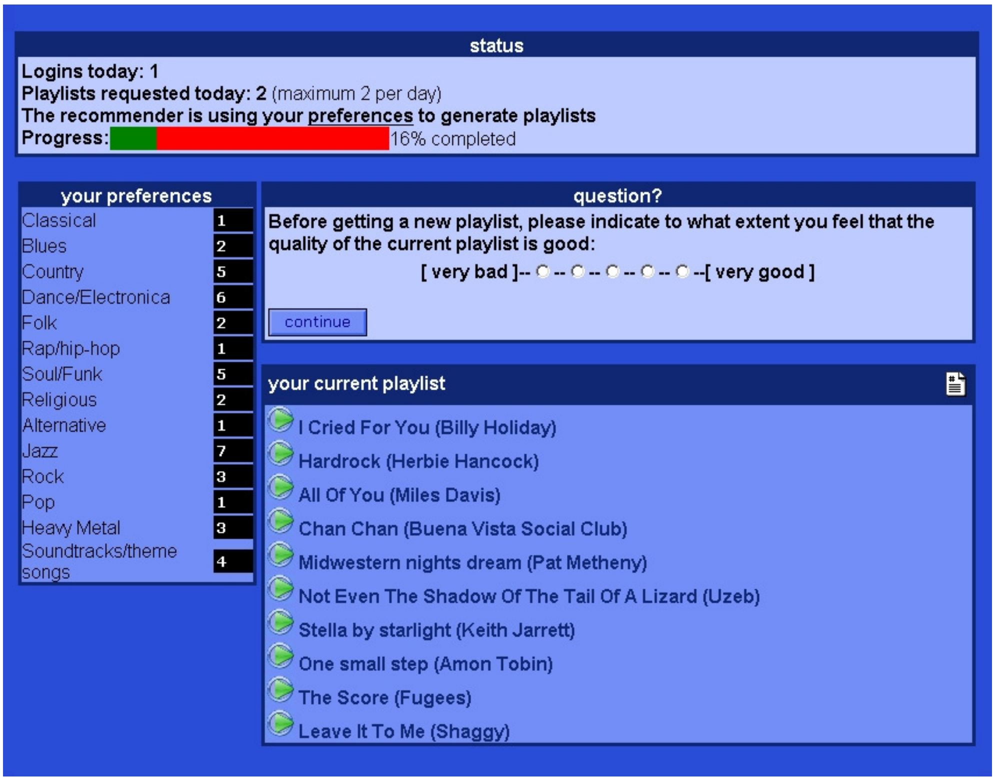
Whilst the Music Recommender was being used the actual level of disclosure chosen (no disclosure, anonymous disclosure, or disclosure including identity) in the four choice situations was recorded. This measure relates to the main aim of the research: to see whether participants would choose different levels of disclosure depending on the type of information involved (either personality traits or music preferences) and the use of the information (for comparison by the system or for showing directly to other users; see Appendix A1).

Besides their choice of disclosure, participants were also asked to rate the quality of each playlist of recommendations on a 5-point scale (see Figure 2.4). This quality rating was included to assess whether there was any relationship between the perceived benefits of the system and the disclosure behavior of participants.

After using the Music Recommender for six days, all participants were asked to complete an on-line questionnaire consisting of some open and some multiple-choice questions (see Appendix A2). This questionnaire served to collect demographic data from participants, as well as participants' opinions regarding the music recommender and various privacy statements. The questionnaire addressed the following topics:

- General demographics and interest in music (gender, age, function and expertise, amount of CD's and MP3 songs possessed, and frequency of listening to music from PC). These questions were included to get an impression of the background of participants and to verify whether they were interested in music.

Figure 2.4. Screenshot of question regarding quality rating of the playlist



status

Logins today: 1
Playlists requested today: 2 (maximum 2 per day)
The recommender is using your preferences to generate playlists
Progress: 16% completed

your preferences

Classical	1
Blues	2
Country	5
Dance/Electronica	6
Folk	2
Rap/hip-hop	1
Soul/Funk	5
Religious	2
Alternative	1
Jazz	7
Rock	3
Pop	1
Heavy Metal	3
Soundtracks/theme songs	4

question?

Before getting a new playlist, please indicate to what extent you feel that the quality of the current playlist is good:

[very bad]-- ○ -- ○ -- ○ -- ○ -- ○ --[very good]

your current playlist

- I Cried For You (Billy Holiday)
- Hardrock (Herbie Hancock)
- All Of You (Miles Davis)
- Chan Chan (Buena Vista Social Club)
- Midwestern nights dream (Pat Metheny)
- Not Even The Shadow Of The Tail Of A Lizard (Uzeb)
- Stella by starlight (Keith Jarrett)
- One small step (Amon Tobin)
- The Score (Fugees)
- Leave It To Me (Shaggy)

- General appreciation of the Music Recommender. Participants were asked to indicate which elements they liked or disliked. These measures were included to see whether participants received benefits from the service or not, and which of the two recommender systems was preferred.
- Attitudes towards disclosing music preferences and personality traits. Participants were asked to reflect on the initial disclosure of music preferences and personality traits to the system. They were asked to indicate whether they worried about the access of this information by other people and a music content provider. The amount of effort involved in the disclosure of these to types of information was measured, as well as the quality of the recommendations for the different types of recommenders. These measures were included to see whether participants felt there was a difference between the two types of information.
- Explanations for the level of disclosure chosen during and after the study (open question). These questions were posed to see whether people's experience of using the recommender would lead them to make different choices afterwards (e.g. due to disappointing benefits or any privacy concerns they had).
- General privacy attitude measures were taken in order to see whether they would explain any differences in disclosure behavior. Privacy attitudes were measured by different tools: the Privacy Segmentation Index (PSI) (Harris Interactive, 2002) and the Privacy Attitude Questionnaire (PAQ) (Chignell et al., 2003). In addition to these tools, some general questions regarding privacy (e.g. "I like to get advance notice if information is collected about me", or "I am willing to provide personal information in return for low-cost products or convenience") and four questions about the worries

concerning the disclosure of personal information in different situations were included.

The PSI consists of three statements about the use of personal information by organizations. Participants have to judge the extent to which they agree with each of these three statements. This tool was included because of its brevity, and because this type of clustering is widely used in HCI research (Ackerman et al., 1999; Berendt et al., 2005, Consolvo et al., 2005).

The PAQ consists of 36 statements about various behaviors relating to privacy that people may or may not exhibit. Example statements are: *"No organization or person should disseminate personal information about me without my knowledge"*, *"I respond to telephone marketing surveys", or "I like to change my passwords frequently"*. Participants had to judge the extent to which they agree with each statement. The tool was originally developed to aid designers, since there is little information they can use as a basis for the design of new technologies and interfaces with privacy implications (e.g. personalization). The PAQ tool was included in this study because of its relevance to the domain of personalization. This also allowed a comparison of the two different tools for measuring privacy attitudes.

In-depth semi-structured individual interviews were conducted, which varied in duration between half an hour and an hour. After the completion of the on-line questionnaires participants were given an interview appointment. Participants were contacted at random. In total 21 interviews were conducted. The aim of the interview was to gain a more thorough understanding of the factors on which disclosure decisions are based and to obtain additional information about some of the answers given in the on-line questionnaire. The interviews were semi-structured and covered the following topics (see also Appendix A3):

- Opinion on the Music Recommender. This topic was included to collect main appreciation or concerns, whether they expected the goal, or thought privacy was an issue. They were not prompted though regarding privacy.
- Expected goal/aim of the research. This topic was addressed in an open fashion, but in a similar way without mentioning privacy at all. The topic was included to check whether people were aware that the research related to privacy, and whether this influenced their disclosure behavior.
- Considerations for choosing a specific level of disclosure during and after the study. This was included to get a deeper insight into underlying factors.
- Some questions to address their understanding of the system, e.g. accessibility of data to other parties or expectations about changes in the system after each disclosure choice.
- Experience with the system after each disclosure choice. This was addressed to see whether participants noticed any benefits from disclosing information and whether this may have influenced their disclosure choices.
- Feelings about the disclosure of music preferences or personality traits profile information. This was addressed in order to see whether participants felt there was a difference between the two types of information.

2.3 RESULTS

This section describes the results of the study on the actual disclosure behavior of users and their self-reported data. It is important to realize that data is obtained in three different ways: by observation, through the post-experimental questionnaire, and through interviews. The data based on observations and the closed questions in the questionnaire are analyzed in a quantitative fashion. The procedure used for the analysis of the qualitative data is explained below.

If necessary, the raw qualitative data was translated into English (all interviews were conducted in Dutch, recorded on tape and transcribed verbatim; the questionnaire questions were posed in English, but a few participants chose to answer in Dutch). Both the questionnaire and interview included open questions where participants were free to express their feelings in their own words. The questionnaire and interview data was analyzed by means of open coding (Strauss & Corbin, 1990). Some numerical summaries of the coded data are given if such an overview is considered to help promote clear presentation of the data, but it should be taken into account that the interview and questionnaire data are of a qualitative nature and should be interpreted as such.

2.3.1 Participants' background

All participants reported an interest in music: 45% of the participants own over 100 CD's, and 75% of the participants indicated to own over 200 MP3 songs. And 66% of the participants indicated to listen frequently to music when using a computer.

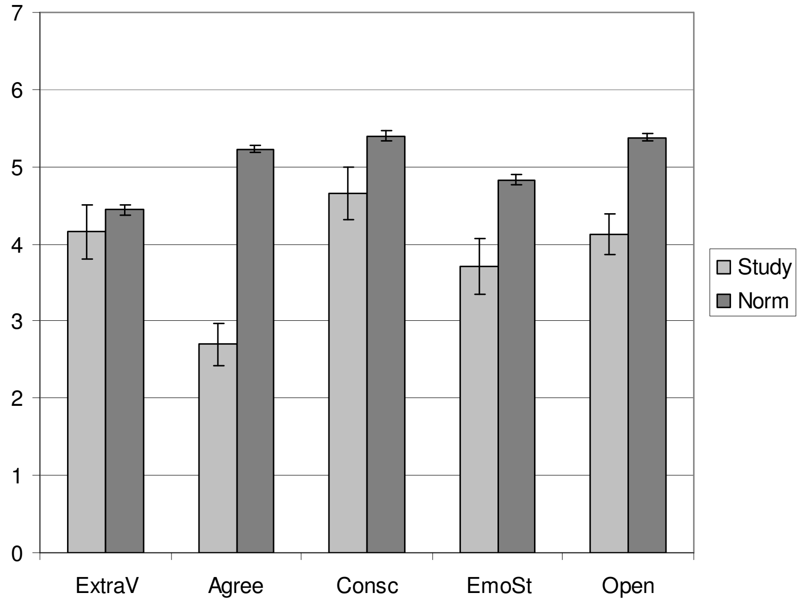
Most participants were students (27), 18 indicated to be working in research and 3 had other, mainly ICT related, jobs. Most participants had a background in architecture, or computer science (both 7). There were 6 participants with various technical backgrounds, and other common areas of expertise were chemistry, and physics (both 5).

Participants' preferences for music genres were obtained during the experiment by the STOMP on a scale from 1 (strongly dislike) to 7 (strongly like). The most appreciated genres by participants were rock, pop and alternative music. Their mean appreciation scores are 5.92, 5.02 and 5.00 respectively. The least appreciated genres were religious, country and folk music. Their mean appreciation scores are 1.71, 2.85 and 2.90 respectively.

Participants' personality traits were obtained during the experiment by the TIPI on a scale that ranges from 1 (low score on trait) to 7 (high score on trait). Participants scored lowest on agreeableness (2.70), and highest on conscientiousness (4.66, see Figure 2.5). For the other three traits (Emotional Stability, Extraversion, and Openness to new experiences) the mean scores were fairly similar and all between 3.7 and 4.3.

Overall these scores are lower than as found by Gosling et al. (2003). Especially the mean score for agreeableness is much lower (2.70) in this dataset than in theirs (5.23). This does not affect the results of the experiment considerably. It just means that different music is recommended to the group of participants, because of a different pattern of personality traits. Further it could be an indication of cultural difference in such a way that US residents tend to be more agreeable than Dutch residents.

Figure 2.5. Personality traits of participants in comparison to norm provided by Gosling et al. (2003)



Note: Mean score on each personality trait including 95%confidence interval. ExtraV = Extraversion, Agree = Agreeableness, Consc = Conscientiousness, EmoSt = Emotional Stability, Open = Openness to new experiences.

2.3.2 Evaluation of the Music Recommender

Opinion about the use of the Music Recommender

On average it took participants 13 days to complete the three phases for both recommender systems. Only 5 participants took the minimum of six consecutive days to complete all phases and 4 participants took over 3 weeks. Except for the latter 4 participants, the study duration was as intended: after two weeks it is likely that participants are still able to remember their disclosure choices made and the underlying motivations.

In the questionnaire after the experiment, all 48 participants were asked to indicate their level of appreciation of the music recommender. Table 2.1 shows to what extent participants appreciated the Music Recommender system in general. In total 48% of the participants were (somewhat) positive about the recommender, and 33% of the participants disliked the Music Recommender system in general.

Table 2.1. Level of appreciation of the Music Recommender system in general

	Participants	
Level of appreciation	No.	%
Like a lot	4	8
Like somewhat	19	40
Neither like, nor dislike	9	19
Dislike somewhat	12	25
Dislike a lot	4	8

Besides their general appreciation of the Music Recommender, all 48 participants were also asked an open question to name their most liked and most disliked aspects of the Music Recommender system. The numerical summaries of the coded responses to this open question are merely intended to provide an impression of the salience of some comments and to support clearer presentation of the data.

In total 57 items were mentioned to be liked about the Music Recommender, consisting of 14 different themes. Four themes were mentioned exclusively as positive aspects, namely see top section of Table 2.2.

Many participants indicated that they appreciated the music that was recommended to them. Especially the fact of being exposed to new or unknown songs and artists was

Table 2.2. Most liked and disliked aspects of the Music Recommender

Aspect of Music Recommender	Liked	Disliked
Being exposed to/getting to know new/unknown songs/artists	12	
Diversity / variety of songs	8	
Being exposed to nice music (but which you don't have, think of, or would play yourself)	4	
Not having to choose music yourself	3	
The concept (personal music recommendations)	5	1
The MP based recommender	4	1
User Interface / Interaction with the application	4	6
Quality of the recommendations	3	9
Surprise element (lack of)	3	1
Being exposed to music you like / don't like	2	10
Specifying music preferences	2	1
The PT based recommender	1	4
Derived personality traits	1	1
Nothing (indicated to be liked/disliked)	5	4
Similar / repetitive recommendations		7
Fragments of songs		6
Control over user profile after providing initial info		5
Feedback not taken into account		4
Limited amount of songs / artists in database		3
Limited possibility for feedback		3
Manually having to start each song		3
Difficult to evaluate quality of playlists (due to fragments)		2
Too broad / general recommendations		2
Comparison of data to other users		1
Info about privacy consequences		1
Interaction with other users		1
Not being able to take mood into account		1

Note: The values represent the number of participants who mentioned a particular aspect in response to an open question regarding the most liked / disliked aspect of the Music Recommender.

valued (e.g. *"It recommended songs I never heard before"*). Others indicated to appreciate the variety of songs that was offered to them, or to appreciate being exposed to nice music that they did not have, or would not think of playing themselves (e.g. a participant indicated: *"It recommended some music I had liked in the past but totally forgot about…."*). And some participants especially liked the fact that they did not have to choose the music explicitly.

Some elements of the Music Recommender seemed to be liked as well as disliked see middle section of Table 2.2. The general notion of receiving personal music recommendations was appreciated by more participants, than it was disliked. However, the recommendations that were actually provided by the system were not appreciated by many participants, both in terms of quality and in terms of liking the music one was exposed to. This indicates that the Music Recommender was perhaps not the most sophisticated recommendation system or that the collection of music accessible was not entirely suitable. Due to these limitations of the music recommendations, smaller benefits were offered than what would be appropriate for a commercial use or for adoption of the service. However, since the aim of the research was on studying privacy behavior, and not on providing good recommendations, this was not a major issue.

Some participants appreciated the surprise element of the Music Recommender, however one participant felt there was a lack of surprise in the recommendations. Only 2 participants indicated to appreciate the fact that they could indicate their music preferences, but 1 participant was not satisfied about this (and indicated to dislike: *"The way of choosing your own music taste. It should be a little bit more specific. For example (by) choosing bands instead of genres"*). Especially the Music Preference based recommender was appreciated by some participants, whereas one participant indicated to dislike it. The feelings about the Personality based recommender was exactly the opposite, more participants indicate to dislike rather than to like it (e.g. *"The music recommended to my personality wasn't really good"*). Quite some participants commented on the User Interface, approximately half of them were positive, and the other half was negative. Finally, there were some participants who did not mention any elements they liked (5), or disliked (4) elements.

Overall participants mentioned more aspects that they disliked than liked. There were 77 items mentioned to be disliked, which consisted of 23 different themes. The 13 elements that were only disliked are shown in the bottom section of Table 2.2. The table shows that there were quite some participants who disliked the fact that the different playlists were somewhat similar and many indicated to dislike the fact that only fragments of songs were available. Some participants disliked the fact that they were unable to make changes to their profile and others felt that their feedback (i.e. the quality ratings of playlists) was not taken into account with the recommendations that followed. The other concepts were mentioned to be disliked by only a few participants, such as the limited amount of songs / artists in database, the limited possibility for providing feedback (e.g. only indicating overall quality of playlist, and not being able to ban disliked artists for the future), the fact that each song has to be selected manually in order to listen to the song, that the quality of the playlists was difficult to judge due to the fragments of songs that were provided, and the fact that the recommendations were of a broad and general nature, the comparison of data to other users, the limited availability of information about the privacy consequences of disclosure, the limited interaction possibilities with other users, the fact that the Music Recommender could not take mood into account.

In the questionnaire participants were asked to comment on how they felt about having to provide music preferences versus personality traits. Due to the open style of questioning, participants were free to comment on whatever felt relevant to them with regard to the assessment of the personal information. This resulted in some participants commenting on the difficulty of filling out the forms or on their expectations of what information a music recommender system may need. Yet others indicated whether or not they feel comfortable about providing specific types of information, and some participants commented on the quality of the resulting recommendations.

Participants were not surprised about having to provide music preferences, but they were surprised about having to provide personality traits. More participants felt that completing the TIPI was difficult compared to completing STOMP test. Participants were more suspicious about the expected quality of the recommendation in the case of personality traits compared to music preferences. This confirms the predictions regarding the legitimacy of the information requested motivating the experiment design.

Finally, participants evaluated the actual quality of the recommendations as more disappointing in the case of personality traits as well. An almost equal amount of participants indicated not having problems with providing either personality traits or music preferences. None of the participants explicitly mentioned being worried about privacy consequences at this stage of the questionnaire.

In the questionnaire, participants were also asked about the required effort of providing both types of profile information to the system. Table 2.3 shows the percentage of participants that indicated what amount of effort it took them to provide the information for creating the profile on the basis of music preferences or personality traits. Most participants (98%) felt that the assessment of preferences for music genres required none or only little effort. The assessment of personality traits was rated as requiring more effort than music preferences by half of the participants, the other half felt it required an equal amount of effort. 23% of the participants felt that the assessment of personality traits required much effort compared to 2% in the case of music preferences.

Overall, the results suggest that there is a significant difference in the amount of effort required for providing the two types of information. The participants felt that relatively more effort was required to provide personality traits than to provide music preferences to the system for user profiling (Wilcoxon Signed Ranks Test, N=48, z=-4.524, p=.000).

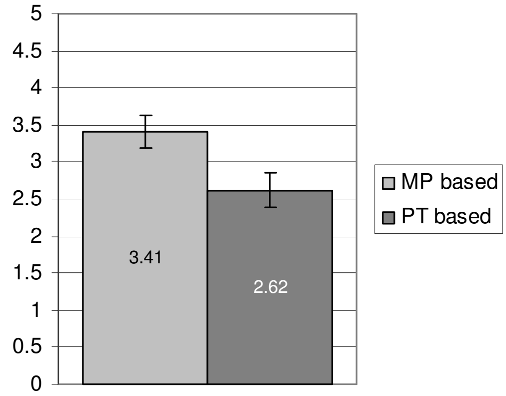
Table 2.3 shows the percentage of participants indicating the amount of effort that is required to provide the requested profiling information (personality traits and music preferences). It shows that all participants rated the amount of effort to provide

Table 2.3. Required effort for the assessment of Music Preferences and Personality Traits

Percent		Effort to provide PT			
		No	Little	Much	
Effort to provide MP	No	18.8	29.2	12.5	60.4
	Little	0.0	29.2	8.3	37.5
	Much	0.0	0.0	2.1	2.1
		18.8	58.3	22.9	

Note: The values represent percentage of participants providing a specific combination of answers.

Figure 2.6. Appreciation of recommendations based on Music Preferences versus Personality Traits



Note: Based on a 5-point scale ranging from 1 (very bad) to 5 (very good). Including 95% confidence interval.

personality traits the same or higher than the amount of effort required to provide music preferences. The correlation between the amounts of effort required for both two types of information is significant (Pearson product-moment correlation is .313, p<0.05).

Recommendations based on Music Preferences appreciated more

During the use of the recommender, participants were asked to rate the quality of each playlist on a 5-point scale ranging from 1 (very bad) to 5 (very good). The average quality rating of all playlists was 3.02. Playlists that were based on music preferences were rated significantly higher on average (3.41) than playlists that were recommended to participants on the basis of personality traits (2.63, p<0.001, see Figure 2.6). This suggests that, based on the inventories used for user profiling (TIPI and STOMP), personality traits are less suitable for providing music recommendations than preferences for music genres.

A similar image arose from the questionnaire data where participants were asked to list "things they liked or disliked". Four participants said they liked the music that was recommended to them on the basis of their preferences for music genres, and only one said they disliked these recommendations. In contrary, with regard to the system based on personality traits, four participants were not satisfied with the recommendations, and only one participant was happy with the outcome.

2.3.3 Evaluation of experimental approach

Participants felt they took part in a study of music recommendations and not privacy

As "things they liked or disliked" most participants mentioned the music that was recommended to them. Hardly any privacy-related topics were mentioned. Only one participant mentioned, among other things, that: "*There is very little information about how your decisions will affect your privacy*". This statement pertains directly to the guidelines for fair information practices discussed in chapter 1. Another participant said to dislike: "*the comparison of my data with that of other persons*" without further explanation or reference to privacy.

In total five participants said they disliked the lack of control over the user profile after the initial information was provided. Even though this does not necessarily imply a lack of privacy, it should be noted that user control is frequently mentioned in relation to privacy (see the definition in the introduction and, for example, W3C, 1998; Margulis, 2003; Bellotti & Sellen, 1993; Günther & Spiekermann, 2005). Nonetheless, the vast majority of participants did not address the topic of privacy explicitly, which suggests that they experienced the system as a music recommender service and not as a study in privacy.

In the interviews with 21 of the participants their initial reaction to the Music Recommender was discussed in order to see if they would mention any privacy issues. Overall, 10 interviewees were positive about the Music Recommender, 5 were negative, and 6 were more or less neutral. None of the interviewees raised privacy issues at this point. Many participants commented on the concept of the Music Recommender or the type of music that was recommended to them (e.g. "*I thought it was very surprising. Nice and surprising. (…) I got to hear music that I didn't already know, but liked nevertheless. It was nice for once to hear some new music instead of the music I have in my own playlist*"). This implies two things: participants perceived the study as being about music recommendations, and the Music Recommender provided actual benefits to them.

Participants were asked via a questionnaire about their initial reaction to having to disclose profile information to the system. Most participants said they had no problem with providing either music preferences (n=21) or personality traits (n=19). Many participants indicated that they expected to be asked about their music preferences (n=18), but the inquiries about personality traits surprised quite a few participants (n=6). No privacy-related comments were made with regard to the collection of music preferences or personality traits. So, although personality traits were not readily associated with music recommender services, it seems that participants were quite open about disclosing them.

Interviewees unaware of the study's focus on privacy

The goal of the research was discussed at the beginning of most interviews. There were some interviewees who expected only the development or improvement of the Music Recommender to be the goal of the research. Although there were also some interviewees who expected privacy to be of interest to the research, it was never mentioned as a single expected goal. On the whole, interviewees turned out to be unaware of the actual aim of the research.

The goal of the research was discussed at the beginning of most interviews. On the whole, interviewees turned out to be unaware of the actual aim of the research. Some interviewees expected only the development or improvement of the Music Recommender to be the goal of the research (e.g. "*To create a jukebox like application (…)*". Although there were also some interviewees who expected privacy to be of interest to the research, it was never mentioned as a single expected goal (e.g. *"Before I participated I thought the aim was to test whether that tool would work properly. (…) But when I answered the questionnaire afterwards, I got the impression that the aim was a little different (…). That it was more about how you deal with ehm, personal information that you share with others or systems (…)".*

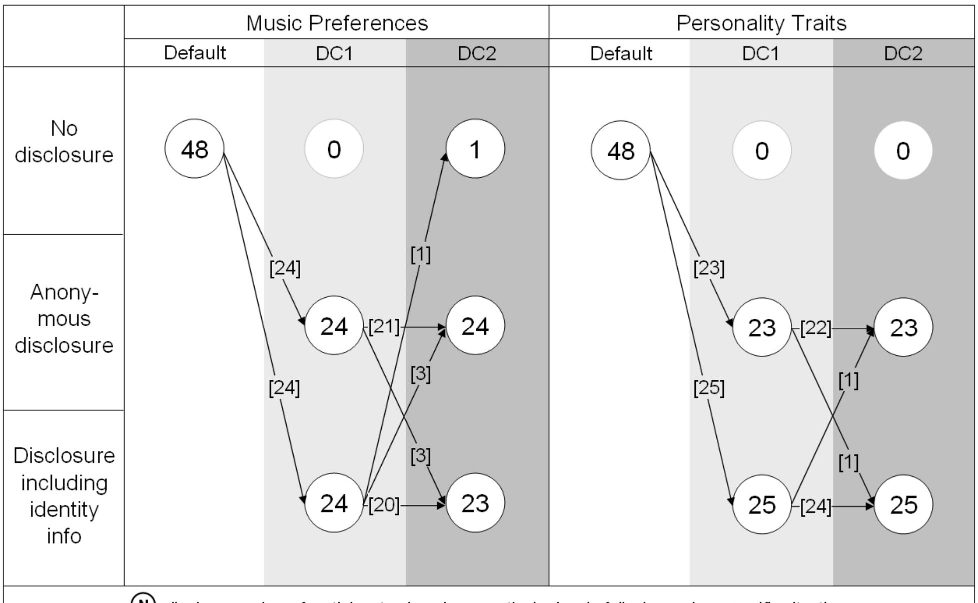
Interviewees who expected that privacy was the focus of the study tended to disclose less information than those who did not mention it. Besides, interviewees tended to disclose less information if they did not expect the focus of the research to be on music preferences (compared to those who did, or those who did not mention it). It seems that participants feel more comfortable disclosing information if they are under the impression that they are using a music service and if privacy is not mentioned. It could be that thinking or being conscious about privacy even when not explicitly primed, will make people more cautious of the risks involved.

2.3.4 Evaluation of disclosure behavior

Disclosure behavior consistent across situations, yet divided between participants

An overview of the disclosure behavior of all participants is shown in Figure 2.7. The number of participants who chose a particular level of disclosure per disclosure situation is shown in a circle. The number between brackets on the arrow between two circles refers to the number of participants who chose a similar set of disclosure levels in two consecutive situations. For example, [21] refers to the 21 participants who chose anonymous disclosure in both situations relating to music preferences. Figure 2.7 shows that participants were divided in their disclosure behavior and maintained the same level of disclosure (44% chose anonymous disclosure, and 42% chose disclosure including identity information) throughout the four choice situations. Only 15% of the participants varied their chosen level of disclosure at different phases of the study. These variations did not show a clear trend towards increasing or decreasing levels of disclosure. Similar findings were reported earlier for the pilot of this study (Perik et al., 2004).

Figure 2.7. Overview of disclosure choices (DC) by all participants during the study


Music Preferences
Default
DC1
DC2
Personality Traits
Default
DC1
DC2
No disclosure
Anony-mous disclosure
Disclosure including identity info
48
0
1
24
24
24
23
[24]
[24]
[1]
[21]
[3]
[3]
[20]
48
0
0
23
23
25
25
[23]
[25]
[22]
[1]
[1]
[24]
(N): displays number of participants choosing a particular level of disclosure in a specific situation
[N] : displays number of participants choosing a similar set of disclosure levels in two consecutive situations

Note: The three rows represent the different disclosure options participants were given at each of the four disclosure choices. The columns represent the three different phases (of which one default situation where no disclosure choice could be made) for the recommender systems based on Music Preference and Personality Traits. The order in which participants used the two recommender systems was counterbalanced.

Privacy concerns lead to anonymous disclosure; expected benefits to full disclosure

In the questionnaires (box 11 in Figure 2.3, page 31) and the interviews (box 12 in same Figure) participants were asked to explain why they chose a specific level of disclosure.

Many participants who chose anonymous disclosure said their choice was based on privacy concerns (n=19). One of them said: "*People may see the information I provided; I do not know who reads it and therefore prefer to have the information anonymous.*" Some chose anonymous disclosure just to be on the safe side (n=4) e.g. "*I felt that others did not need to know my name…*"

However, most of the participants who disclosed identity information based their decision on the benefit they might gain in return (n=12). As expressed by one participant: "*… I want the system to perform best. That's why I gave full permission.*" Another large group (n=10) said they chose disclosure including identity information simply because they had "*no problem*" about disclosing the information.

A number of participants said that they wanted to support the research by disclosing their information (n=7), and some of them added that they did not care about the information disclosure either. The on-line questionnaire and the interview data together indicated that participants felt quite safe disclosing personal information within the context of this experiment, even though they were actually allowing the system to show their personal information to other users. It can therefore be argued that participation in the research did have some (but not much) influence on the behavior of subjects.

All interviewees said they were influenced to some extent in their disclosure decisions by the costs and benefits involved. The costs and benefits expected as a result of the disclosure of information were often mentioned simultaneously, e.g.: "*I first wanted to see what the quality would be like, without giving full permission immediately*". Another participant stated: "*You have to weigh up (…) the benefits and the costs. And yes, of course, it is difficult to estimate the cost of the information you provide. (…) If it is clear that it is going to be of benefit, then I will do it*".

In summary, disclosure choices were influenced by people's perception of privacy risks and the expected benefits. This was in line with the motivation of the experiment design and the initial expectation that participants would balance their privacy against expected benefits from personalization and would adjust their disclosure behavior accordingly.

Possible alternative explanations for disclosure behavior

Besides the factors mentioned above, such as the type of information involved or what the information is used for, it could very well be that disclosure behavior was influenced by other factors such as gender, age, experience of using technology, or personality traits.

For gender no significant differences in disclosure behavior were found in each of the four disclosure situations (p=0.701 for comparing Music Preferences; p=0.703 for sharing Music Preferences, p=0.454 for both comparing and sharing Personality Traits, all 2-sided Fisher's Exact Test). See Table 2.4. Similarly, no correlation was found between age and disclosure behavior in each of the four disclosure situations (see Table 2.5).

Table 2.4. Level of disclosure by men and women

	Music Preferences				Personality Traits			
	System comparison		Sharing with others		System comparison		Sharing with others	
	NA	ID	NA	ID	NA	ID	NA	ID
Men (n=40)	47.5	52.5	50	50	45	55	45	55
Women (n=8)	62.5	37.5	62.5	37.5	62.5	37.5	62.5	37.5
FET	p=0.701		p=0.703		p=0.454		p=0.454	

Note: The values represent percentage of men/women choosing a specific level of disclosure in each of the four disclosure choice moments. Bottom row shows p-value for 2-sided Fisher's Exact Test (FET). NA = No Disclosure or Anonymous Disclosure, ID = Disclosure including identity information.

Table 2.5. Correlation between age and level of disclosure

	Music Preferences		Personality Traits	
	System comparison	Sharing with others	System comparison	Sharing with others
Correlation Coefficient	0.152369	0.022593	0.188739	0.049827
Sig. (2-tailed)	0.301199	0.878853	0.198885	0.736629
N	48	48	48	48

Note: Correlation by Spearman's rho.

Since the participants in this study were recruited from the Eindhoven University of Technology and the Philips Research Labs in Eindhoven, it was assumed that most participants would be experienced users of technology. Therefore, experience in using technology was not measured, and it cannot be used in an attempt to explain individual results.

With regard to the Personality Traits, only openness to new experiences could explain disclosure behavior. Participants who chose disclosure including identity information in all four choice situations scored significantly higher on the openness to new experiences trait than participants who chose only anonymous disclosure (U=105.0, p=0.005).

Motives for disclosure not consistent with behavior

Comparison of the chosen levels of disclosure and the reported explanations of participants in questionnaires did not lead to a clear explanation of why some participants varied their level of disclosure whereas others did not. Sometimes participants provided a consistent motivation for different disclosure choices and varying reasons for identical levels of disclosure.

For example, a participant who chose disclosure including identity in the situations concerning showing information directly to other users and anonymous disclosure in the other situations provided the same explanation for these varying levels of disclosure, namely: "*I thought it would improve the recommender*".

Another participant who chose anonymous disclosure in all four situations gave different explanations, namely "*because I thought it would give me better playlists*" in the situations relating to showing information directly to other users and "*I want to stay anonymous in things I do over the Internet*" in the other situations. The expectations with regard to the changes in the system after making a specific disclosure choice were discussed with 9 interviewees. All but one said they had expected there would be some improvement in the recommendations afterwards.

PAQ & PSI poor behavior predictors; context-specific privacy concerns better

The relationship between the actual disclosure behavior of participants and their privacy attitudes based on the PAQ or PSI were investigated. The PAQ scores did not provide a good indication of the disclosure behavior in this context, except for the 'Personal Information' factor. The higher score on this factor relates to a higher level of disclosure. For the 'Exposure', 'Monitoring' and 'Protection' factors there is no clear relationship with disclosure behavior. As for the PSI, one would expect that people who are 'Privacy Unconcerned' would choose high levels of disclosure, and 'Privacy Fundamentalists' would choose low levels of disclosure. However, this was not the case in the current study (see Table 2.6). There is very little difference in the level of disclosure chosen between the three PSI segments. Some participants who can be characterized as 'Privacy Fundamentalists' chose disclosure including identity and said they had *"no problem"* with the information disclosure. Furthermore, some of the 'Privacy Unconcerned' participants argued that they valued their anonymity when they were asked to explain their disclosure behavior.

The questionnaire items relating to worries about disclosing personal information to other people or to a music content provider do give a better indication of actual disclosure behavior. The participants who said they were not worried about disclosing music preferences or personality traits tended towards a higher level of disclosure than participants who said they were worried about these types of disclosure.

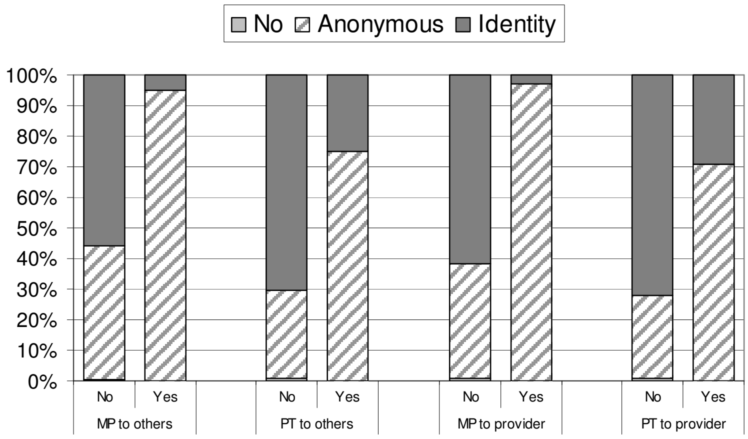
Figure 2.8 shows the relation between the expressed worries about disclosure of information and percentage of participants choosing no disclosure, anonymous

Table 2.6. Level of disclosure by different PSI segments

		Unconcerned (n=6)			Pragmatists (n=24)			Fundamentalists (n=18)			Total (N=48)		
		N	A	ID	N	A	ID	N	A	ID	N	A	ID
MP	System comparison	0	67	33	0	46	54	0	50	50	0	50	50
	Sharing with others	0	67	33	0	46	54	6	50	44	2	50	48
PT	System comparison	0	67	33	0	42	58	0	50	50	0	48	52
	Sharing with others	0	67	33	0	42	58	0	50	50	0	48	52

Note: The values represent percentage of participants within a group (based on PSI segmentation and for all participants) choosing a specific level of disclosure in each of the four disclosure choice moments. N = No Disclosure, A = Anonymous Disclosure, ID = Disclosure including identity information, MP = Music Preferences, PT = Personality Traits.

Figure 2.8. Relation between worries about disclosure and chosen level of disclosure



disclosure or disclosure including identity information across all four situations during the experiment. This clearly shows that participants who indicated not to be worried about disclosing music preferences or personality traits to other people or a music content (X-axis) provider tended to disclose on a higher level compared to the participants who indicated to be worried about these types of disclosure.

The relation between presence or absence of worries and level of disclosure is analyzed by Fisher's Exact Test. The relation is studied for all four disclosure situations in combination with the two possible sources for worries (disclosure towards other people or towards a provider). It turns out that in all except one of those instances (showing music preferences to other people and worries about such disclosure) absence of worries leads to significantly higher levels of disclosure. For the disclosure comparison a one-sided hypothesis was used, testing whether absence of worries would lead to higher disclosure compared to presence of worries (see Table 2.7).

Table 2.7. Relation between worries about disclosure and chosen level of disclosure

		Music Preferences				Personality Traits			
		System Comparison		Sharing with others		System Comparison		Sharing with others	
Worries		NA	ID	NA	ID	NA	ID	NA	ID
Others	No	19	24	21	22	7	20	7	20
	Yes	5	0	4	1	16	5	16	5
	FET (p)	0.025		0.201		0.001		0.001	
Provider	No	15	24	17	22	6	18	6	18
	Yes	9	0	8	1	17	7	17	7
	FET (p)	0.001		0.016		0.002		0.002	

Note: The values represent number of participants choosing a specific level of disclosure in each of the four disclosure choice moments. Bottom row shows p-value for 2-sided Fisher's Exact Test (FET). NA = No Disclosure or Anonymous Disclosure, ID = Disclosure including identity information.

2.3.5 Evaluation of attitudes

Interviewees worry about unclear purpose of disclosure & accessibility of info to others

Many interviewees said they were influenced in their disclosure choices by other parties possibly having access to their data. For example, one participant explained that: "*the most important reason not to choose full permission but anonymous, was because I didn't know the other people who could see the information*". Other factors mentioned were the fact that they were participating in a research study, or that they wanted to try out the system.

Also, the specific features of the system (especially the lack of information about the purpose or consequences of information disclosure and the accessibility of information to other people) did influence participants' disclosure behavior. For example, one participant stressed the importance of knowing the purpose: "*I would like to know what the purpose is of releasing information. (…) [providing information] anonymously is not such a problem for me. If my information is published together with my name, then in the case of the Music Recommender I have to question what purpose that serves. I did not see the benefit of that.*" Another participant mentioned various desirable system features: "*It should be really clear why you need to provide certain information. And you should know in what domain the information is used, and who gets to see the information.*"

In addition to the information provided in questionnaires, interviewees stressed the importance of knowing the purpose for which information should be disclosed, and expressed worries about other people gaining access to their information.

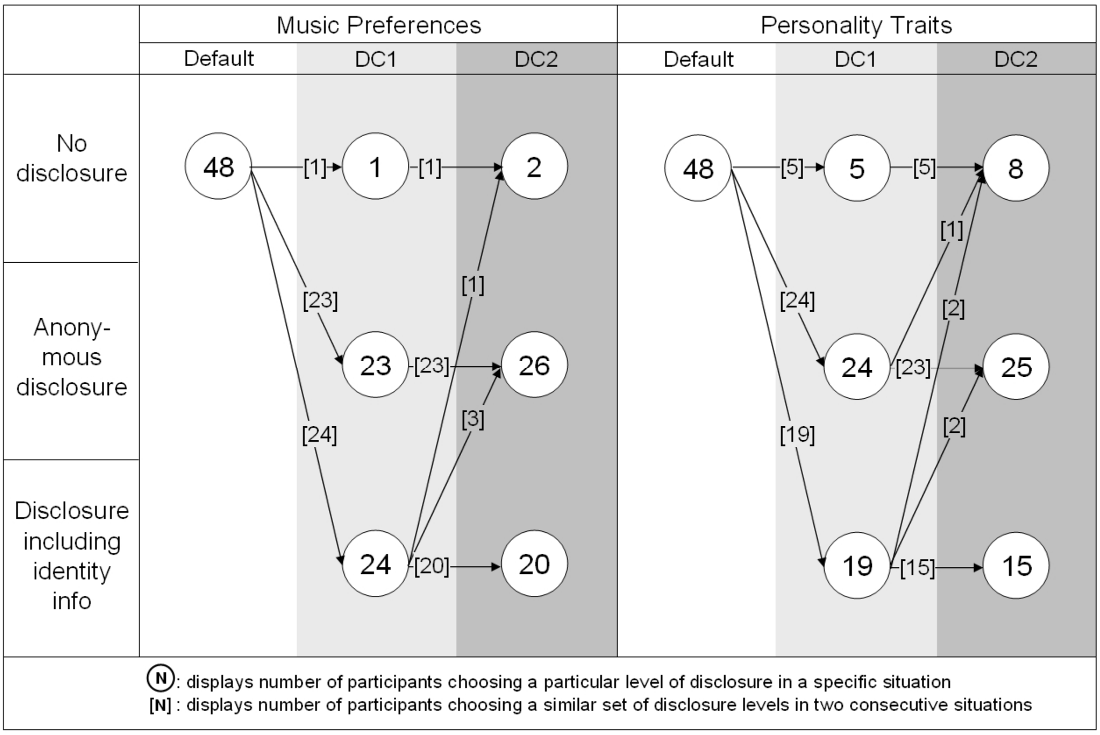
Participants less open to disclosure post-experiment & expected more benefits

In the questionnaire participants were asked what level of disclosure they would choose for the same four situations they were asked about during the experiment. A different picture arose for the level of disclosure participants would choose after the study (see Figure 2.9) compared with the level they chose during the study. Although most participants said they would choose exactly the same level of disclosure in all four situations as they did whilst using the recommender. Quite a number of participants (27%) said they would choose lower levels of disclosure in all or some of the situations (e.g. those situations relating to personality traits or to showing profile information directly to other users).

To check whether there are any differences in the chosen level of disclosure between the four disclosure situations a Chi-squared test was performed. Due to the low occurrence of people choosing no disclosure, the disclosure choices 'no disclosure' and 'anonymous disclosure' were combined. None of the differences turned out to be statistically significant. For the comparison between the two situations involving music preferences, personality traits, system comparison and sharing with others Chi^2 (1, N=48) = 0.67; 0.73; 1.05 and 1.12 respectively.

More or less the same reasons were mentioned for the disclosure choices during and after use of the recommender. However, after using the recommender fewer participants mentioned privacy concerns or their wish to support research as a reason for their chosen level of disclosure. Yet, more participants mentioned that there was no privacy risk or private information involved, and some participants mentioned that they expected better recommendations and more substantial improvements as a benefit from the

Figure 2.9. Overview of disclosure choices (DC) by all participants after the study


Music Preferences
Personality Traits
Default
DC1
DC2
Default
DC1
DC2
No disclosure
Anony-mous disclosure
Disclosure including identity info
48
[1]
1
[1]
2
[23]
[1]
23
[23]
26
[24]
[3]
24
[20]
20
48
[5]
5
[5]
8
[1]
[24]
[2]
24
[23]
25
[19]
[2]
19
[15]
15
Ⓝ: displays number of participants choosing a particular level of disclosure in a specific situation
[N] : displays number of participants choosing a similar set of disclosure levels in two consecutive situations

Note: The three rows represent the different disclosure options participants were given at each of the four disclosure choices after the experiment. The columns represent the three different phases (of which one default situation where no disclosure choice could be made) for the recommender systems based on Music Preference and Personality Traits.

disclosure of personal information. Similarly, most of the participants who chose different levels of disclosure during and after use of the recommender also explained their changes by pointing at privacy-related issues or the lack of benefits. This finding was confirmed in interviews with eight of these participants.

Sample quite representative in terms of privacy attitudes

The Privacy Segmentation Index (PSI) was used as a measure for privacy attitudes. According to the PSI, 38% of participants were privacy fundamentalists (very high privacy concern), 50% were privacy pragmatists (balanced attitudes), and 13% were privacy unconcerned (very low or no concern). This matches well with the Harris Interactive sample, where the segments were 34%, 58%, and 8% respectively (Harris Interactive, 2002), indicating that the participants of this study are not particularly skewed in any direction regarding their privacy attitudes.

The Privacy Attitude Questionnaire (PAQ) was used as a second measure for the privacy attitudes of 43 participants. These participants had a fairly neutral attitude towards the disclosure of personal information and were generally willing to be monitored. Analysis of the results shows that the participants were, on average, willing to expose their images to the public and they had an interest in protecting against unwanted intrusions. While PAQ gives a more refined account of privacy attitudes, there is no data reported for the overall sample of Chignell et al. (2003) against which to compare the findings of the study described in this chapter.

Table 2.8. Amount of interviewees addressing sensitivity with regard to different information types

	Music Preferences	Personality Traits	Identity
Sensitive	0	7	9
Non-sensitive	12	6	2
Not addressed (clearly)	9	8	10

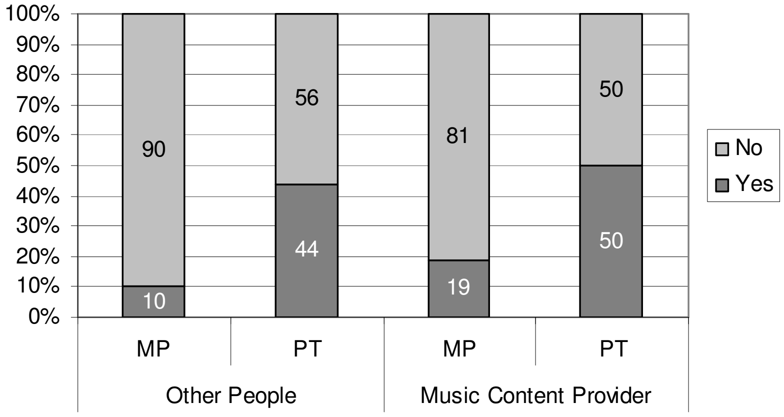
Participants' opinions about some general privacy issues were uncovered. It turned out that they liked to receive advance notice or a clear description of the purpose of the information collected. Furthermore, participants said they valued being able to check and correct the personal information held by a system. Nonetheless, participants do little to protect themselves; they rarely read privacy policies, and they do not use encryption of e-mail. Participants did tend to be more willing to provide personal information in return for low-cost products or convenience. However, participants also said they provided fictitious data in some cases.

Personality Traits perceived as more sensitive than Music Preferences

In the interviews the sensitivity of the various types of information involved (music preferences, personality traits and identity information) were discussed. Most interviewees indicated that identity information was regarded as sensitive, followed by personality trait information. None of the interviewees said they regarded music preference information as sensitive (see Table 2.8).

In the questionnaire participants were also asked about how they felt regarding the disclosure of information either to other people or to a music content provider. It turned out that more participants worry about disclosing personality traits than about disclosing music preferences (see Figure 2.10: 44% versus 10% respectively with regard to disclosure to other people, and 50% versus 19% respectively with regard to disclosure to a music content provider). Both of these ratios are significant (p = 0.012, and p = 0.002, 2-sided Fisher's exact test).

Figure 2.10. Percentage of participants worrying or not about the disclosure of information



Note: Two types of information are compared (MP = Music Preferences; PT = Personality Traits). Disclosure to two different parties is considered (other people versus a music content provider).

2.4 DISCUSSION

When setting up the study presented here, there were several concerns and expectations. The concerns were mostly about creating realistic privacy dilemmas that participants would experience in a realistic context of use. The development of a purpose-built application enabled the study to provide a personalized service and to apply the experimental protocol for collecting empirical data. Although this approach is very laborious, it has a lot of potential for privacy research. The results of this study complement similar findings from surveys or experiments conducted in the artificial setting of the laboratory.

Regarding the initial concern about the realism of the privacy dilemmas, several precautions were taken, and verified post-hoc. The incorporation and verification of the following precautions was fundamental in ensuring the validity of empirical results relating to privacy:

- Ensuring the participants were not aware of the study's focus on privacy;
- Avoiding sampling bias;
- Ensuring that benefits and costs from disclosure were actually experienced as such;
- Providing rewards for participants to encourage honest disclosure (as was done in this study);
- A purpose-built application should have a look and feel analogous to current services and should not appear minimal or scientific (software made for experimentation normally looks different from a commercial service).

Throughout the experiment, a number of measures were taken to avoid priming participants as to the study's interest in privacy because this might have induced normative reactions. On the whole, this was successful; for example, none of the participants spontaneously mentioned privacy issues when discussing the system. This indicates that the setup succeeded in not sensitizing them to privacy, and that their behavior during the study would be a good representation of actual behavior in such a situation.

One concern, in terms of how representative privacy experiments are, is the potential tendency of privacy-concerned individuals to decline to participate in research. Clearly, when consent is obtained or when the nature of the study is described, individuals who are more concerned about privacy may refrain from participating. Possible strategies to encourage these privacy-concerned individuals to participate include:

- Recruit participants for an experiment with a non-privacy-related topic (e.g., music recommendations, as in the current study);
- Recruit participants for a survey study, as this may be considered more anonymous and less threatening;
- Use field observation and ask people for permission to use their data for research purposes afterwards. However, this leads to obvious ethical concerns, and arguably privacy-concerned individuals may still be prone to decline.

To prevent and to check for a potential sampling bias in this study, potential participants were not informed about the focus on privacy and, finally, participants were questioned about their general and context-specific privacy attitudes. According to the Privacy Segmentation Index (PSI) and Privacy Attitude Questionnaire (PAQ) the participants varied in their level of concern for privacy; some were unconcerned about their privacy, whilst others had a high level of concern about their privacy.

There was a spread between participants in the extent to which they perceived privacy risks while using the Music Recommender. Subjects reported differences in perceived privacy risks in questionnaires and interviews and disclosure behavior was also divided. Ensuring a spread in privacy attitudes among study participants and assessing the actual level of perceived risk that participants experience during a study should be a standard procedure for privacy research. The assessment of perceived risk in particular is often omitted in privacy research, thus constituting a serious threat to the validity of results reported.

Despite the fact that the participants did not notice that the purpose of the study related to privacy, their nuanced behaviors and comments relating to the reasons why they chose a specific level of disclosure show that they were conscious of and influenced by costs and benefits relating to privacy and personalization. This is consistent with published results relating to disclosure behavior (Chellappa & Sin, 2005; Teltzrow & Kobsa, 2004), showing that the privacy issues they faced were very realistic and representative for this application area.

Initially, it was anticipated that participants would consider information regarding personality traits to be more personal than music preferences and would be less inclined to disclose the information concerned. At the very least, this reluctance towards disclosure was expected from participants with a high level of concern about privacy. This expectation was indeed consistent with the opinions expressed by participants, but this difference in sensitivity did not translate into differences in their disclosure behavior. One could draw two different conclusions from this finding:

- Storage of a model of users' personalities is less sensitive with respect to privacy than was initially expected; removing one of the most serious barriers for its acceptance as a basis of personalization (this was reported before about the pilot of this study, see Perik et al., 2004).
- Users may need to be protected from disclosing personal information too easily in contexts where it does not fulfill the legitimacy criterion (Iachello & Abowd, 2005). For personality traits to be viable as a user-modeling approach, future research should provide a thorough understanding of privacy risks relating to misuse or leaks of personality profiles.

Another expectation during the set up of the experiment was that participants would balance privacy costs against expected benefits from personalization and would vary their behavior through the experiment accordingly. For example, appreciation of music should encourage them to become more open to disclosure, or at least some individuals should modify their disclosure choices according to the recipient of the information they have disclosed.

Surprisingly, such a trade-off did not take place. The vast majority of participants selected a specific level of disclosure throughout the experiment and kept it constant throughout the experimental conditions. Furthermore, the quality of the recommendations based on personality traits was perceived to be lower than those based on music preferences. So, the personality-based recommender system seemed to involve a higher risk and to provide lower benefits, yet participants still chose similar levels of disclosure for music preferences and personality traits. An explanation for this mismatch of perceived risks and disclosure behavior could be because the difference in sensitivity between music preferences and personality traits is small or because the benefits they experienced did not justify changing disclosure. However, the questionnaire and interview data reported do not support this latter explanation. An alternative explanation, given the novelty of profiling the personality of users, could be that curiosity about the effect of personality traits on their recommendations drove participants to experiment and explore this feature, despite their privacy concerns.

Prior to the study it was expected that showing information directly to other users might be considered as more risky than the mere comparison of user data by the system. However, no difference in disclosure was found between these situations, and participants' comments did not support this expectation either. Participants said they were somewhat hesitant or cautious in their disclosure choices since they did not know exactly what would happen with the information involved or who would see the information.

When studying privacy, it is important that the privacy dilemmas are actually experienced as such (as was the case in the study described here). Otherwise, ecological validity is compromised as the risk-situation in the study may deviate substantially from the real-world setting to which the researcher wants to generalize (Riegelsberger, 2005). Also, the system should provide benefits to participants that measure up to current offerings. In practice this could mean it is necessary to carry out a pilot study to confirm the quality of the system itself before using it to study privacy.

In this study ecological validity was addressed in two ways: the music recommender service was set up to be used as any other music service, and participants were exposed to actual risks of disclosure of information. Depending on participants' choices, their personal information would actually be used by the system or shown to other people. As such, participants' were exposed to a real risk of other people and/or third parties accessing their personal information.

Depending on the hypothesis tested, it is necessary to check that the privacy dilemmas introduced as a manipulation are experienced indeed as such by participants and that they do also produce the expected range of behaviors. For example, in the study presented a check was carried out to verify that personality traits and music preferences are perceived to be sensitive. Furthermore, the quality of the recommendations was assessed. However, the trade-off between costs and benefits in the study was not evident, probably because the variations were not large enough to motivate participants to adapt their disclosure during the experiment. In order to study dynamic modification of disclosure preferences, a pilot study should be carried out first to check that the variation in costs and benefits is sufficient to motivate disclosure behavior that varies across the choice situations of the experiment.

The results of this study show that the question of whether or not disclosure is anonymous is more important than the type of information disclosed or the situation involved. Regardless of the type of information or the way it is going to be used, some participants were particularly anxious to safeguard their anonymity. The study by Berendt et al. (2005) also identified a group of participants who were primarily concerned about their identity. Other studies indicate the influence of identification on information disclosure; however, they do not distinguish groups of users on the basis of this influence (see e.g. Ackerman et al., 1999). Future research could explore the potential of segmenting users on the basis of their need for anonymity versus their general privacy preferences.

A common element in the results described is a discrepancy between the privacy attitudes stated in questionnaires and interviews and people's actual behavior. The most obvious difference is that personality traits were considered by more people to be more sensitive than music preferences, yet the extent to which these two types of information were disclosed was practically identical. Even some privacy-concerned individuals chose to disclose their profile and identity information despite their self-reported concerns about such disclosure.

As mentioned already, a similar discrepancy between privacy attitudes and behavior is found in the study by Spiekermann et al. (2001) or Berendt et al. (2005) in the context of disclosing personal data to a shopping 'bot'. Their findings could be challenged on four accounts. Firstly, experimental tasks were conducted in the context of a laboratory, which may influence participants' perception of privacy. Secondly, attitudes were measured prior to the behavior and in the absence of a specific task context. Thirdly, participants were explicitly shown privacy statements of the companies involved before starting their shopping experience, which may have raised their awareness of privacy issues. The present study is consistent in its findings (albeit in a different application domain) while addressing these threats. The Music Recommender appeared to be similar in every way and was used in similar situations to any Internet-based recommendation service. Furthermore, participants were on the whole not aware of the focus on privacy and experienced the privacy risks as real.

The study by Ackerman et al. (1999) had also found that some participants were quite willing to disclose personal data regardless of whether or not they reported a high level of concern about privacy. However, their study involved a survey in which participants did not experience the actual consequences of their stated disclosure behavior. The present study provides stronger evidence of this discrepancy as it relates to surveyed attitudes regarding a specific context after the relevant disclosure choices had been made.

Regarding instruments that exist for measuring privacy-related attitudes, the PAQ and PSI inventories did not give sufficient insight into actual disclosure behavior. It seems that the development of standardized and validated instruments for assessing general privacy attitudes would be a useful methodological advance. In contrary, the simple questions concerning the worries people had about disclosing music preferences and personality traits did form a good indication of actual disclosure behavior. This emphasizes that it is important to assess attitudes in a way that relates closely to the context of interest, since it is known that attitudes expressed outside a specific context are very poor predictors of actual behavior (Ajzen & Fishbein, 2005).

The interviews turned out to be invaluable for understanding participants' motivation for disclosure. Since participants were not informed about the study's focus on privacy before answering the questionnaire, some of their answers were not straightforward in their implications for privacy. The qualitative data obtained in interviews allowed the experimenter to clarify ambiguous comments made in the questionnaire.

The chosen setup provided great control over the experimental conditions, although it took a lot of time and effort to build the application for the Music Recommender service. Nevertheless, one could question the external validity of such an experimental setup: as discussed above, the mere thought of participating in research may change some people's concerns about privacy. Potentially, these issues could be overcome by using an existing service and logging actual use. However, ethical issues regarding deception arise because data cannot be logged without notifying the users a priori. If permission is obtained to collect user data for research purposes then this may influence user behavior in very similar ways to the purpose-built setup.

Alternatively, people's behavior and motivations regarding existing services could be investigated by means of the Experience Sampling Method. This method intends to obtain random samples from people's experiences in everyday-life (Hormuth, 1986), such as those related to activity, social interaction, location, psychological state, and thoughts (Csikszentmihalyi & Larson, 1987). In an Experience Sampling study participants carry a device and are instructed to report their experiences immediately whenever they receive a signal (Hormuth, 1986). The potential use of Experience Sampling for the evaluation process of ubiquitous computing was also addressed by Consolvo & Walker (2003).

Analysis of the use of an existing application gives less control over the context in which disclosure choices are made. This may cause difficulties in eliminating conflicting variables, in ensuring a balanced sample in surveying opinions at appropriate points in time, and in obtaining the right logs. This difficulty of applying proper research methodologies to study privacy attitudes and behavior has been addressed in workshops (Romero et al., 2005; Patil et al., 2006).

2.5 CONCLUSIONS

The aim of this study has been to examine how specific types and uses of personal information would influence people's privacy decisions and attitudes. For this purpose participants used two different Music Recommender systems: one based on music preferences and one based on personality traits. Participants were asked whether or not the system was allowed to use their personal information for either profile matching within the system or for direct disclosure to other users. Participants experienced four choice situations in which they could choose the desired level of disclosure. A combination of logging disclosure behavior, questionnaires and interviews made it possible to study disclosure behavior, the sensitivity of personality as an element of user modeling and the relationship between attitudes and behavior in this domain.

The type of information (music preferences, personality traits) and the intended use of the information (collaborative filtering and access by other users) did not impact upon disclosure behavior. On the other hand, it appears that identity information in particular was very important to some participants and less so to others.

The study suggests that modeling personality traits of users does not present an acceptance barrier relating to privacy concerns (see also Perik et al., 2004). However, the potential misuse of this information is not yet understood sufficiently. This lack of understanding of the potential risks of modeling the personality traits makes users unable to guard their privacy, which raises practical and ethical problems relating to the development of related services. Considering the ease with which users disclose information that they consider personal, safeguards may be needed to prevent disclosure in contexts in which this is not safe. Further research needs to be conducted to see if the findings relating to personality can be extended to other applications as well.

This research contributes to existing literature on personalized systems and privacy in several ways. The current study has provided strong evidence regarding the discrepancy between stated attitudes and user behavior relating to privacy. Personality traits were claimed to be sensitive information yet they were disclosed to much the same extent as the less sensitive music preferences, despite participants' claims that they balance costs against the benefits of disclosure. Even privacy-concerned individuals disclosed their profile information, including their identity information.

This study also illustrates the difficulties of doing ethically responsible and ecologically valid experimental work in the domain of HCI and privacy. Furthermore, limitations of existing inventories for surveying privacy preferences have been proposed. Sensitivity towards disclosing one's identity seems to be more important to people than the other information they exchange.

Important implications for future empirical studies concerning privacy are: triangulation of different data-collection methods, representative sampling by profiling the pool of participants with an established privacy attitudes inventory, exposure to realistic privacy risks (unlike in privacy surveys where participants are not confronted with the consequences of their self-proclaimed behavior), making sure these risks are not mitigated by trust in the experimenter and, finally, disguising the experimenter's interest in privacy (since this may influence participants' behavior). Using a purpose-specific application that provides partial control for the context of disclosure was an interesting but laborious approach; compared to the alternative of logging existing services it provided more control over the context of disclosure and allowed the sampling of user opinions to be timed very precisely with regard to the use of the system.

3 Evaluation of Privacy Guidelines

This chapter[6] *examines whether applying principles of Fair Information Practices is an adequate approach to address people's privacy concerns in an Ambient Intelligence environment. Taking the perspective of the user, it describes four studies that were conducted regarding the interpretation and perceived importance of privacy guidelines to potential users of ambient intelligent health care systems. The studies aimed to address the following questions:*

- *What are people's information privacy concerns?*
- *How to communicate privacy consequences?*

First two pilot studies that were aimed at investigating the possibilities of using scenarios to study privacy issues in a personalized system will be presented. These studies illustrate the limits to the ability of users to interpret correctly privacy statements. Based on the results of these pilot studies two follow-up studies were conducted.

One experiment was conducted that compared people's ability to judge correctly compliance to privacy guidelines when scenarios are presented in video versus textual form. Again, it was found that privacy-related statements (both video and text) are hard to understand. A large number of erroneous judgments were made regardless of medium. Furthermore, interpretation varied across media. Comprehension of privacy statements could be improved, if a text scenario is preceded by a video scenario.

Also, an empirical study regarding the relative importance of complying with privacy related guidelines in the context of a health monitoring system was conducted. Participants were confronted with text-based scenarios describing privacy related aspects of a health monitoring service for daily use at home. Participants assessed the relative importance of privacy guidelines for the protection of personal data. The guidelines that relate to insight and openness were most valued. The guidelines relating to modification and data quality were valued least by most participants in this context.

[6] This chapter is based on the following publications: Garde-Perik, E. van de, Markopoulos, P., & Ruyter, B. de. (2006b). Privacy policies and text-based empirical research: Methodological issues. *CHI 2006 Workshop on Privacy & HCI: Methodologies for Studying Privacy Issues*; Garde-Perik, E. van de, Markopoulos, P., & Ruyter, B. de (2006a). On the relative importance of privacy guidelines for ambient health care. *NordiCHI 2006*, 377-380; Mahmud, Al A., Kaptein, M., Moran, O., Garde-Perik, E. van de, & Markopoulos, P. (2007). Understanding compliance to privacy guidelines using text- and video-based scenarios. *Interact 2007*, 156-168.

3.1 INTRODUCTION

A large body of work relating to privacy and information systems, dating back to the work of Westin has focused on the use of guidelines for regulating practices regarding the handling of personal data, whether that is by private businesses or non-profit organizations and the state. The initial principles of Fair Information Practices formulated in the US during that era (US Department of HEW, 1973) have developed into the current Organization of Economic Cooperation and Development (OECD) guidelines (OECD, 1980). This chapter examines whether applying the principles of Fair Information Practices is an adequate approach to address people's privacy concerns in a personalized or ambient intelligence environment.

This chapter will present two pilot studies and two follow-up studies relating to the interpretation and importance of privacy guidelines from the perspective of the user. A general introduction to the four studies of this chapter will be provided. First, it will show that Fair Information Practices are seen as a possible way to address people's privacy concerns in an Ambient Intelligence environment. Next, one instance of these practices, namely the guidelines by the OECD, will be discussed since all of the studies in this chapter are based on these OECD guidelines.

Ideally, the privacy and trust implications of new systems should be investigated using fully working prototypes, since it is very difficult for potential users to envision the actual privacy consequences of a future application. In earlier phases of a design project where this is not yet feasible alternative approaches to assessing user privacy concerns are needed that do not rely on users experiencing a working prototype.

In order to make reported attitudes regarding privacy correspond better to actual privacy related behaviors, one possibility is to contextualize inquiry with the use of scenarios, i.e. to inquire regarding particular actions in the context of a specific situation described in a scenario. Human-computer interaction research and interaction design practice have endorsed scenarios as a means to contextualize inquiry and design activities (e.g., Carroll, 1995). Scenarios for human-computer interaction are typically delivered as narrative texts, but are often also shown as storyboards or short videos.

Indeed several recent empirical investigations concerning privacy and ubiquitous computing systems are either direct questionnaires about people's attitudes, or based on scenarios delivered to them in textual or video form (Ackerman et al., 1999; Günther & Spiekermann, 2005; Spiekermann et al., 2001).

Textual scenarios were used by Ackerman et al. (1999) as a means to investigate how people would respond to situations where personal information is collected. Participants were asked about their concerns through specific scenarios involving online data collection. One scenario, for example, asked respondents whether they would be more or less likely to provide data to a website with a privacy policy that explained that their information would be removed from the site's database if they did not return to the site for three months.

In the study by Günther and Spiekermann (2005) video scenarios were used to illustrate RFID technology for an automated supermarket check-out. Participants were shown different PETs (Privacy Enhancing Technologies) available for controlling their privacy. After viewing the video scenario participants were questioned about privacy preferences and perceived control in the scenario presented to them. It turned out that participants feared losing their privacy due to the introduction of RFID.

In the studies of this chapter scenarios will be used to contextualize the inquiry regarding the interpretation and importance of privacy guidelines. All four studies use scenarios in textual form, and one study (study 3, see section 3.4) will use scenarios in both textual and video form.

Privacy researchers have proposed collections of design principles and guidelines for ensuring privacy through interaction design. Jiang et al. (2002) proposed principles for regulating the flow of information in ubiquitous systems. Chung et al. (2004) proposed a set of design patterns to solve privacy problems. Others have adopted principles originating from legislation for technical systems and privacy, such as the five principles of Fair Information Practices (Culnan & Armstrong, 1999; Langheinrich, 2001) prescribing how to deal with collection, storage and use of personal data.

There are many variations of Fair Information Practices. Each country seems to have its own rules and regulations. However, due to the high similarity between the various principles, this chapter will focus on only one set of guidelines, namely those by the OECD (1980). The OECD is an organization consisting of 30 member countries. On 23 September 1980 these countries adopted the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. These OECD guidelines were formulated in reaction to the increased development of automatic data processing. The guidelines intended to harmonize national privacy legislation and to support human rights, such as the unlawful storage of personal data, the storage of inaccurate personal data, or the abuse or unauthorized disclosure of such data. Hence, the OECD guidelines represent international consensus on general guidance concerning the collection and management of personal information.

Even though the OECD guidelines were formulated before the vision of Ambient Intelligence arose, the original context of the guidelines is relevant since Ambient Intelligence is based on automated data processing. Many scholars refer to the solution that Fair Information Practices may offer in minimizing privacy concerns related to Ambient Intelligence. However, hardly any research to date provides empirical evidence regarding the relevance and importance of these principles for end-user acceptance of ambient intelligence systems and services. The studies in this chapter aim to address this issue.

The OECD guidelines are based on eight core principles (see first two columns of Table 3.1). They play an important role in assisting governments, business and consumer representatives in their efforts to protect privacy and personal data, and in preventing unnecessary restrictions to data flows across borders, both on and off line.

The original OECD principles are too long and include too many sub clauses to be used effectively in a user study. Therefore, the original OECD guidelines were shortened in an attempt to represent their main content. The second column of Table 3.1 shows the original OECD principles as well as the elements that are included in the guidelines as used in this chapter (printed in italics). The actual descriptions of the guidelines as they are used in this chapter and the differences from the original OECD principles are listed in the last two columns of Table 3.1.

Table 3.1. Overview of the FIP principles by the OECD and as used in this chapter

Principle	OECD (1980)	This chapter	Differences
Collection Limitation	There should be limits to the collection of *personal data* and any such data *should be obtained* by lawful and fair means and, where appropriate, *with the knowledge* or consent *of the data subject*.	Data is collected with the knowledge of the user, or in other words, that the user is informed about the type of data that is collected	Omitted is the part that: requires collection by lawful and fair means.
Data Quality	*Personal data should be relevant to the purposes for which they are to be used*, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.	The relevance of the collected data to the purposes for which they are to be used	Omitted is the part that: this data is accurate, complete and kept up-to-date.
Purpose Specification	*The purposes for which personal data are collected should be specified* not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.	The purposes for which the data are collected are specified	Omitted is the part that: the timing of Purpose Specification, and that data use is limited to the fulfillment of those purposes, and that each occasion of change of purpose should be specified as well.
Use Limitation	*Personal data should not be* disclosed, made available or otherwise *used for purposes other than those specified* in accordance with Purpose Specification Principle except: a) with the consent of the data subject; or b) by the authority of law.	Data is not used for purposes other than those specified	Omitted is the part that: the data is not be disclosed, or made available for purposes other than those specified, and that there are exceptions in case of consent of the data subject and by authority of law.
Security Safeguards	*Personal data should be protected by reasonable security safeguards* against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.	Protection of data by reasonable security safeguards	Omitted is the part that: it offers protection against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

Note: The italicized sections indicate which elements are included in the guidelines of this chapter.

Table 3.1. (continued)

Principle	OECD (1980)	This chapter	Differences
Openness [1]	*There should be a general policy of openness* about developments, practices and policies with respect to personal data. *Means should be* readily *available* of *establishing* the existence and nature of personal data, and the main purposes of their use, as well as *the identity* and usual residence *of the data controller*.	The user is informed about the other parties that have access to the collected data	Somewhat different from: a general policy of openness about developments, practices and policies with respect to personal data, and the availability of means to establish the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
Individual Participation [2]	*An individual should have the right*: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) *to have communicated to him, data relating to him* (within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him); c) to be given reasons if a request made under subsections(a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him *and*, if the challenge is successful *to have the data erased, rectified*, completed or amended.	-	Individual Participation requires that individuals are able to get a confirmation about collected data, or getting data communicated; if either of these is denied then the reasons should be given, and the person should be able to challenge data. In this chapter this principle was split to two parts, Insight (IN) and Modification (MO) to allow compliance questions to be asked unambiguously.
Insight	-	The possibility of inspecting stored data	Originally part of Individual Participation. This is used instead of: getting a confirmation or having data communicated.
Modification	-	The possibility to modify or erase collected data	Originally part of Individual Participation.
Accountability [3]	A data controller should be accountable for complying with measures which give effect to the principles stated above.	-	The accountability principle is omitted in this chapter since it implies general compliance with all other guidelines.

Note: 1) Openness in this chapter is not identical to the italicized sections; but the notion is the same 2) Individual Participation in this chapter is split in two parts: Insight & modification. The formulation is not identical to the italicized sections; but the notion is the same. 3) Accountability is omitted in this chapter.

Two pilot studies were conducted to establish whether or not users understand textual descriptions of privacy implications of a system. These pilot studies are described in sections 3.2 and 3.3. Based on the findings of the pilot studies two-follow up studies were performed. One study is presented on people's ability to correctly judge compliance to these guidelines for both video and textual scenarios (section 3.4). Finally in section 3.5, a study will be presented that investigated whether or not some of the OECD guidelines have more influence on user acceptance of a system than others.

3.2 STUDY 1[7]

3.2.1 Introduction to Study 1

As mentioned before in the general introduction it is very difficult for potential users to envision the actual privacy consequences of a future application. A privacy policy is intended to inform users about these consequences, prescribing how the system deals with collection, storage and use of personal data. However, it should be explored whether privacy policies are effective in this. Therefore, the aim of this pilot study is to investigate whether people are able to comprehend textual descriptions of the privacy consequences of a health related system as based on the OECD principles for Fair Information Practices.

3.2.2 Method

Design

The eight guidelines of this chapter, as shown in the third column of Table 3.1 were used for two different purposes. First of all, they were used for the formulation of eight system features (see Table 3.2). And secondly, two usage scenarios were created based on compliant and deviant versions of the guidelines (see Table 3.3).

Table 3.2. Guidelines used in Study 1 and implications of their compliance for the system features

Guideline	Acronym	Implication of guideline compliance in terms of system feature
Collection Limitation	CL	John is informed in advance about the type of data that will be collected
Purpose Specification	PS	John is informed about the use/purpose of data collection
Data Quality	DQ	All the data that is collected is relevant to the main purpose
Use Limitation	UL	The data will be used only to serve the main purpose
Openness	OP	John is informed about the other parties that have access to his data
Security Safeguards	SS	The data is securely stored
Insight	IN	John can get insight into the data that is stored about him
Modification	MO	John has the possibility to make changes in the stored data

[7] This section is based on the following publication: Garde-Perik, E. van de, Markopoulos, P., & Ruyter, B. de. (2006b). Privacy policies and text-based empirical research: Methodological issues. *CHI 2006 Workshop on Privacy & HCI: Methodologies for Studying Privacy Issues.*

Table 3.3. Scenarios for system descriptions used in Study 1

	Health support system 1	Health support system 2
CL	The health support system *does not inform* John about the various types of information that are collected and stored. (D)	The health support system *informs* John that it collects and stores information about weight, blood pressure, pulse and glucose levels. (C)
PS	The system *informs* John that the collected information will be used to monitor his health parameters. (C)	The system *does not inform* John what the collected information will be used for. (D)
DQ	The system *collects information that is relevant for monitoring John's health.* (C)	The system *may also collect information that is not related to health monitoring, for example the amount of time John spend watching TV, or registering what websites he visited.* (D)
UL	The collected information *may be disclosed and used* for purposes other than those John is informed about, such as marketing or advertising. (D)	The collected information *will not be disclosed or used* for purposes other than those John is informed about, such as marketing or advertising. (C)
OP	John *knows* what services, organizations or individuals have access to his personal information. (C)	John *does not know* what services, organizations or individuals have access to his personal information. (D)
SS	The stored information *is not protected* by any means against security risks. (D)	The stored information *is protected* against risks by security safeguards. (C)
IN	John *can not inspect* all the information that is stored about him. (D)	John *can inspect* all the information that is stored about him. (C)
MO	John *can not modify or erase* the information that is stored about him. (D)	John *can modify or erase* the information that is stored about him. (C)

Note: In the study the description were presented as continuous text. This figure shows the descriptions used for each guideline separately. The difference in formulation between the deviant and compliant form is italicized. The compliance or deviance with guidelines is indicated in brackets (C = Compliant, D = Deviant).

Participants were asked to evaluate the compliance or deviance from the guidelines for both system descriptions. More specifically they were presented with the descriptions of the eight system features (see Table 3.2), and were asked to indicate whether the scenario provides the feature or not (in other words whether the scenario is compliant with the underlying guideline or not). The expectations were that participants would correctly interpret the scenario fragments which would allow us to use such statements in further research. It has to be noted, that this pre-study was conducted as a measure of caution before investing effort in the main study and with the intention to fine-tune the phrasing of the attributes in advance.

Participants

For this preliminary study colleagues from the University and a Research lab were asked to evaluate the two system descriptions. Nine persons, mainly PhD students, participated in the pilot. The participants have an advanced knowledge of English as a foreign language.

Materials

For this pilot study the main material was a paper-based questionnaire (see Appendix B1). The first page described a possible context of system use, and the purpose of the questionnaire. The next page included the first system description (see left column of Table 3.3) and the corresponding eight evaluation questions. The system description was nothing more then a summation of the eight guidelines in either the compliant or deviant form. In the evaluation questions participants were asked to judge guideline compliance by indicating whether or not the system provided a certain system feature, e.g. for the guideline of collection limitation: “John is informed in advance about the type of data that will be collected (Yes/No)”. The phrasing of system features is shown in Table 3.2.

After answering all eight evaluation questions for the first system, participants were shown a second system description (see right column of Table 3.3) and the same evaluation questions were asked. Finally, participants were asked to rewrite parts of the original system description in case their interpretation was opposite to how they were intended. This was done for both systems separately.

Measures

This pilot study measured whether participants correctly interpreted the eight system features as deviant or compliant with the shortened OECD-based guidelines for both system descriptions. Finally for all system features that were interpreted differently than intended, the participants were asked to rewrite the original text in such a way that it would describe the system feature as intended. This was done in order to elicit their understanding of the feature description. E.g., if a participant would have indicated that the system provides a feature such that “John is informed about the type of data that will be collected”, whereas the system described the opposite, then the participant was asked to reformulate the concerning section in such a way that the system does not provide this feature. After the completion of the questionnaire, with most participants a short discussion was held about the problems of understanding the scenario text.

Procedure

Participants were asked for fifteen minutes of their time to take part in a questionnaire. In total nine people participated. Participants were informed about the purpose of the pilot study, namely to investigate whether the questions and text to be used in future research were clear enough. The participants filled out the questionnaire page by page and handed each completed page to the experimenter. This way the experimenter could check which questions needed to be asked for the re-writing part of the questionnaire.

3.2.3 Results

In total 9 participants completed the questionnaire about the evaluation of two system descriptions and the re-writing of differently interpreted fragments. It took most participants over 15 minutes to complete the questionnaire.

None of the eight system features was interpreted as intended by all participants for both system descriptions. Of the eight system features in the first system description, only half were interpreted as intended by all participants. In case of the second system description none of the system features were correctly interpreted by all participants (see also Table 3.4). Overall system 2 was interpreted opposite to the intentions more often (22

Table 3.4. Incorrect interpretations of the system features in Study 1

	System 1		System 2		Total
Collection Limitation	D	4	C	2	6*
Purpose Specification	C	4	D	4	8*
Data Quality	C	5	D	2	7
Use Limitation	D	0	C	8	8
Openness	C	2	D	3	5
Security Safeguards	D	0	C	1	1
Insight	D	0	C	1	1
Modification	D	0	C	1	1
Deviant features	4		9		13
Compliant features	11		13		24
System total	15		22		

Note: Values represent number of incorrect interpretations per system feature (for system description 1, system description 2 and for both descriptions together). D = Deviant from guideline. C = Compliant with guideline. System total represents total number of incorrect interpretations per system description. * One participant incorrectly interpreted both descriptions of the system feature.

instances) than system 1 (15 instances). This difference in correct interpretation of the two system descriptions was mainly caused by two guidelines: Data quality and use limitation.

It turns out that especially with regard to the system features data quality, purpose specification and use limitation participants made reverse interpretations. Also, the descriptions regarding collection limitation, and openness where frequently interpreted opposite to the original intentions. Based on participants' reformulation of the original system descriptions and the short discussions held with participants after completing the questionnaire some insight was gained regarding underlying causes of the confusions.

Also, it turned out that the statement for collection limitation ("The health support system informs John that it collects and stores information about weight, blood pressure, pulse and glucose levels") is easily confused with the way the information will or might be used (purpose specification & use limitation). As if having information about what data is collected is an indication of how the information will be used. Even though the user may be informed that only health related information will be collected by the health support system, this is no guarantee that it will only be used for health related purposes, it may as well be used for marketing or advertising. But apparently this distinction is not realized by the participants. A participant who was asked to rewrite the original section that related to collection limitation ("John is informed in advance about the type of data that will be collected") rewrote the section as: *"The system informs John what the collected information will be used for"*. So, this person did not write about being informed about the data collection (collection limitation), but about being informed about the way the information will be used (purpose specification).

The first system description did not comply with collection limitation, i.e. there was no information provided about the type of data that was collected. However, the fact that this first system was compliant with data quality (relevance of data collection for a specific purpose), led many people to believe that the user would know what type of data was collected (collection limitation).

There was also confusion about the distinction between the relevance of collected data for a specific purpose (data quality) and the actual use of the information (use limitation). One participant rewrote the data quality section as: *“The collected information will solely be used to monitor health conditions”*. Despite the fact that it is likely in case only data relevant to health monitoring is collected, that it will also be used for a health related purpose, this is not what the text states (or provides guarantees for). Again, the information may be used for marketing or advertising purposes as well. Another participant was asked to rewrite the section concerning use limitation. This person wrote the following: *“The system will only collect information that is related to health monitoring”*, which is clearly an expression that is compliant with data quality and not so much with how the information might be used (use limitation).

Also information about the way the collected information would be used (purpose specification) was frequently confused with the relevance of the collected information to a specific purpose (data quality). Yet again, these are two different concepts, one is about the use of information, and the other indicates whether or not redundant or irrelevant data is collected besides information that is relevant to the system purpose. Even though both are related to the system purpose, one can be compliant, and the other may be deviant.
Another confusion that occurred was the lack of distinction between information about the way the collected information would be used (purpose specification) and the actual use of information for certain purposes (use limitation). For example, one participant who was asked to re-write the section concerning the fact that “John is informed about the use / purpose of the data collection” wrote the following: *“The collected information may only be used for purposes John is informed about”*. Despite the fact that this rewritten version conveys being informed about the purpose of the data collection (purpose specification), it also includes a reference to the way that the data will be used (which corresponds to the principle of use limitation).

Even though one may expect that deviant system descriptions are less often correctly interpreted due to negations in the descriptions themselves and due to the opposed phrasing compared to the system features, this is not the case. The deviant system descriptions were less often interpreted opposite to the intentions (13 instances in total) than the compliant system descriptions (24 instances in total; see Table 3.4).

The task in which participants were asked to re-write the system description was in some cases frustrating. Participants commented that the loose connection between the sentences made it harder to read and interpret the text.

3.2.4 Discussion and conclusions

The aim of this pilot study was to investigate whether an approach based on scenarios can be used to study user acceptance of personalized systems depending on compliance with Fair Information Practices. Despite the fact that participants mastered the English language at a sufficient level, and had a high level of education, many of the system features were interpreted opposite to the original intentions. This could be an indication of unclear system descriptions, or of an even more substantial problem with the use of scenarios. This will be explored further below.

The system description and evaluation questions were presented in a fixed order. Participants only needed to read the first sentence in order to answer the first evaluation question and the third sentence for answering the third question. Although this may have easily been discovered, it turns out that it was still not easy for participants to interpret the sentences as intended.

The difference in correctness of interpretation between system description 1 and 2, and consequently between deviant and compliant features was to a great extent caused by only two guidelines: Data quality and use limitation. Detailed comparison of the two different versions of the guideline data quality showed that there was a difference in the level of detail and length between the two versions. The deviant version of data quality used in system description 2 contained more detail and was longer in comparison to the compliant version used in system description 1. Interestingly, the compact version was more often misinterpreted (5 instances compared to 2). For use limitation the compliant version used in system description 2 was quite complicated (8 incorrect interpretations compared to 0). It stated that collected information will not be disclosed or used for other purposes, yet it provided examples of what such other purposes might have been.

One may expect that participants need some practice in order to learn how to interpret the text. However, the fact that the second system description was interpreted even worse than the first does not indicate a learning effect. However, it may have been the case that participants were confused by information that was provided to them previously.

It may be that especially sentences with negations are difficult to interpret, but the data does not support such an explanation. Deviant statements were less often interpreted opposite to the intentions than the compliant ones.

The fact that participants confused separate system features, or simply had a looser interpretation of some system features than was justified by the text, has interesting consequences for published privacy policies. If these results apply more generally to similar texts or websites, it would mean that people do not comprehend or internalize what is actually written, but instead jump to conclusions which are not warranted directly by the privacy policy. For example, being informed about the purpose of the data collection was interpreted as if the data will only be used for these purposes. This difference of interpretation is a serious problem for creating a proper understanding of the privacy consequences involved when using a particular system. This may lead to serious privacy conflicts.

This pilot study also shows us something about the possibility to conduct text-based empirical studies to study privacy. Privacy related statements expressed in text, involving the concepts of information collection versus use, require an extremely accurate reading and interpretation of text that cannot be assumed. They originate from a business and legal context, where accuracy and precision in expression is perhaps more to be expected than in a situation where participants approach a system description as hypothetical users. Even the interpretation of relatively simple statements was not unambiguous, perhaps because of the pre-conceptions and expectations of the participants.

For the purposes of privacy research, where such statements are presented to participants as a pre-experiment or post-experiment survey, it seems that it is necessary to be very thorough about testing the ability of subjects to comprehend accurately the questions presented to them or to grasp the fine differences in text scenarios that describe privacy issues.

Participants commented on the difficulty of reading and interpreting a text based on loosely connected sentences – the scenarios that were used lacked a fluent narrative structure to ensure a clear correspondence with the eight privacy attributes. It would be interesting to further explore whether a coherent narrative structure for scenarios, as is typically expected in HCI research (Nardi, 1992; Robertson, 1995; Karat, J. 1995), would still be hampered by these problems.

Another possibility is that the participants joining this pilot were trying to double-guess the researchers, looking for hidden assumptions in the phrasing of the privacy related statements. This does not seem very likely considering the cases where the expression of an attribute was in some cases almost verbatim present in the text.

3.3 STUDY 2

3.3.1 Introduction to Study 2

An attempt was made to improve the system descriptions on the basis of the results of the first pilot study, Study 1. This second pilot study is conducted to establish whether users could better understand these improved textual descriptions of the privacy implications of a health monitoring system.

3.3.2 Method

Design

In principle the second pilot was similar to the first. However, based on the results of Study 1 the original system descriptions were adapted. First of all, it was tried to minimize confusion between the various guidelines by omitting words that seemed to have caused confusion. I.e. the word health parameters was omitted in the guideline dealing about purpose specification, since it might give people the impression that it deals with the type of data being collected. Besides, the scenario fragments would speak of the user John and his diabetes condition. The system features used for evaluation would speak in general terms about the user and the main purpose of the system. This was done to make the distinction between the scenarios and the evaluation questions clearer. Also for this pilot, two complete usage scenarios were created in the same combination as it was used for the Study 1. However the description of the system features was somewhat modified (see Table 3.5).

For this second version pilot it was expected that participants would more frequently interpret the scenario fragments correctly, and that less confusion between fragments would occur.

Participants

For this pilot study, several people (colleagues and acquaintances of the researcher) were asked to evaluate the two system descriptions. Only people that did not have a

Table 3.5. Guidelines used in Study 2 and implications of their compliance for the system features

Guideline	Acronym	Implication of guideline compliance in terms of system feature
Collection Limitation	CL	The user is informed about the type of data that will be collected.
Purpose Specification	PS	The user is informed about the main purpose for which the data will be used.
Data Quality	DQ	The system only collects data that is relevant to the main purpose of the system.
Use Limitation	UL	The data will be used solely to serve the main purpose of the system.
Openness	OP	The user is informed about which other parties have access to the collected data.
Security Safeguards	SS	The data is securely stored.
Insight	IN	The user can inspect the stored personal data.
Modification	MO	The user has the possibility to make changes in the stored data.

Table 3.6. Scenarios for system descriptions used in Study 2

	Health support system 1	Health support system 2
CL	The system *does not inform* John that it will collect data regarding his health, blood pressure, pulse and glucose level. (D)	The system *informs* John that it will collect data regarding his health, blood pressure, pulse and glucose level. (C)
PS	The system *informs* John that data is collected in order to monitor his diabetes condition. (C)	The system *does not inform* John that data is collected in order to monitor his diabetes condition. (D)
DQ	The system informs John that it will *only collect data that is useful for tracking his diabetes condition*. (C)	The system informs John that it *collects also data that is useful for things other than tracking his diabetes condition*. (D)
UL	The system informs John that it *uses his data for other reasons than the main purpose of the system as well*. (D)	The system informs John that it will *not use his data for any other reason than the main purpose of the system*. (C)
OP	The system *informs* John regarding all the organizations or individuals who can access his data. (C)	The system *does not inform* John regarding all the organizations or individuals who can access his data. (D)
SS	The system informs John that his *data is not protected by any security safeguards*. (D)	The system informs John that all his *data is securely stored*. (C)
IN	The system *does not provide* facilities for John to inspect all data collected about him. (D)	The system *provides* facilities for John to inspect all data collected about him. (C)
MO	The system *does not provide* facilities to allow John to modify or erase any data about him. (D)	The system *provides* facilities to allow John to modify or erase any data about him. (C)

Note: In the study the description were presented as continuous text. This figure shows the descriptions used for each guideline separately. The difference in formulation between the deviant and compliant form is italicized. The compliance or deviance with guidelines is indicated in brackets (C = Compliant, D = Deviant).

relation to the research project, or who were not specializing in privacy research were contacted. Also this time 9 persons participated in this pilot. None of the participants in Study 2 took part in Study 1. The participants have sufficient knowledge of English.

Materials

Except for the actual text of the system descriptions, the materials used in the second version of this study were similar to the ones used in the first version. Table 3.6 shows both system descriptions that were used in this second pilot. Appendix B2 provides the questionnaire used in this pilot study.

Measures

The measures taken in this second pilot were similar to those in Study 1. The following data was obtained:

- Correctness of interpretation of all deviant and compliant system features;
- A reformulation of the original text in the participant's own words for each system feature that was incorrectly interpreted;
- A concluding discussion about the problems regarding the interpretation of the scenario text was held with some participants.

Procedure

Participants were asked to pilot a questionnaire. The remainder of the procedure was similar to the first version of the pilot. Participants were first informed about the purpose of the pilot study. Then participants filled out the questionnaire and handed each completed page to the experimenter. Finally, participants were asked to rewrite those system features that were interpreted differently than intended and in some cases a short discussion was held for clarification.

3.3.3 Results

Nine participants completed the questionnaire. There were quite some differences between respondents with regard to the amount of time needed to complete the questionnaire. Some were done in less than 10 minutes, whereas it took others almost half an hour.

Two of the eight system features, purpose specification and modification, were interpreted as intended by all participants for both system descriptions (see Table 3.7). For the first system description these were the only two system features that were interpreted as intended by all participants. In case of the second system description five of the system features were correctly interpreted by all participants. Overall the eight features of system 1 were interpreted opposite to the intentions more often (13 instances) than of system 2 (6 instances).

It turns out that especially the system features concerning data quality, use limitation and collection limitation led to reverse interpretations. To a lesser extent the description regarding openness, security safeguards and insight were interpreted opposite to the original intentions.

Of the 7 participants who were confused about the interpretation of the data quality fragment, 3 correctly rephrased the section when they were asked to reformulate it. The other 4 participants were confused by various fragments, either dealing with use limitation, collection limitation or purpose specification. For example, one participant indicated with reference to the data quality system feature that: *"The system uses his data for other reasons than the main purpose of the system as well"*. Here data quality is confused with the use limitation guideline. Similar confusions occurred in the first pilot.

Table 3.7. Incorrect interpretations of the system features in Study 2

	System 1		System 2		Total
Collection Limitation	D	2	C	1	3
Purpose Specification	C	0	D	0	0
Data Quality	C	5	D	2	7
Use Limitation	D	1	C	3	4
Openness	C	2	D	0	2
Security Safeguards	D	2	C	0	2
Insight	D	1	C	0	1
Modification	D	0	C	0	0
Deviant features	6		2		8
Compliant features	7		4		11
System total	13		6		

Note: Values represent number of incorrect interpretations per system feature (for system description 1, system description 2 and for both descriptions together). D = Deviant from guideline. C = Compliant with guideline. System total represents total number of incorrect interpretations per system description.

Also 1 of the 4 participants, who misinterpreted the fragment about use limitation, confused this with data quality. This person rewrote the use limitation system feature "The data will be used solely to serve the main purpose of the system" as follows: *"The system informs John that it collects data that is only useful for tracking his diabetes condition"*. Two other participants correctly rephrased the section, whereas one participant was unable to rephrase it.

Of the 3 participants who were confused about the interpretation of the fragment dealing with collection limitation, 2 correctly rephrased the concerning section. The third person was still confused about the fact that information could be used for other purposes (use limitation) and not being informed about the purposes for which they will be used (Purpose specification).

Most of the other interpretations that were opposite to how they were intended were solved at the point of reformulating the section. Besides that, there was one participant who was probably confused because of the English language, and yet another participant had a very personal interpretation of secure storage, namely that it would not be possible to alter data concerning one's condition.

Table 3.8 shows the improvement in interpretations in the second pilot study compared to the first. Most system features were more frequently interpreted correctly in the second pilot. Only the interpretations of data quality and insight were unchanged, and the interpretation of security safeguards slightly deteriorated.
In both pilot studies the deviant system descriptions were less often interpreted opposite to the original intentions (8 instances) than the compliant system descriptions (11 instances in total, see Table 3.7).

Table 3.8. Incorrect interpretations per system feature for both pilot studies compared

	Overall Study 1	Overall Study 2
Collection limitation	5	3
Purpose Specification	7	0
Data Quality	7	7
Use Limitation	8	4
Openness	5	2
Security Safeguards	1	2
Insight	1	1
Modification	1	0
Total	35	19

3.3.4 Discussion and conclusions

The aim of the two pilot studies was to investigate whether an approach based on scenarios can be used to study user acceptance of personalized systems depending on compliance with Fair Information Practices. After the adaptations that were made to the scenarios based on the results of the first version, the interpretations of the second version were more often in accordance with the intentions. However, limitations to the comprehension of statements describing privacy policies based on guidelines such as those by the OECD still remained.

Also in this second pilot the system description and evaluation questions were presented in a fixed order, such that the first sentence of the system description related to the first evaluation question. However, it wasn’t easy for participants to interpret the sentences as intended.

One may expect that participants need some practice in order to learn how to interpret the text. In this second pilot, participants more often correctly interpreted the fragments of the second system. This gives the impression that participants better understood the provided task, and did benefit from their practice with the first system description. It also indicates that participants’ confusion about the interpretation of each system feature was not entirely due to the preceding text; otherwise the second system would have been interpreted worse.

Although it seems likely that especially fragments with negations are difficult to interpret, the deviant statements were less often interpreted opposite to how they were intended than the compliant ones in both versions of the story. This indicates that it is not the complexity of the negation that makes the text difficult to comprehend, but that there is something else that complicates the understanding of the guidelines. Perhaps it is the complex nature of legal texts that makes it difficult to comprehend.

Although, there was less confusion about separate system features in the second pilot compared to the first pilot, it still occurred that participants had a looser interpretation of some system features. People do not comprehend or internalize what is actually written, but instead jump to conclusions which are not warranted directly by the privacy policy.

The results of the two pilot studies imply caution in two respects. In empirical research regarding privacy the exact interpretations of privacy related questions and descriptions must be tested rigorously. And secondly, guidelines and experiments in favor of stating privacy policies in statements, however simple, should be scrutinized as the correct interpretation of related statements cannot be assumed.

Two different studies (Berendt et al., 2005; Kobsa & Teltzrow, 2005) investigated the influence of privacy statements on disclosure of information. However, neither of these studies tested the interpretation of the statements provided to participants.

In the laboratory experiment by Berendt et al. (2005) participants took a virtual shopping trip. Participants were asked to sign the store's privacy statement. One group of participants received a privacy statement that informed that user data would be handed over to a reputable company and advised them of their rights under the European Union Directive on Data Protection, the other group of participants received a privacy statement which did not mention the EU Directive but instead told them it was unknown how the data would be used. The type of privacy statement did not impact disclosure behavior significantly. However, the privacy statement which referred to the EU Directive induced slightly more participants to provide their address.

In the experiment by Kobsa and Teltzrow (2005) participants were asked to test a new version of an online bookstore with an intelligent book recommendation engine. The standard privacy policy of the web retailer was provided on the website, but two different conditions were used regarding the explanation about privacy practices and personalization benefits that participants would receive. One group of participants received contextual explanations describing the consequences of disclosure; the other group did not get these explanations. The contextual communication of privacy practices and personalization benefits turned out to have a significant positive effect on users' willingness to share personal data.

The pilot study reported in this section, suggests that the ability to comprehend privacy statements represents a threat for related results. It would be necessary to verify participants' interpretation of the various privacy statements used in the studies by Berendt et al. (2005) and by Kobsa and Teltzrow (2005), in order to be sure what caused the difference in behavior for both studies. As a methodological guideline for related privacy research, checks for correct interpretation of privacy statements should be carried out and reported along with the eventual results.

3.3.5 Introduction to the follow-up studies

Based on the results of the two pilot studies (Study 1 & 2) discussed before, two simultaneous follow-up studies were conducted. These studies will be described in the following two sections. The first study to be described, study 3 (see section 3.4), contained a comparison of video and text scenarios for people's comprehension of compliance to privacy guidelines. The other follow-up study, study 4 (see section 3.5) encompassed an investigation of the relative importance of privacy guidelines.

3.4 STUDY 3[8]

3.4.1 Introduction to Study 3

In this third study, it is examined whether the interpretation of scenarios relating to privacy are affected by the medium in which the scenario is delivered. In the following section, the context of this study and the reasons behind the hypothesis that a medium effect exists with respect to the ability of informants to discuss privacy-related issues are presented.

This third study will be useful to the field of Human Computer Interaction in two ways. The results of this study will provide insight into the reliability of text or video scenarios for surveying attitudinal responses to different system designs. Secondly, the results will provide quantitative evidence regarding the difficulty of conveying privacy related functions and policies to users; earlier research has shown that users often do not read such policies (Kobsa & Teltzrow, 2005; Milne & Culnan, 2004) or are not able to comprehend them (see Study 1 & 2 reported in this chapter; Jensen & Potts, 2004; Milne & Culnan, 2004).

Jensen and Potts (2004) analyzed readability of website privacy policies by calculating two different scores based on the average number of syllables per word and the average sentence length. Very few policies (6%) turned out to be readable by Internet users with high school education or less. And more than half of the privacy policies studied was too complex for over half of the Internet population (measured in terms of education level required). Thus, Jensen and Potts (2004) concluded that a major part of the population can only be expected to understand a small fragment of the privacy policies posted on websites. In the study by Milne and Culnan (2004) perceived comprehension of privacy notices (privacy policies) was measured subjectively. Participants were asked to rate five statements such as "Web privacy notices are usually easy to understand." Especially the qualitative comments collected in the study show people's frustration with privacy notices. Privacy notices are considered too long, wordy and legalistic.

In the next study, described in section 3.5, subjects were required to indicate their preferences regarding the relative importance of individual OECD guidelines by means of a scenario relating to tele-monitoring for healthcare. As a methodological precaution, two pilot studies were conducted (see section 3.2 and 3.3), where the ability of participants to answer correctly whether a particular system complied with a particular guideline or not was tested. Study 1 revealed a very limited comprehension of the system's privacy policy. While this was improved substantially by rephrasing the text scenarios in Study 2, many participants still could not correctly interpret the consequences of the system with regard to their privacy, even though the scenario contained the guideline text almost verbatim.

Based on these previous studies it was expected that the subtleties of the wording of OECD guidelines are not always understandable with common sense; people tend to make assumptions regarding the use of their personal information when they are told the purpose of its collection, or to assume policies regarding purpose by a description of the nature of information collected, etc. Further, it was suspected that minimal scenarios as

[8] This section is based on the following publication: Mahmud, Al A., Kaptein, M., Moran, O., Garde-Perik, E. van de, & Markopoulos, P. (2007). Understanding compliance to privacy guidelines using text- and video-based scenarios. *Interact 2007*, 156-168.

those presented in the two pilot studies, lack a narrative structure and a believable context so they are hard to understand.

Hopefully, a video scenario, which is typically used in informal evaluations during interviews or focus groups to assess how a particular technology might be used, could provide a more compelling and easily comprehensible version of the scenario and would allow users to better express their preferences. This third study was designed to test experimentally whether providing a video-scenario can improve matters. A formal experiment was conducted to test this. The main aim was to compare the variation of interpretation across video- and text-based scenarios.

3.4.2 Method

Design

A counterbalanced within-subject design was chosen to compare the variation of interpretation for two media (video or text). Participants were exposed to both a text-based and a video-based scenario in a counterbalanced manner. In a counterbalanced design, experimental control is achieved by entering all participants into all treatments (Campbell & Stanley, 1966) see diagram below:

	Time 1	*Time 2*
Group A	X_1O	X_2O
Group B	X_2O	X_1O

Where X is considered to be a treatment (video versus text scenario) and O is the observation (correctness of the interpretation of each separate guideline / overall scenario).

Participants were provided with scenarios reflecting compliance or deviance from OECD guidelines. Participants were asked to judge whether the scenario complied or did not comply with several guidelines presented to them in a shorthand manner. For each guideline, there was a correct answer. The dependent variable was the correctness of the response for each guideline and the overall correctness of the interpretation for each scenario.

Some participants were surveyed offline and others over the internet. These two different ways of testing were used in combination because of their specific advantages. Offline surveys make it possible to have short discussions with participants afterwards to get more insight into underlying causes for differences in interpretations. Whereas surveys conducted over the internet enable a larger group of potential participants to be reached. Since both the ability to have post-experimental discussions and reaching a large sample were valued a combination of both approaches was used. The potential effect of online versus offline surveying on guideline comprehension was not a primary interest.

Materials

The original text descriptions of the eight OECD guidelines (OECD, 1980) were adapted in such a way that they cover the essence of each guideline (see Table 3.1), without being too elaborate and especially omitting those parts of the guideline that are meaningful only as legal text rather than as design guidance. In this spirit, also the

Table 3.9. Overview of information provided per guideline for both text- and video-based scenario

1	2: Scenario text	3
-	John is checking his diabetes condition using his newly installed health support system that helps him easily and comfortably measure his glucose, blood pressure and pulse.	-
CL	The system does not give a complete breakdown of all of the data that is collected,	(D)
PS	but informs John that it collects data to monitor his diabetes.	(C)
DQ	He is also assured about the fact that all data collected is necessary for this purpose.	(C)
UL	In the menu of his health support system, John can see that his data can be used for other purposes as well	(D)
OP	and shows him a list of people and organizations that may access his data	(C)
IN	John is not one of these people. He may not inspect,	(D)
MO	modify or erase data collected about him.	(D)
SS	In the same menu, John also finds out that the system does not protect his data with any security safeguards	(D)

Note: Column 1 presents guideline acronym. Column 2 displays the information provided in relation to each guideline, which was presented as continuous text / voice over in the study. Column 3 shows compliance or deviance with guidelines. (C = Compliant, D = Deviant).

guideline of accountability was omitted, as it serves a legal purpose stipulating compliance with all other guidelines.

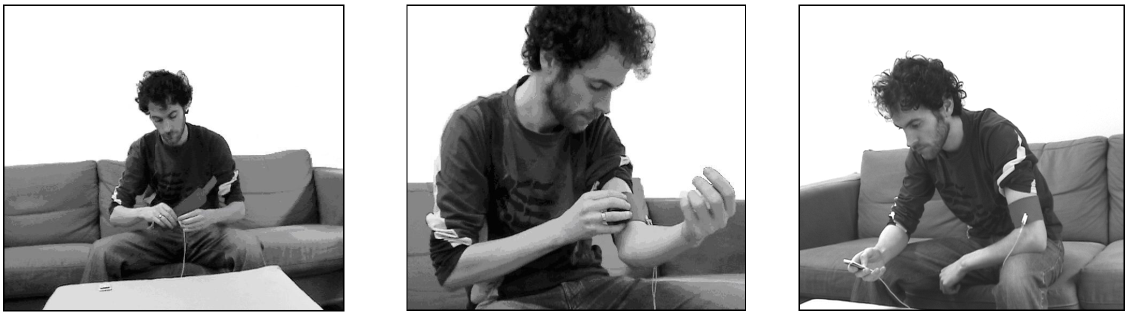
The scenario describing the healthcare system was a slightly improved version of the scenario used in the pilot studies described in sections 3.2 and 3.3. It was adapted to eliminate some of the comprehension problems that were identified in the pilot studies and to provide a more coherent and natural narrative structure. The scenario describes how a diabetic patient called John uses a health-support system for monitoring diabetes. The same text (see Table 3.9) was given in printed form and was read out as a voice-over to a related video. The text describes a system that clearly meets only three of the eight OECD guidelines for privacy and security (namely PS, DQ, OP), whereas the system did not comply with the other five guidelines.

The video shows John, interacting with a machine, presumably the health-support system (see Figure 3.1). The exact nature of this interaction could not be discerned from the video image since John remained unexpressive and the machine was not shown in detail (to avoid drawing attention to interaction details unimportant for this experiment).

Participants

Participants for the offline questionnaire were recruited amongst University employees who were not familiar with the purpose of the experiment or privacy research in general. Participants for the online questionnaire were gathered through invitation on email lists and message boards and through asking department secretaries in other departments of the University to forward an email invitation to their colleagues. Because of the high level of education and knowledge of the English language, it could be expected that their comprehension should be no worse than that of participants recruited for the purposes of related evaluation studies.

Figure 3.1. Screenshots of the video-based scenario



Note: The video shows John preparing himself for and taking a physiological measurement; the video does not make more explicit than the text what John is measuring.

In total 104 participants took part in the study: 25 people participated in the offline questionnaire; 79 participated in the online questionnaire. The procedure used for recruiting ascertained that all participants were familiar with websites/computers and the English language. Participants had various nationalities, and were not restricted to residents of the Netherlands.

Procedure

As in the previous studies, participants were first introduced to John and the function of the health-support system in his daily life through a short text before being shown one of the scenarios in either text or video format (see Table 3.9). Participants were asked to read or watch each scenario before answering if they agreed with eight statements about the system described to them. These statements described compliance with an individual guideline, so in effect participants were asked whether the system met the guidelines or not and which guidelines it met. The system features used in this study are presented in Table 3.10 (identical to those used in Study 2 but presented here again for ease of reference). Participants were allowed to view the video or read the scenario again while answering these questions. When finished with answering the questions for one scenario, participants were then presented with the same scenario via the other medium and the experiment was repeated. The experiment was conducted under two conditions: offline and online.

This experimental set-up allowed for a number of experimental controls. First, conducting simultaneous offline and online questionnaires allowed a double-check for bias. If the results for each of the experimental conditions were the same then it could be concluded that there was no interviewer bias during offline questionnaires or that results would differ systematically due to the absence of social control during online questionnaires. Systematic variation was employed during the presentation of the two scenarios. Offline questionnaires varied presentation of text- or video-based scenarios for every other participant. Online questionnaires varied presentation of media randomly per participant.

Importantly, the questionnaire was conducted as a single-blind test. Participants were introduced to the experiment under the belief that they were going to be shown two scenarios and that they were then to be asked questions about these scenarios. They were not informed that they were going to be shown either a text- or video-based

Table 3.10. Guidelines used in study 3 and implications of their compliance for the system features

Guideline	Acronym	Implication of guideline compliance in terms of system feature
Collection Limitation	CL	The user is informed about the type of data that will be collected.
Purpose Specification	PS	The user is informed about the main purpose for which the data will be used.
Data Quality	DQ	The system only collects data that is relevant to the main purpose of the system.
Use Limitation	UL	The data will be used solely to serve the main purpose of the system.
Openness	OP	The user is informed about which other parties have access to the collected data.
Security Safeguards	SS	The data is securely stored.
Insight	IN	The user can inspect the stored personal data.
Modification	MO	The user has the possibility to make changes in the stored data.

scenario or that both scenarios would be ‘identical’. This set-up prevented participants from guessing the purpose of the experiment and so, intentionally or not, influencing its outcome. The offline and online questionnaires used exactly the same text and formatting and were divided across three identical pages (see Appendix B3).

In setting up the experiment, three criteria were strived for:
- Identical content of the text- and video-based scenarios;
- Controlling for the presentation order of the media;
- Participants are not aware that the medium is being tested.

If all three criteria are met, then it can be concluded that any variance in participants' answers across the media will be due to the effect of that medium.

3.4.3 Results

In both methods of research (online and offline), the tasks, their layout, and the procedure were kept the same. Nevertheless, it is necessary to examine possible differences between these two methods. It was anticipated that there would be no significant influence upon the test results caused by the method of data gathering.
To check this assumption, a t-test was performed on the difference between the two data gathering methods for both the text-based scenarios and the video-based scenarios separately. Within the text based scenario there was no significant difference between the Internet (M=71.1, SD=12.1) and the offline condition (M=80.0, SD=19.4), t(102)=-0.215, p=0.831). The same was true for the video-based scenario (online: M=74.4, SD=15.6; offline: M=74.5, SD=14.6), t(102)=-0.39, p=0.969.

Finally, before aggregation of the data from these two different methods of data collection, one extra check of the reliability of the assumption was performed. To check for differences on individual items between the internet and offline questionnaires, a Chi-square test for every individual guideline was conducted.

Table 3.11. Comparison of offline and Internet results per question

Item	Chi^2	Df	Sig.
Collection Limitation (CL)	0.42	1	0.516
Purpose Specification (PS)	1.08	1	0.299
Data Quality (DQ)	0.45	1	0.501
Use Limitation (UL)	2.32	1	0.128
Openness (OP)	2.31	1	0.128
Security Safeguards (SS)	0.40	1	0.525
Insight (IN)	1.88	1	0.171
Modification (MO)	0.15	1	0.702

Table 3.11 presents the results of these individual Chi-square tests per item by presenting the Chi-squared value, the degrees of freedom and the significance level. There is not sufficient evidence in favor of a relationship between the data collection method and the number of correct responses. Based on these results, the data for the two methods of data collection were combined for further analysis.

Results were obtained by calculating the percentage of correct answers given for each question relating to one of the guidelines in each of the following conditions:

1. The text-based scenario shown first to participants;
2. The video-based scenario shown second (i.e. immediately after the text-based scenario had been shown);
3. The video-based scenario shown first;
4. The text-based scenario shown second (i.e. immediately after the video-based scenario had been shown).

The overall result for the whole scenario in each condition was also calculated.

Initial interpretations showed interesting results. On average, overall scores for each condition were approximately the same, with text performing slightly better. However, large variations in scores were obvious between the guidelines for each condition. Table 3.12 shows the percentage of good answer per guideline for each condition. Rows in this table show the condition and columns show the percentage of correct results for each guideline. The final column shows the overall percentage of correct answers per condition.

Of the participants who read the text-based scenario first, 83.0% correctly interpreted the collection limitation guideline based on text, while this was only 68.0% in the case of video (which was shown second). The other group was exposed to the video-based scenario first, and to the text-based scenario afterwards. Of these 47.1% of the

Table 3.12. The percentage of correct answers per question by condition

Condition	CL	PS	DQ	UL	OP	SS	IN	MO	Overall
Text first	83.0	66.0	34.0	84.9	73.6	94.3	86.8	98.1	77.6
Video second (after text)	68.0	66.0	43.4	75.5	71.7	94.3	83.0	100.0	75.2
Video first	47.1	78.4	58.8	72.5	70.6	82.4	82.4	96.1	73.5
Text second (after video)	66.7	72.6	51.0	86.3	86.3	92.2	98.0	96.1	81.1

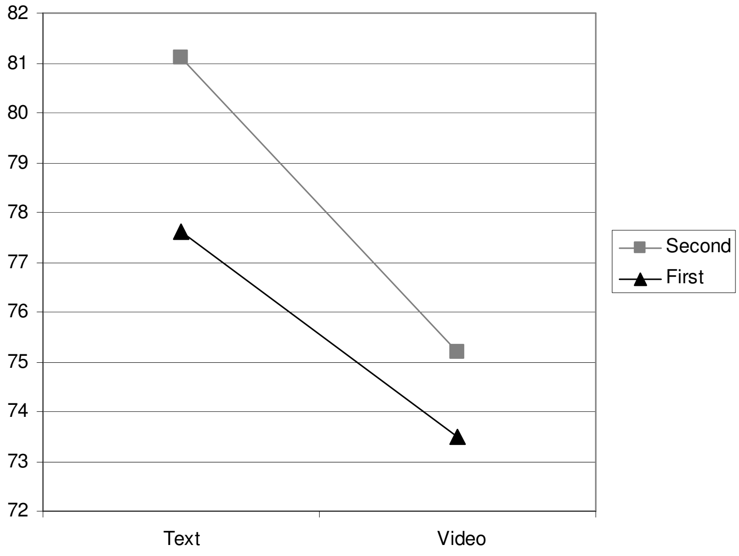
participants correctly interpreted the guideline in the case of video while 66.7% interpreted it correctly for the text-based version.

The aggregated percentage of good answers on the text-based questions and the video-based questions was 79.4% and 74.4%. Analysis of variance, using both the order and the medium as independent variables, showed a significant main effect for medium (p=0.001).

Again, analysis of variance was performed using both the order and the medium as independent variables. No significant main effect was found for order (p=0.715), showing that results were not affected by learning effects (either because of the purpose of the experiment or the content of the scenarios). This result is consistent with the pilot studies reported previously in this chapter. Furthermore, it confirms that medium was the main effect. However, an indicative effect was found for interaction between medium and order (p=0.077). Taken individually, both text and video performed a little better when shown second – a different measure to check for an order effect which tested the average score of both media when-shown-first against the average score of both media when-shown-second. This 'interaction effect' means, for example, that text performed better when shown second not for the fact of being shown second – it is already known that there was no effect for order – but because it was preceded by the video-based scenario. Scores for video improved also when preceded by text but by a lesser degree. Thus, the best results were obtained when the text scenario was preceded by the video scenario (see last column of Table 3.12).

The above points are illustrated in Figure 3.2. It shows the overall percentage of correct answers for medium and presentation order. It shows clearly that there is a higher overall score for text scenarios in comparison to video, which is the main effect

Figure 3.2. Overall percentage of correct interpretations for the four conditions



Note: The four conditions are text first, text second (after video), video first and video second (after text).

mentioned above. In addition, it shows that the overall percentage of correct answers does not differ that much for the order of presentation of each medium (either first or second), explaining why the order effect was not significant.

Figure 3.2 shows the overall percentage of correct answers for the four different conditions: text first, text second (after video), video first, and video second (after text). The interaction effect, which was significant at a ten-percent level, means that the difference between the percentage of correct interpretations for video and text scenarios changed according to whether the scenario was presented first or second. Figure 3.2 shows that the difference in the overall percentage of correct answers between the text and video scenarios was greater for the second presentation of the scenario than for the first presentation. There was a greater difference in correct interpretation between the first and second presentation for the text scenario than there was for the video scenario. The overall percentage of correct interpretations was almost the same for the first and second presentation of the video scenario, but for the text scenario the second presentation (after having seen the video) performed considerably better.

3.4.4 Discussion

As has been explained before, the experiment aimed to investigate the variance in interpretation between video- and text-based scenarios. First of all, both types of scenarios showed limited understanding of the compliance with privacy guidelines. On average the text-based scenario resulted in 79.4% correct interpretation, while for the video-based scenario this was 74.4%. This means that about one fifth to one quarter of the privacy guidelines in this experiment were interpreted incorrectly. Jensen and Potts (2004) explain that text with long words and/or long sentences are more difficult to read. The text used in the scenarios consisted of fairly short sentences and yet proved difficult to read. This confirms the results of the two pilot studies. It shows that caution is required when surveying users regarding scenarios, whether this is for research purposes or as part of an iterative interaction design process.

The results obtained call into question the reliability of scenarios – both text- and video-based – for surveying users' attitudes regarding privacy-related issues. As mentioned, it is common practice to use scenarios of this kind as a means to explain a system to users and facilitate discussion regarding privacy. Clearly, results from such studies when relying on statements referring to legal guidelines such as those by the OECD, are contingent upon sufficient user comprehension, so future studies should include appropriate checks of the users' comprehension of the (sometimes) futuristic scenarios presented to them.

Another striking result is the interaction between media. Video, when shown first, "lifted" the results of the text-based scenario shown afterwards more than the text scenario did for video. This has led to the hypothesis that video-based scenarios are more suited to act as contextualizing overviews to the more detail-affording qualities of text. Such a hypothesis does not take account for the differences in answers given for the individual guidelines between video and text.

In interaction design practice, the implication of this finding is that where a video scenario is made to solicit reactions of users to a particular design concept it can be wise to offer a corresponding text, which they will consult after viewing the video in order to answer detailed questions that require in depth understanding of the concept described.

To help explain the results further, seven of the offline participants were contacted again to discuss the study's findings with them. These return interviews were undertaken first to double-check for flaws in the experiment design and second to elicit explanations, which might have been overlooked. All seven interviewees could remember the experimental set-up with accuracy and the general function of the device in the scenario. Participants were then presented with the two scenarios once again in the order in which they had been shown in the original experiment. They were then informed that both were the same and provided with the answers, which they had given in the original experiment. These interviews took the form of a discussion of these answers with participants.

A number of participants argued that the video imagery did not provide extra detail regarding interaction with the device. While this point is true, it was necessary in order to maintain equivalence between both media and thus necessary for the experiment as a whole.

On the matter of the experiment results, half of the re-interviewed participants had performed better on the video prototype. However, regardless of their actual results, participants insisted on the differences between text and video, contradicting the results data, mainly suggesting that text is vastly easier or that there was a learning effect.

One participant did refer to the interaction effect, suggesting that the benefit of video is that it helps frame a subject while text solidifies it. This opinion was reflected in the responses of other participants. They argued that overall they would prefer a mixed-medium, criticizing both video and text on their own. While the benefits of video were that it acted as a guide to a topic and can be digested passively, *"once it's gone, it's gone".* Another participant linked it to TV news, where text and video appear on screen at once, and others talked of the benefits of being able to "cross-reference" between video and text. These points, raised by participants, support the suggestion for the use of both video and text scenarios in succession.

Further to the methodological implications noted, the flawed understanding of privacy-related consequences of system use is noteworthy. Similar (and usually even more complex) texts to the scenarios are presented as privacy policies in commercial websites; this may lead to wrong assumptions about systems. When users realize the inaccurateness of their assumptions, they experience an invasion of their privacy (Adams & Sasse, 2001).

It has to be noted that the concepts that were presented to the participants in this study were based on legal documents and perspectives unfamiliar to most people. However, it is precisely such concepts that are translated into privacy policies used on websites. These policies are known to present comprehension problems to users (Jensen & Potts, 2004; Milne & Culnan, 2004) and often are used to inform the interaction design for such systems (Langheinrich, 2001; Iachello & Abowd, 2005).

3.4.5 Conclusions

The experiment examined differences in understanding of privacy guidelines between text and video scenarios. This study has shown that a variation exists, both overall and more importantly in users' understanding of individual issues. It has also been shown that the order in which text and video are shown has a significant effect on the level of understanding.

Text scenarios resulted in slightly better understanding. Moreover, if a video-based scenario is shown first then the interpretation of a text-based scenario improves. As a result of this study many questions are raised. Why does video appear to support text more than the other way around? What is the underlying process of this phenomenon? And why is there such a great variance in the answers for individual questions between media? This study cannot yet explain the reasons underlying these results.

For the time being, it is recommended that text-based scenarios preceded by a video-based version should be used for the purposes of privacy- and security-related user surveys to enhance people's understanding of the scenario. Future research into methodologies for investigating privacy should compare how video and text scenarios relate to actual or staged (e.g., Wizard of Oz) experiences of pervasive systems.

Future work should examine whether similar results are obtained outside the specific context of privacy. Extending this inquiry can provide methodological guidance as to when different media are appropriate for presenting scenarios.

3.5 STUDY 4[9]

3.5.1 Introduction to Study 4

As indicated before in the general introduction one commonly used approach for addressing privacy concerns is to rely on Fair Information Practices. The two pilot studies described before aimed at studying people's ability to comprehend textual descriptions of privacy guidelines. In this study the relevant importance of these guidelines for end-users is investigated.

In this study participants were asked to explicitly rate the importance of guidelines based on system descriptions. This is important in order to establish whether the OECD guidelines capture user concerns, and whether people differ in terms of their priorities in more nuanced ways then just being concerned or not. Furthermore, it provides designers of privacy sensitive systems with concrete advice on where to start in dealing with privacy concerns, namely with the most important guidelines. The investigation is conducted in the context of a health support system that allows the daily monitoring of health parameters of individuals from the comfort of their homes.

Prior to the study, the following expectations existed concerning to the importance of individual guidelines:

- Collection limitation and purpose specification will be more important than data quality. Since knowledge of what data is collected (collection limitation) and for what purpose (purpose specification) can help infer the relevance of the data collected (data quality). Whereas knowing that the collected data is relevant for a particular purpose, does not inform the user about the type of data or the purpose involved.

[9] This section is based on the following publication: Garde-Perik, E. van de, Markopoulos, P., & Ruyter, B. de (2006a). On the relative importance of privacy guidelines for ambient health care. *NordiCHI 2006*, 377-380.

- Security safeguards is important, since without secure storage there can be no real guarantees about data use, access by other parties, and reliability of stored data (since anyone could make modifications).
- The ability to modify data (Data modification) is more important than having insight in the data (insight), since being able to make modifications would imply having some insight in the data already.

3.5.2 Method

Design

Participants were shown a text scenario describing the health care system. The description provided general context information about the system and then detailed its privacy related features; the system described does not adhere to any of the OECD-based guidelines (see second column of Table 3.13, this was presented as continuous text).

Participants were then presented with potential 'fixes' to the system each of which would make it comply with one specific OECD-based guideline (see last column of Table 3.13). These fixes were presented in pairs (an example is shown in Figure 3.3), and participants were asked to choose which of the pair they thought was most important to them.

Table 3.13. Overview of base deviant scenario and potential fixes to the health monitoring system

	Base deviant scenario (D)	Potential fixes (C)
CL	The system *does not inform* John that it will collect data regarding his health, blood pressure, pulse and glucose level.	The system *informs* John that it will collect data regarding his health, blood pressure, pulse and glucose level.
PS	The system *does not inform* John that data is collected in order to monitor his diabetes condition.	The system *informs* John that data is collected in order to monitor his diabetes condition.
DQ	The system informs John that it *also collects data that is useful for things other than tracking his diabetes condition*.	The system informs John about the fact that it will *only collect data that is useful for tracking his diabetes condition*.
UL	The system informs John that it *uses his data for other reasons than the main purpose of the system as well*.	The system informs John about the fact that it will *not use his data for any other reason than the main purpose of the system*.
OP	The system *does not inform* John regarding all the organizations or individuals who can access his data.	The system *informs* John regarding all the organizations or individuals who can access his data.
SS	The system informs John that his *data is not protected by any security safeguards*.	The system informs John about the fact that *all his data is securely stored*.
IN	The system *does not provide* facilities for John to inspect all data collected about him.	The system *provides* facilities for John to inspect all data collected about him.
MO	The system *does not provide* facilities to allow John to modify or erase any data about him.	The system *provides* facilities to allow John to modify or erase any data about him.

Note: The first column displays acronyms for the guidelines. The second column shows each sentence of the base deviant scenario, which was presented as continuous text in the study. The last column shows the potential fixes that were presented in pairs. The difference in formulation between the deviant and compliant form is italicized. The compliance or deviance with guidelines is indicated in brackets (C = Compliant, D = Deviant).

Figure 3.3. Example of the presentation of a pair of potential fixes to the health monitoring system

Please indicate which of the two adaptations you would prefer by checking the appropriate box below.

	Preferred adaptation
The system informs John that it will collect data regarding his health, blood pressure, pulse and glucose level.	0
OR	
The system informs John regarding all the organizations or individuals who can access his data.	0

Participants

Participants were recruited by placing adverts on local mailing lists in the respective organizations of the authors (a University and an Industrial Research lab). Recruitment was aimed at obtaining two groups of individuals depending on their need for medical attention. The first group consisted of people with a chronic health condition and people aged over 65. The second group consisted of individuals younger than 65 years of age and without a specific need for medical attention. A total of 50 persons participated.

Materials

The original OECD guidelines are written in quite terse and lengthy language intended for legal purposes. For this reason simplified expressions relevant to the scenario of this study were created. To ensure that the text and the guidelines were understood properly the two pilot studies described in the previous section were conducted. Since these pilot studies revealed some difficulties with the comprehension of privacy related statements; the texts were rephrased (see Table 3.13).

Participants were asked to make their judgment regarding the privacy guidelines through a web-based questionnaire. The first page contained information about the study and the kind of participants needed. The next pages consecutively described a context of a diabetic person that may benefit from a health monitoring system, the purpose of the questionnaire, the base scenario (see second column of Table 3.13) and the explanation of the pairs of adaptations that would be offered to them (see last column of Table 3.13 and the example of the presentation in Figure 3.3).

Measures

The relative importance of complying with the eight privacy guidelines was measured by pairwise comparison. Participants were offered all combinations of complying with the guidelines in pairs of two (a total of 28 pairs; all 8 guidelines combined with all 7 others, without doubles). Participants were asked to choose their most preferred adaptation for each pair. From each participant a total of 7 judgments per guideline was obtained, indicating the importance of complying with that guideline compared to the other guidelines. This total score per guideline was divided by 7 to obtain a score for importance between 0 (never regarded more important than other guidelines) and 1 (always regarded more important than all other guidelines). Besides the preferences for each of the guideline, participants were also asked about chronic conditions, age and country of residence.

Procedure

After accepting to take part in the study, participants entered the website, read the context description and were informed about the purpose of the study. Then they were offered the base deviant scenario (see second column of Table 3.13). Subsequently, participants were offered a pair of possible adaptations. They were asked to indicate which of the two adaptations they would prefer. This process was continued until the participant judged all 28 possible pairs of guidelines. Finally, the additional questions about chronic conditions, age and country of residence were asked.

All pairs of possible adaptations were offered to participants in random order. Besides, the position of each adaptation was alternated so that each adaptation would be offered a similar amount of times as the first or the second option within a pair (see Appendix B4). For the first eight participants a different procedure for a paper-based study was followed. The position of each adaptation within a pair was still alternated, but the 28 pairs of possible adaptations were not presented in random order to prevent administrative problems.

3.5.3 Results

In total 50 participants completed the questionnaire – this number includes 8 participants from the paper-based study for whom health related information had not been obtained. Most participants (69%) were between 26 and 45 years old and reside in the Netherlands. Table 3.14 shows the occurrence of different chronic conditions among the remaining 42 participants in the sample. It turns out that 6 of the participants suffer from heart failure, 5 suffer from diabetes and also 5 from asthma. A disease of the lungs, named Chronic Obstructive Pulmonary Disease (COPD) and Depression was mentioned by only 1 participant as a current condition. On the other hand 6 out of 30 participants indicated to suffer from another condition than the ones specified (this question was added later, and hence only answered by a small group of participants).

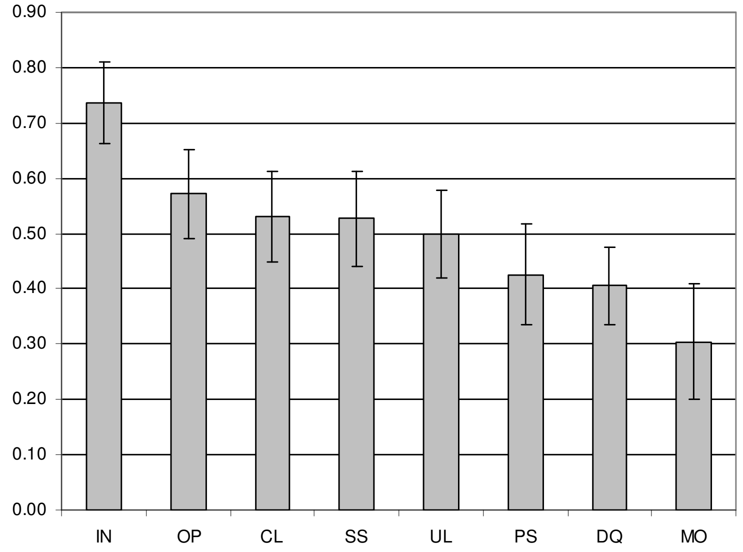
Figure 3.4 shows the importance of all eight guidelines compared to the other guidelines for the whole sample on average. Insight is the preferred adaptation in almost three quarters of the situations (0.73), and openness is found more important than other guidelines in more than half of the situations (0.57). Least preferred were the guidelines of data quality and modification. Data quality was preferred to other guidelines only in 41% of the situations, and modification in 31%. There is however, quite some difference

Table 3.14. Data on health condition of participants of study 4

Chronic condition	Participants
Heart Failure	14%
Diabetes	12%
COPD	2%
Asthma	12%
Depression	2%
Other Chronic Condition*	20%

Note: COPD: Chronic Obstructive Pulmonary Disease. N=42, for all conditions except Other Chronic Condition (n=30).

Figure 3.4. Relative importance of OECD guidelines for health monitoring scenario



Note: Relative importance (0-1), including 95% confidence interval.

in preference by participants for the guidelines modification, purpose specification, security safeguards and collection limitation. Repeated measures ANOVA with Bonferroni correction showed that the difference between insight and other guidelines is statistically significant except when comparing to openness and security safeguards (respectively p=.150 and p=.074). None of the differences between the 'middle' six guidelines from openness to data quality were statistically significant. Furthermore, the difference in relative importance between modification and insight and openness was also statistically significant (respectively p<.001 and p=.002).

In order to check whether there is a difference in guideline importance between users depending on their need for medical monitoring (people with a chronic condition, people over 65 and those with no specific need for medical monitoring), a one-way ANOVA analysis was performed. The analysis revealed that there is no significant difference in mean guideline importance between the groups based on their need for medical monitoring except for security safeguards (p=.028) and purpose specification (p=.036). Since there were no significant differences for the other six guidelines, it was decided that it was acceptable to add the data of all participants together and treat them as one single group. Apparently, there is no clear difference in guideline importance depending on people's need for medical monitoring.

3.5.4 Discussion and conclusions

It was anticipated that collection limitation and purpose specification would be more important than data quality. As knowledge of what data is collected and for what purpose may help infer the relevance of the data collected. However, the results show that there is not much difference in importance between purpose specification and data quality and that collection limitation is valued somewhat more. Also, it was expected that security safeguards would be regarded as important, however in this study security safeguards turned out to be somewhat neutral compared to the other guidelines.

Furthermore, it was anticipated that the possibility to modify data would be valued more than having insight in the data, since the ability to make modifications to one's data would imply having access to and thus having insight in the data already. However, in this study insight was valued much more (0.73) than being able to make modifications to data (0.31). This means that insight was preferred over other guidelines in almost three quarters of the situations, whereas the ability to modify was only preferred over other guidelines in less than one third of the situations. From comments participants made it is known that people feel that modifying health related data is not regarded useful.

As a follow up to this experiment two focus groups were conducted, one with young diabetics (under 30 years of age) and one with aging heart failure patients (over 50 years of age). The qualitative data obtained reveals radically different perceptions regarding privacy between these two groups, especially with regards to the dimension of control. However, for both groups the disinterest in data modification found in this study was confirmed.

The heart failure participants indicated to feel more secure with technology that will constantly monitor their condition and did not have any concerns about privacy. These participants did not have any reservations about full insight into their data by the doctor. They felt that abuse of their personal data was not possible, since the more data that would be available to the medical staff the more beneficial it would be for them.

The young diabetic participants expressed more concern about automatic disclosure of medical data. They did not want the doctor to have insight into their data at all times. They regard their glucose levels as highly personal data and do not want to share this with anybody. The diabetic participants want to be in control over their data, and to decide for themselves when and how their doctor or nurse could obtain access to their medical data. A health monitoring system for these diabetics should not allow anyone to collect or access medical data without the patients' permission.

3.6 CONCLUDING REMARKS

This chapter presented several studies relating to the interpretation and importance of privacy guidelines from the perspective of the user. First of all the interpretation of privacy guidelines was investigated in two pilot studies. These pilot studies aimed to establish whether an approach based on scenarios can be used to study user attitudes relating to privacy or acceptance of personalized systems depending on compliance with guidelines describing Fair Information Practices. It turned out that participants' understanding of the guidelines was limited. Participants confused separate system features, or simply had a broader interpretation of some system features. Also, study 3 on the variance in interpretation between video- and text-based scenarios showed limited understanding of the compliance with privacy guidelines. About one fifth to one quarter of the privacy guidelines were interpreted incorrectly in total.

The findings of the studies described in this chapter have consequences in different areas such as system design, publishing of privacy policies and empirical research regarding privacy. Privacy related statements expressed in text, involving the concepts of information collection versus use, require an extremely accurate reading and interpretation of text that cannot be assumed. Even the interpretation of relatively simple statements was not unambiguous.

Participants tend to interpret privacy statements loosely. Their common sense perhaps makes them infer facts that are not explicitly stated or even make inferences exactly opposite to what is said. Such a loose interpretation of privacy related statements may cause serious problems and provide a poor understanding of the privacy consequences involved when using a particular system. This may result in serious privacy conflicts (Adams & Sasse, 2001).

For the purposes of privacy research, where such statements are presented to users as a pre-experiment or post-experiment questionnaire, it seems that it is necessary to be very thorough about testing the ability of subjects to comprehend accurately the questions presented to them or to grasp the fine differences in text scenarios that describe privacy issues. It would be interesting to further explore whether a coherent narrative structure for scenarios, as is typically expected in HCI research, would still be hampered by these problems.

Study 3 that examined differences in the understanding of privacy guidelines between text and video scenarios has shown that a variation indeed exists. Text scenarios resulted in slightly better understanding. Furthermore, it showed that the order in which text and video are shown has a significant effect on the level of understanding. If a video-based scenario is shown first then the interpretation of the subsequent text-based scenario improves. Perhaps video-based scenarios are more suited to act as contextualizing overviews to the more detail-affording qualities of text. In interaction design practice where a video scenario is made to solicit reactions of users to a particular design concept it can be wise to offer a corresponding text which can be consulted afterwards. However, it should be investigated whether the results of the privacy guidelines scenarios will be replicated for an interaction design context.

In study 4 (on the relative importance of the privacy guidelines) it turned out that insight was preferred over other guidelines in almost three quarters of the situations, whereas the ability to modify was only preferred over other guidelines in less than one third of the situations. Participants felt that modifying health related data is not regarded useful. The difference in relative importance between modification and other guidelines was only statistically significant for two guidelines. The difference in relative importance between insight and other guidelines was statistically significant except for openness and security safeguards.

The studies in this chapter have shown serious pitfalls in using scenarios as a basis of judgment tasks regarding privacy. This effect was present even when a video medium was used to describe the scenario and when scenarios were almost identical to the questions put to people. It may be that the concepts presented in privacy guidelines are inherently difficult, or that the questions posed may be the source of confusion. It may be that making such judgments is just as difficult for situations they experience themselves as it is for a scenario. The source of the confusion could be investigated in future research. For the time being the recommendation is not to avoid scenarios all together as a basis for research, but to pilot them to ensure difficulties in comprehension are removed as far as possible and to report comprehension measures.

4 Evaluation of Privacy Interfaces

This chapter presents a comparative study of three different interfaces for the specification of privacy preferences by end-users: privacy interfaces. This study addresses the following research questions:

- *What are people's information privacy concerns?*
- *What influences people's information disclosure behavior?*
- *How to design privacy interfaces?*

Three privacy interfaces (Profiles UI, Use UI and Split UI) were used by 78 participants in the context of a laboratory study. The interfaces were evaluated in terms of overall difference, and compared with regard to five different attributes namely: trust, risk, usefulness, ease of use, and intention to use. Participants' ratings of the three interfaces on the five attributes, as well as their qualitative comments with regard to the models were analyzed. Overall, results were in favor of the Profiles UI. This interface was considered to be clear, most precise and specific, and offered good overview.

However, participants were not uniform in their attitudes and preferences regarding the three different interfaces. Four clusters of participants were distinguished by means of hierarchical cluster analysis. The first 'Practical' cluster preferred the Profiles UI most and the Use UI least and valued an interface that is (initially) easy to use and provides many options. The second 'Pessimistic' cluster almost equally preferred the Profiles and Use UI. This cluster valued an interface with a lot of options and one that can be set quickly. The third 'Concern & Control' cluster was most concerned about their privacy; it had a strong preference for the Profiles UI and a strong dislike for the Split UI. Many aspects were important in an interface, such as control and safety. The last cluster was a rest group which was the least outspoken in their preference for any of the interfaces and least concerned about their privacy.

An important aim of this study was to investigate acceptance of privacy interfaces; for this reason an acceptance model was developed. Analysis using a Partial Least Squares (PLS) approach found that trust, usefulness and ease of use are important determinants of acceptance. This confirmed the initial expectation that even in the context of privacy concerns, other features can be more important than the reduction of risk. For the separate clusters only usefulness and ease of use played a significant role in intention to use. Trust has been argued to predict intention to use, yet this study suggests that this is not always the case.

4.1 INTRODUCTION

It has been argued that concerns about privacy can be addressed by giving users more control over their personal information stored and used by personalized applications, services and environments (Bellotti & Sellen, 1993; Olivero & Lunt, 2004; Günther & Spiekermann, 2005). Bellotti and Sellen (1993) present a framework for design for privacy in ubiquitous computing environments which argued the importance of control. However, the framework itself is not based on empirical evidence.
Günther and Spiekermann (2005) describe an experiment in which two different privacy-enhancing technologies (PETs) are offered to consumers in a future intelligent shopping environment enabled with RFID technology. However, neither of the PETs is successful in providing enough perceived control in order to provide a greater degree of privacy.
Olivero and Lunt (2004) conducted long qualitative interviews with 23 participants and analyzed them by means of grounded theory (Strauss & Corbin, 1990). The aim was to study attitudes and perceptions of regular internet users about data collection, self-disclosure and privacy on the internet. Their participants claimed the need to exercise control over the ownership of personal data in order to avoid unwanted privacy intrusions. These studies do stress the importance of control in the light of privacy concerns, yet they lack empirical evidence and/or do not involve the use and evaluation of systems by participants. The study described in this chapter will examine what mechanisms are preferred by users for controlling disclosure of their personal information. It will provide empirical evidence and involve the actual use and evaluation of privacy interfaces.

Several studies have demonstrated the relevance of three factors on people's willingness to disclose information while using the Internet. The privacy model by Adams and Sasse (2001) consists of three major privacy factors: information sensitivity, information receiver, and information usage. The model was developed in the context of multimedia communication and emerged by analysis of both qualitative and quantitative data based on grounded theory. A study by Whiddett et al. (2006) about patient's attitudes towards the disclosure of their personal health information found that willingness to share information was influenced by the identity of the recipient, the level of anonymity of the information, and the type of information involved. The Music Recommender study reported in chapter 2, also found that willingness to disclose information depends on factors like recipient, purpose of use, and sensitivity of the information involved (determined by the type of information and possibly level of anonymity).

This study aims to investigate the effect of privacy and trust on intention to use in the context of Ambient Intelligence scenarios. There are many related studies that put forward predictive models relating perceptions of privacy and trust, but few of them refer to actual use (Corritore et al., 2005; Featherman & Pavlou, 2003); mostly user attitudes are surveyed without reference to specific use situations (Dinev & Hart, 2006; Malhotra et al., 2004; Suh & Han, 2002).

In addition, most related studies present the evaluation of only one system. Such studies can provide some qualitative feedback regarding the suitability of a particular system concept or general points of concerns for the user, but it is hard to produce more general guidance regarding the design of privacy interfaces. Lederer et al. (2004) evaluate only one prototype and provide design guidance on the basis of that. However, they can not be entirely confident that their advice generalizes to all privacy interfaces; it may only apply to their particular prototype evaluated. Stronger conclusions can be made in a comparative study of multiple systems at once. Participants will always be able to find some good or positive points about any system. However, without drawing comparisons between systems it is hard to put their judgments in perspective and reach concrete conclusions about the adequacy of any particular user interface. If multiple systems are evaluated simultaneously (as is done for example in Cranor et al., 2006) this provides an indication of the direction participants prefer. This is of course dependent on the total set of systems evaluated.

The studies of chapters 2 and 3 showed that empirical research on privacy attitudes and behaviors is a difficult endeavor, as the research may influence the behaviors studied and the opinions users will report. Therefore, instead of taking such a complex phenomenon as privacy as the main focus of investigation, in this study the aim is to check whether or not the perception of privacy risk is more or less important in comparison to other known important factors such as usefulness and ease of use.

This chapter presents an experimental study which compared three conceptual models for privacy interfaces that could potentially provide users with more control over their personal information. More specifically, it concerns an evaluation of conceptual models for interfaces that allow users to specify their privacy preferences with regard to the disclosure of information. The conceptual models in the study are based on the following three dimensions: the type of information involved, the recipient (only for two interfaces), and the purpose of use. The study is a formal evaluation of the conceptual models as instantiated by the interfaces.

This study will give insight into the three research questions underlying this thesis:

- What are people’s information privacy concerns?
- What influences people’s information disclosure behavior?
- How to design privacy interfaces?

The specific aim of the study is to investigate:

- The effect of different conceptual models for privacy interfaces on user’s preferences in order to guide design of such interfaces.
- The influence of perceived privacy and trust on intention to use (i.e. which user interface aspects have the greatest impact on intention to use?).
- Whether there are any individual differences between participants.

These aims will be further explained in the following three sections.

4.1.1 Privacy Interfaces

Different interfaces have been proposed as a tool for users to specify privacy preferences (see also the introduction to this thesis). Many of these interfaces were developed to support office workers (e.g. Neustaedter & Greenberg, 2003; Rode et al., 2006) or internet users (e.g. Cranor et al., 2006; Ackerman & Cranor, 1999, Lau et al., 1999) or users in mobile contexts (Lederer, Hong, et al., 2003).

Since Ambient Intelligence environments are not readily available, it is not surprising that there are no interfaces developed for this specific context. Langheinrich’s (2002) privacy awareness system is perhaps a first attempt in this direction. However, Langheinrich’s work focuses on the technical support of such a privacy system instead of investigating appropriate privacy interfaces from a user point of view.

In this chapter three different conceptual models for privacy interfaces are distinguished. These conceptual models are called Self-Representation, Information-Use and Split-Dimension. They differ in the way they support the management of one's privacy preferences regarding disclosure of personal information. The following types of privacy settings can be specified with each conceptual model:

- Self-Representation: approved representations of the self that are suitable for a particular context (based on Goffman, 1959), i.e. approved disclosure instances based on combinations of recipient, purpose of use as well as type of information;
- Information-Use: disapproved disclosure instances based on both purpose of use and type of information.
- Split-Dimension: approved levels of information disclosure split across the three separate dimensions, namely recipient, purpose of use, and type of information.

For each conceptual model the next sections will describe existing privacy interfaces, the interface developed for the purpose of this chapter's study, as well as a comparison between both.

Privacy Interfaces based on Self-Representation

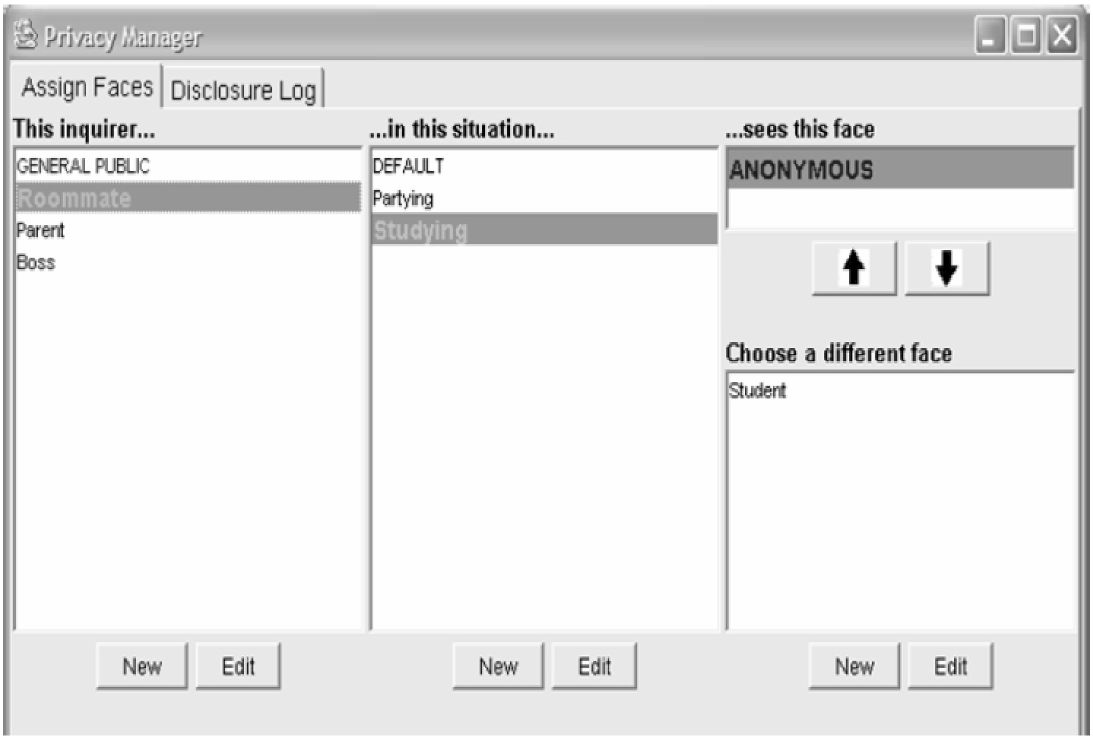
The concept of Self-Representation supports users in the presentation of their 'self' through selective disclosure of information depending on the context they are in. This is based on the work by Goffman (1959) who describes how people choose to present parts of themselves based on what is appropriate in a certain situation and depending on the reactions of people surrounding them. According to Goffman people consciously choose to show specific parts of themselves to control the impressions that others form about them. Goffman's work has influenced other privacy related work. Ackerman (2000) and Boyd (2002) both argue that the process of impression management as described by Goffman could be used for the regulation of privacy in mediated environments.

Ackerman (2000) describes that a gap exists between the social requirements of Computer Supported Cooperative Work (CSCW) and its technical mechanisms. Ackerman states (in accordance with Goffman) that people wish to control the disclosure of private information on an ongoing basis. People do this everyday, and do not have to deliberate about this in detail. However, according to Ackerman there are no HCI mechanisms that support this naturally occurring and everyday activity of handling personal information entirely in a straightforward manner. Ackerman proposes to address the social-technical gap by solutions that are based on what is known to be appropriate in social circumstances, such as the balancing of personal information disclosure.

Similarly, Boyd (2002) states that people are much more proficient in presenting particular facets of their internal identity depending on the environment in offline social interaction than it is for online social interaction. Boyd discusses what adjustments need to be made in order for people to be able to properly negotiate social interactions in a digital world.

An example of an existing privacy interface based on Self-Representation is the faces metaphor by Lederer et al. (2004). Their desktop interface is shown in Figure 4.1. It shows the main screen where users can define combinations of inquirers, situations and

Figure 4.1. Desktop interface for the faces metaphor by Lederer, Hong, et al. (2003)



Note: This figure shows the main screen for creating inquirers, situations and faces, and combining them. A face represents a set of privacy preferences that is used when a given inquirer makes a request when the user is in a given situation.

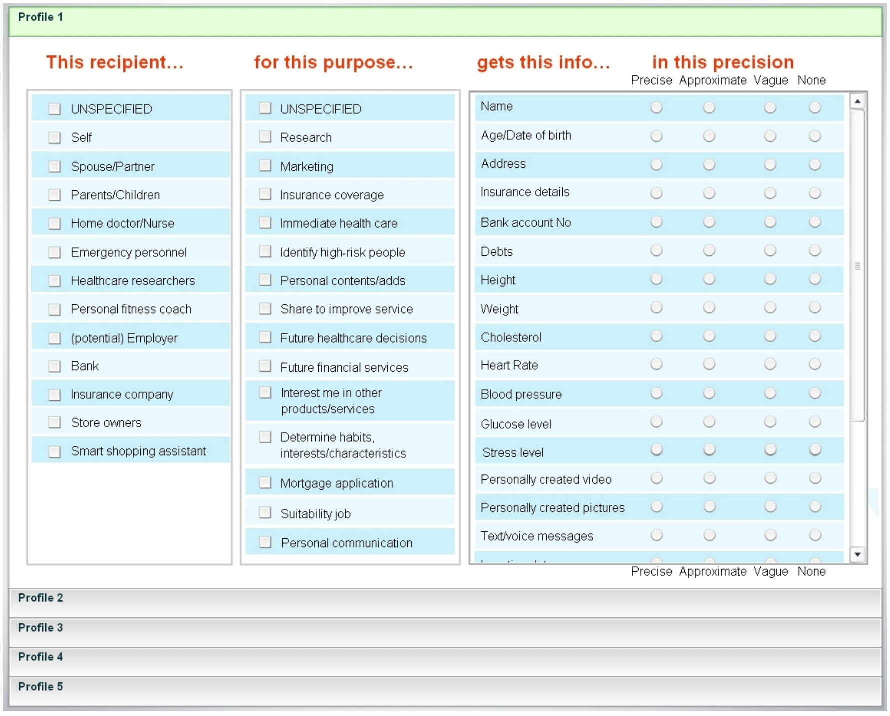
faces. The situation represents the context of information inquiries and disclosures and is a combination of location, activity, companions, and time. The user's privacy preferences are represented by faces. A face is an indication of the desired levels of precision (precise, approximate, vague or undisclosed) at which various types of information, such as name, location, activity, and companions should be disclosed. Users can assign a specific face to a combination of inquirer and situation.

The authors performed an evaluation of their rendition of this conceptual model (Lederer et al., 2004). They first asked participants to set the interface for a combination of parties and situations they find themselves frequently involved with or in. Afterwards participants were inquired about the precision levels at which they would prefer to disclose their information to specific inquirers in some hypothetical scenarios. It turned out that participants' a priori configured preferences often differed substantially from their stated preferences during the scenarios. Also, participants had difficulty remembering the precision preferences they had specified inside their faces. Participants regarded the situation and the desired face in a particular situation as inseparable.

The interface based on Self-Representation which was developed for the purpose of the present study is called the Profiles UI. The Profiles UI (shown in Figure 4.2) allows users to specify multiple representations of the self, called profiles, which are different combinations of recipient, purpose of use and type of information. This means that this privacy interface includes the three dimensions that are known to influence people's

Figure 4.2. Screenshots Profiles UI

A



Profile 1

This recipient...

- □ UNSPECIFIED
- □ Self
- □ Spouse/Partner
- □ Parents/Children
- □ Home doctor/Nurse
- □ Emergency personnel
- □ Healthcare researchers
- □ Personal fitness coach
- □ (potential) Employer
- □ Bank
- □ Insurance company
- □ Store owners
- □ Smart shopping assistant

for this purpose...

- □ UNSPECIFIED
- □ Research
- □ Marketing
- □ Insurance coverage
- □ Immediate health care
- □ Identify high-risk people
- □ Personal contents/adds
- □ Share to improve service
- □ Future healthcare decisions
- □ Future financial services
- □ Interest me in other products/services
- □ Determine habits, interests/characteristics
- □ Mortgage application
- □ Suitability job
- □ Personal communication

gets this info... in this precision

	Precise	Approximate	Vague	None
Name	○	○	○	○
Age/Date of birth	○	○	○	○
Address	○	○	○	○
Insurance details	○	○	○	○
Bank account No	○	○	○	○
Debts	○	○	○	○
Height	○	○	○	○
Weight	○	○	○	○
Cholesterol	○	○	○	○
Heart Rate	○	○	○	○
Blood pressure	○	○	○	○
Glucose level	○	○	○	○
Stress level	○	○	○	○
Personally created video	○	○	○	○
Personally created pictures	○	○	○	○
Text/voice messages	○	○	○	○

Precise Approximate Vague None

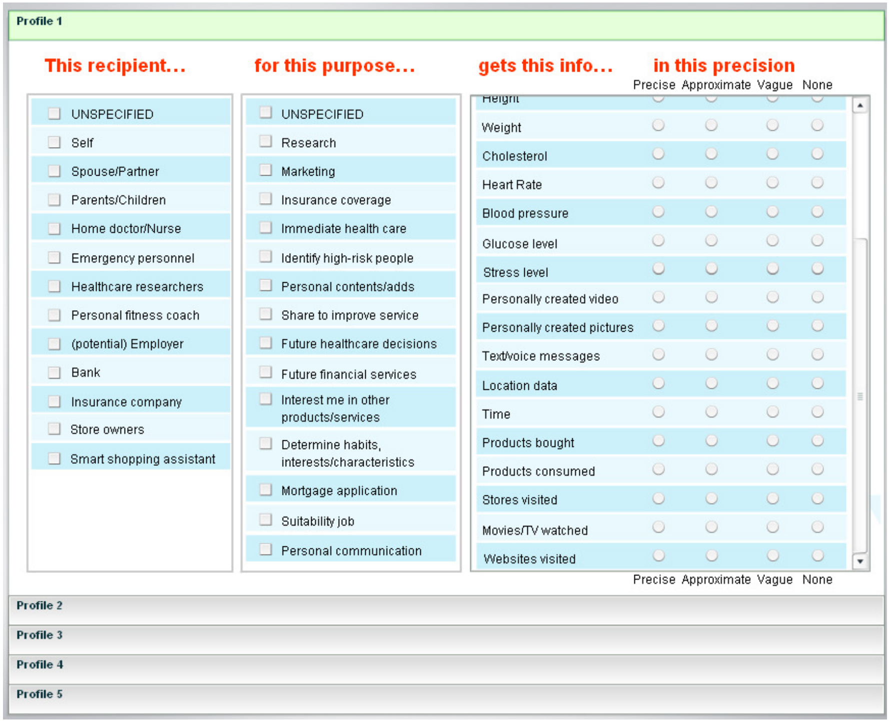
Profile 2

Profile 3

Profile 4

Profile 5

B



Profile 1

This recipient...

- □ UNSPECIFIED
- □ Self
- □ Spouse/Partner
- □ Parents/Children
- □ Home doctor/Nurse
- □ Emergency personnel
- □ Healthcare researchers
- □ Personal fitness coach
- □ (potential) Employer
- □ Bank
- □ Insurance company
- □ Store owners
- □ Smart shopping assistant

for this purpose...

- □ UNSPECIFIED
- □ Research
- □ Marketing
- □ Insurance coverage
- □ Immediate health care
- □ Identify high-risk people
- □ Personal contents/adds
- □ Share to improve service
- □ Future healthcare decisions
- □ Future financial services
- □ Interest me in other products/services
- □ Determine habits, interests/characteristics
- □ Mortgage application
- □ Suitability job
- □ Personal communication

gets this info... in this precision

	Precise	Approximate	Vague	None
Height	○	○	○	○
Weight	○	○	○	○
Cholesterol	○	○	○	○
Heart Rate	○	○	○	○
Blood pressure	○	○	○	○
Glucose level	○	○	○	○
Stress level	○	○	○	○
Personally created video	○	○	○	○
Personally created pictures	○	○	○	○
Text/voice messages	○	○	○	○
Location data	○	○	○	○
Time	○	○	○	○
Products bought	○	○	○	○
Products consumed	○	○	○	○
Stores visited	○	○	○	○
Movies/TV watched	○	○	○	○
Websites visited	○	○	○	○

Precise Approximate Vague None

Profile 2

Profile 3

Profile 4

Profile 5

Note: The user can specify which recipient is allowed to use which information in a certain precision (Precise, Approximate, Vague or None) for which purpose. Different combinations can be created by using multiple profiles. A: Visible when interface is first presented. When the scroll bar at the right side of the screen is used the remaining types of information become visible (compare right side in figure A and B).

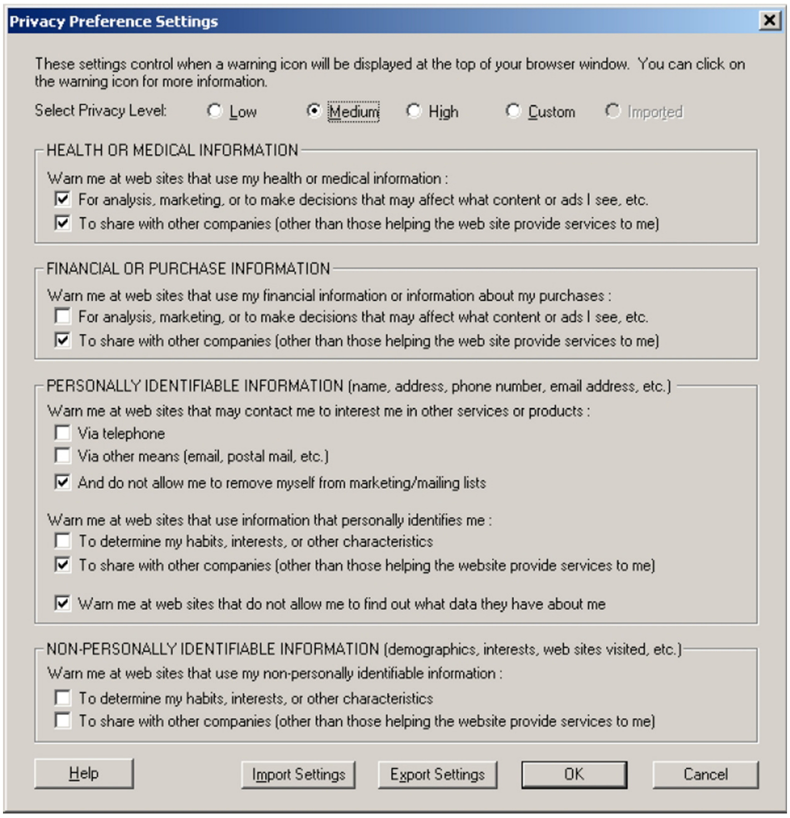
willingness to disclose and which were described before (see section 4.1). With this interface users can specify for what purposes they allow which recipient to use what information in which precision. Users are able to make different combinations among the dimensions (recipient, purpose of use and type of information) by using five different profiles. In this Profiles UI no default settings are available to users.

Some elements were similar in the Profiles UI to that of the faces metaphor by Lederer et al. (2004). For example in both interfaces users could choose between four different levels of precision (precise, approximate, vague and none) for the disclosure of each type of information. Furthermore, both interfaces allowed multiple combinations of privacy settings to be specified in the form of faces or profiles.
The faces metaphor allowed users to specify particular situations for which privacy preferences could be specified. In the evaluation by Lederer et al. (2004) of their interface it was discovered that situations and faces were regarded as belonging together. Therefore, in this study it was felt that a different dimension was needed instead of situations. Since usage is known to influence willingness to disclose information as mentioned before, this was taken as an alternative. Therefore, in the Profiles UI the option of specifying situations as available in the interface by Lederer et al. (2004) was replaced with purpose of use.

Privacy Interfaces based on Information-Use

The concept of Information-Use enables users to specify which types of information may not be disclosed for specific purposes of use. This conceptual model considers

Figure 4.3. Privacy preference specification interface for Privacy Bird (Cranor et al., 2006)



These settings control when a warning icon will be displayed at the top of your browser window. You can click on the warning icon for more information.

Select Privacy Level: ○ Low ● Medium ○ High ○ Custom ○ Imported

HEALTH OR MEDICAL INFORMATION

Warn me at web sites that use my health or medical information :

☑ For analysis, marketing, or to make decisions that may affect what content or ads I see, etc.

☑ To share with other companies (other than those helping the web site provide services to me)

FINANCIAL OR PURCHASE INFORMATION

Warn me at web sites that use my financial information or information about my purchases :

☐ For analysis, marketing, or to make decisions that may affect what content or ads I see, etc.

☑ To share with other companies (other than those helping the web site provide services to me)

PERSONALLY IDENTIFIABLE INFORMATION (name, address, phone number, email address, etc.)

Warn me at web sites that may contact me to interest me in other services or products :

☐ Via telephone

☐ Via other means (email, postal mail, etc.)

☑ And do not allow me to remove myself from marketing/mailing lists

Warn me at web sites that use information that personally identifies me :

☐ To determine my habits, interests, or other characteristics

☑ To share with other companies (other than those helping the website provide services to me)

☑ Warn me at web sites that do not allow me to find out what data they have about me

NON-PERSONALLY IDENTIFIABLE INFORMATION (demographics, interests, web sites visited, etc.)

Warn me at web sites that use my non-personally identifiable information :

☐ To determine my habits, interests, or other characteristics

☐ To share with other companies (other than those helping the website provide services to me) management as refined control of information flows (what information is disclosed for what purpose). This concept is intended to follow the privacy specifications as rules for the identification of inappropriate information use and to warn its users accordingly. As such, it does not support automated disclosure of information. Furthermore, this conceptual model does not allow the specification of recipients in advance. Instead the user can decide for each instance whether a particular recipient is allowed to receive information or not.

An example of an existing privacy interface based on Information-Use is Privacy Bird by Cranor et al. (2006). The privacy preference specification interface Privacy Bird is shown in Figure 4.3. Users can indicate when they want to be warned about inappropriate information use which is based on a combination of four different types of information (Health, Financial, Personally Identified, and Non-Personally Identified Information) and various purposes of use. Users can choose to set each of the twelve combinations separately, or to start from one of the four default privacy levels (Low, Medium, High and Custom).

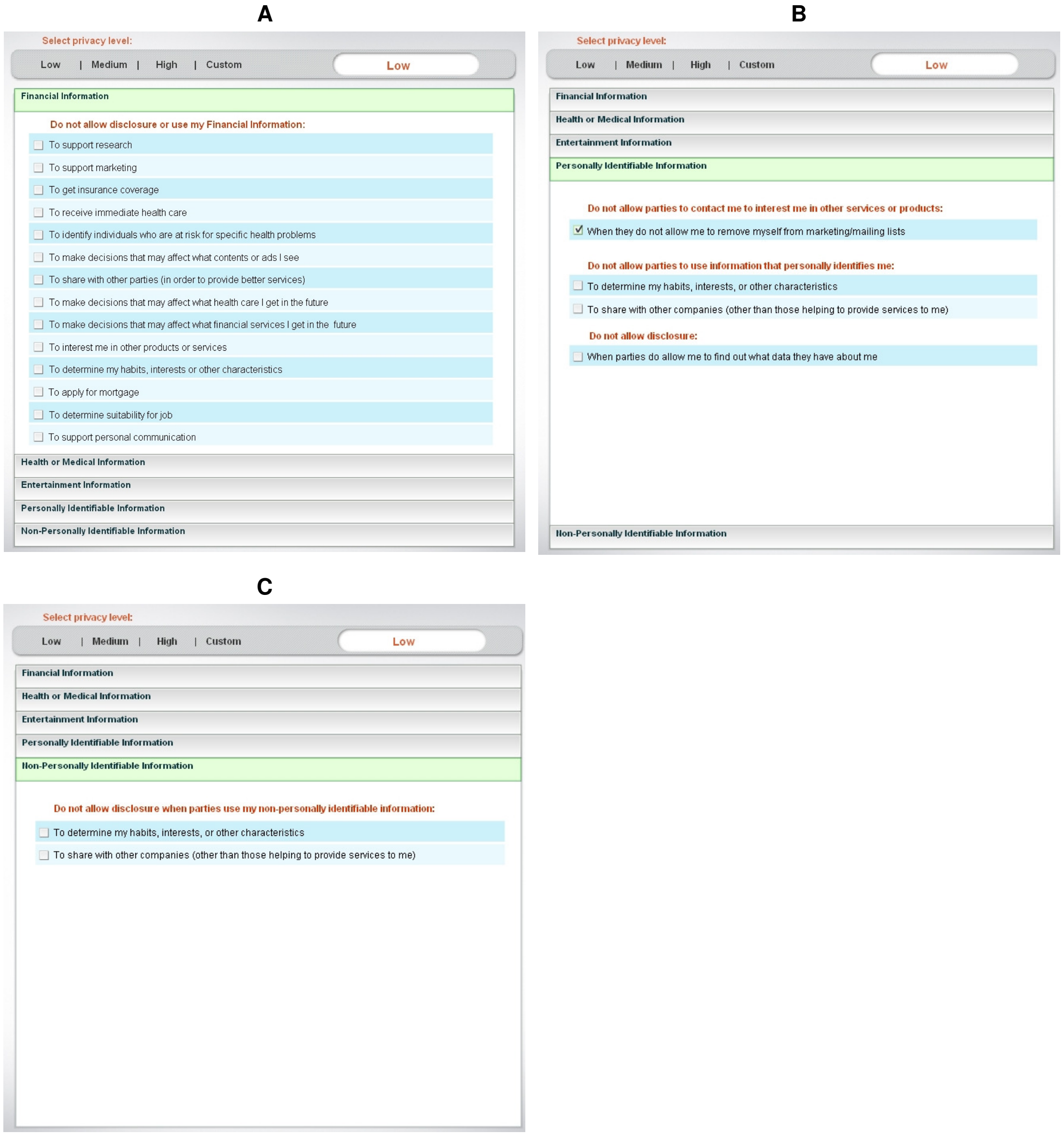
Another example of a privacy interface based on Information-Use is the specification of privacy preferences in Internet Explorer 6.0 or 7.0. With Internet Explorer the user can choose between 6 different types of privacy levels that relate to the use and blocking of cookies. It is also possible to specify exceptions for specific recipients (more specifically make exceptions in cookie handling for specific websites).

The interface that was based on Information-Use which was developed for the purpose of this chapter's study is called the Use UI. The Use UI (shown in Figure 4.4) enables users to specify the purposes for which specific types of information are not allowed to be used. This interface is different from both others in this study, since it requires users to specify which information may not be disclosed in a specific context. Furthermore, it is the only interface which allows users to start from default privacy settings.

Some elements were similar in the Use UI to that of Privacy Bird by by Cranor et al. (2006). For example both interfaces do not include the recipient dimension. Users can choose between four different default privacy settings (Low, Medium, High or Custom). Each of these settings can be adapted to fit personal preferences, but at any time only the currently selected level (including possible modifications) is active. It is only possible to choose between two different levels of disclosure: allowing disclosure (by leaving a box unchecked), or not allowing disclosure (by checking a box).

The Use UI provided one additional type of information in comparison to Privacy Bird, namely Entertainment Information. Furthermore, the list of purposes was extended in comparison to the Privacy Bird interface in order to fit a general personalization context.

Figure 4.4. Screenshots Use UI



A

Select privacy level:

Low | Medium | High | Custom — Low

Financial Information

Do not allow disclosure or use my Financial Information:

- □ To support research
- □ To support marketing
- □ To get insurance coverage
- □ To receive immediate health care
- □ To identify individuals who are at risk for specific health problems
- □ To make decisions that may affect what contents or ads I see
- □ To share with other parties (in order to provide better services)
- □ To make decisions that may affect what health care I get in the future
- □ To make decisions that may affect what financial services I get in the future
- □ To interest me in other products or services
- □ To determine my habits, interests or other characteristics
- □ To apply for mortgage
- □ To determine suitability for job
- □ To support personal communication

Health or Medical Information

Entertainment Information

Personally Identifiable Information

Non-Personally Identifiable Information

B

Select privacy level:

Low | Medium | High | Custom — Low

Financial Information

Health or Medical Information

Entertainment Information

Personally Identifiable Information

Do not allow parties to contact me to interest me in other services or products:

- ☑ When they do not allow me to remove myself from marketing/mailing lists

Do not allow parties to use information that personally identifies me:

- □ To determine my habits, interests, or other characteristics
- □ To share with other companies (other than those helping to provide services to me)

Do not allow disclosure:

- □ When parties do allow me to find out what data they have about me

Non-Personally Identifiable Information

C

Select privacy level:

Low | Medium | High | Custom — Low

Financial Information

Health or Medical Information

Entertainment Information

Personally Identifiable Information

Non-Personally Identifiable Information

Do not allow disclosure when parties use my non-personally identifiable information:

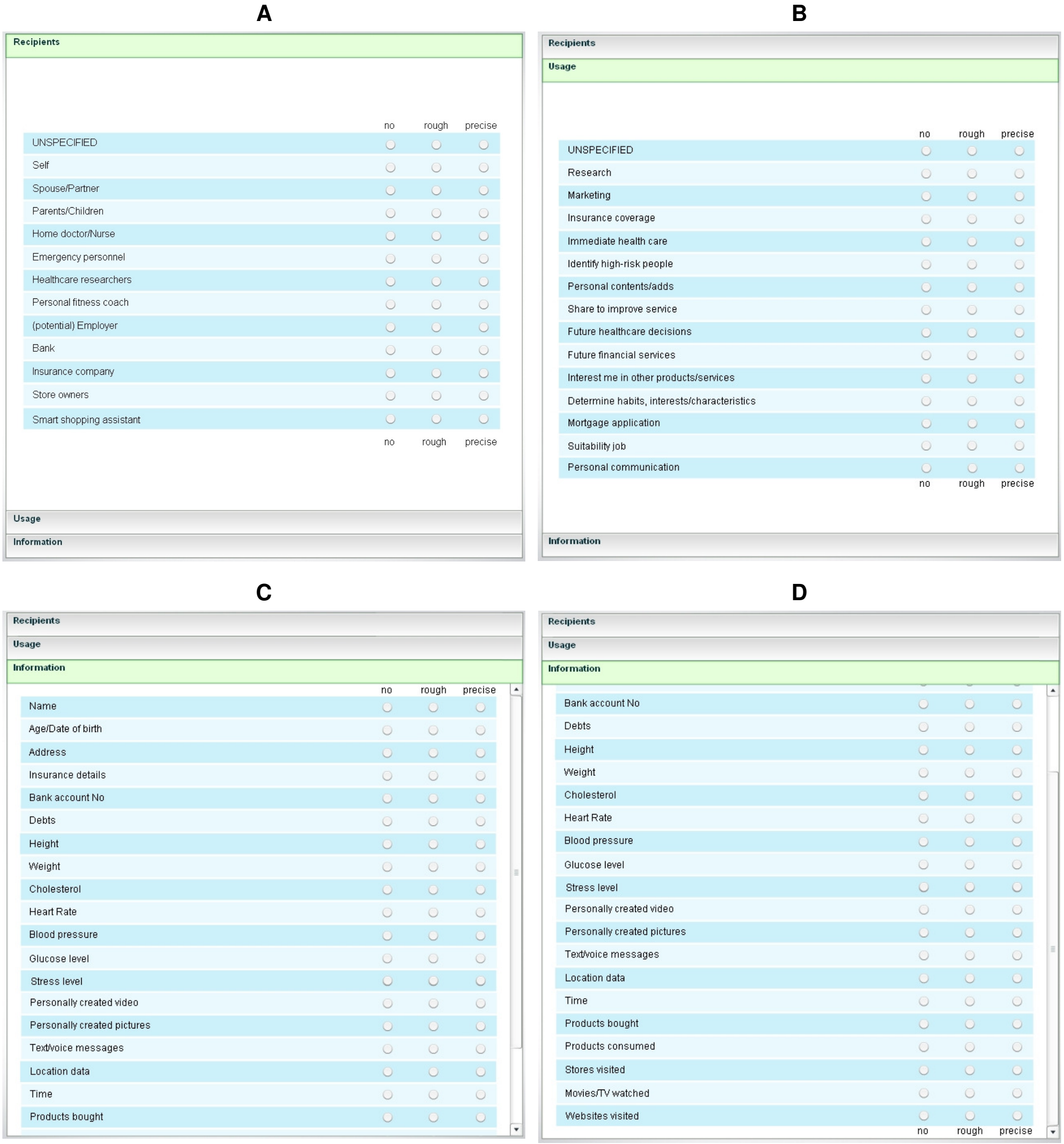
- □ To determine my habits, interests, or other characteristics
- □ To share with other companies (other than those helping to provide services to me)

Note: The user can choose any of the four default privacy levels (Low, Medium, High or Custom) on top of the interface. By default the Low privacy Level is selected. These levels represent an increasing amount of purposes that are disallowed. For different types of information (Financial, Health or Medical, Entertainment, Personally Identifiable, and Non-Personally Identifiable) the purposes of use can be blocked separately. A: Visible when interface is first presented. (The same purposes are included in the menus for Health or Medical Information & Entertainment Information). B: This part becomes visible when the user clicks on the 'Personally Identifiable Information' bar at the bottom of the screen and the Low privacy level is selected. C: This part becomes visible when the user clicks on the 'Non-Personally Identifiable Information' bar at the bottom of the screen and the Low or Medium privacy level is selected.

Privacy Interfaces based on Split-Dimension

The concept of Split-Dimension enables users to specify approved levels of information disclosure split across the three separate dimensions, namely recipient, purpose of use, and type of information. This conceptual model is simpler and more restrictive compared to the previous two, since the appropriate disclosure level of information can only be specified for each dimension (recipient, purpose of use and type of information) separately. It is relatively easy to specify the appropriate setting for each dimension; however the user is less flexible in defining the combinations between the different dimensions.

Figure 4.5. Screenshots Split UI



A

Recipients

	no	rough	precise
UNSPECIFIED	○	○	○
Self	○	○	○
Spouse/Partner	○	○	○
Parents/Children	○	○	○
Home doctor/Nurse	○	○	○
Emergency personnel	○	○	○
Healthcare researchers	○	○	○
Personal fitness coach	○	○	○
(potential) Employer	○	○	○
Bank	○	○	○
Insurance company	○	○	○
Store owners	○	○	○
Smart shopping assistant	○	○	○
	no	rough	precise

Usage

Information

B

Recipients

Usage

	no	rough	precise
UNSPECIFIED	○	○	○
Research	○	○	○
Marketing	○	○	○
Insurance coverage	○	○	○
Immediate health care	○	○	○
Identify high-risk people	○	○	○
Personal contents/adds	○	○	○
Share to improve service	○	○	○
Future healthcare decisions	○	○	○
Future financial services	○	○	○
Interest me in other products/services	○	○	○
Determine habits, interests/characteristics	○	○	○
Mortgage application	○	○	○
Suitability job	○	○	○
Personal communication	○	○	○
	no	rough	precise

Information

C

Recipients

Usage

Information

	no	rough	precise
Name	○	○	○
Age/Date of birth	○	○	○
Address	○	○	○
Insurance details	○	○	○
Bank account No	○	○	○
Debts	○	○	○
Height	○	○	○
Weight	○	○	○
Cholesterol	○	○	○
Heart Rate	○	○	○
Blood pressure	○	○	○
Glucose level	○	○	○
Stress level	○	○	○
Personally created video	○	○	○
Personally created pictures	○	○	○
Text/voice messages	○	○	○
Location data	○	○	○
Time	○	○	○
Products bought	○	○	○

D

Recipients

Usage

Information

	no	rough	precise
Bank account No	○	○	○
Debts	○	○	○
Height	○	○	○
Weight	○	○	○
Cholesterol	○	○	○
Heart Rate	○	○	○
Blood pressure	○	○	○
Glucose level	○	○	○
Stress level	○	○	○
Personally created video	○	○	○
Personally created pictures	○	○	○
Text/voice messages	○	○	○
Location data	○	○	○
Time	○	○	○
Products bought	○	○	○
Products consumed	○	○	○
Stores visited	○	○	○
Movies/TV watched	○	○	○
Websites visited	○	○	○
	no	rough	precise

Note: The user can indicate the level of disclosure (No, Rough or Precise) one allows for each recipient, purpose of use (usage) or type of information separately. A: Visible when interface is first presented. B: This part becomes visible when the user clicks on the 'Usage' bar at the bottom of the screen. C: This part becomes visible when the user clicks on the 'Information' bar at the bottom of the screen for the first time. When the scroll bar at the right side of the screen is used, the remaining types of information become visible (see bottom of figure C and D).

The interface that was based on Split-Dimension and which was developed for the purpose of this chapter's study is called the Split UI (see Figure 4.5). This third interface was considered as an extension and simplification of the Use UI in that it also considers the recipient of information, yet it does not allow explicit combinations of privacy preferences to be specified.

With the Split UI users can choose between three levels of disclosure (no, rough, precise), depending on the three dimensions that are known to influence people's willingness to disclose (recipient, purpose of use, and type of information). However, people cannot explicitly indicate combinations between these three dimensions. One can specify the desired level of disclosure for each recipient, for each purpose of use and for each type of information separately. The actual disclosure level in each situation will be determined by the lowest disclosure level chosen for each of the instances of the three dimensions currently present. For example if you have indicated precise disclosure for home doctor/nurse, no for research and rough for blood pressure, there will be no information disclosed for a situation involving these instances. There are no default settings available to users in this Split UI.

4.1.2 The acceptance model for privacy interfaces (PI-Model)

This study aims to examine the influence of various factors upon the acceptance of privacy interfaces such as perceived trust, risk, usefulness and ease of use. Earlier work on potential relations between these factors is available in the form of various models. A literature study was performed in search for models that included either (privacy) risk or trust factors. Eight studies were found that included models meeting these requirements. The eight existing models were used to guide the creation of a model predicting the acceptance of privacy interfaces. In the remainder of this chapter the former will be referred to as background models and the latter as the acceptance model for privacy interfaces (PI-Model for short).

Among these eight background models, three models were extensions of the Technology Acceptance Model. The Technology Acceptance Model (TAM) attempts to predict intention to use by both usefulness and ease of use (Davis et al., 1989). The extensions of TAM included either risk (Featherman & Pavlou, 2003), trust (Suh & Han , 2002) or both (Lui & Jamieson, 2003). Another model including both risk and trust was the model by Corritore et al. (2005), which also included ease of use. The other four models all included (privacy) concern, trust and some form of intention to use (Chellappa & Sin, 2005; Dinev & Hart, 2003; 2006; Malhotra et al. 2004).

All background models except the model of Suh and Han (2002) included either risk or concern in their model. Wide variations of items are used to measure either risk or concern.

Ease of use is included in half of the background models. All of these models use (slight adaptations of) the original TAM items. Only Featherman and Pavlou (2003) do not provide the items used in their study to represent ease of use. The other three studies use the same four items in slightly different wording. Suh and Han (2002) use one additional item.

Intention to use is represented in different forms (such as adoption intention or intention to transact) and is included in all background models except that by Corritore et al.

(2005). Again Featherman and Pavlou (2003) do not provide the items used in their study to represent the construct. The other models use wide variations of items to measure intention to use.

Trust is included in all background models except that by Featherman and Pavlou (2003). Lui and Jamieson (2003) include various trust constructs in their model, for example propensity to trust and technology trust. The other background models include only one trust construct which is measured by a range of items regarding aspects such as safety, reliability, and trustworthiness.

Three background models include usefulness as used in TAM (Featherman & Pavlou, 2003; Lui & Jamieson, 2003; Suh & Han, 2002), whereas one model includes a slight variation of usefulness, namely value of personalization (Chellapa & Sin, 2005).

The eight background models are shown in Figure 4.6. The relations between the variables indicated by straight arrows symbolize causal relationships; the variable at the end of the arrow is assumed to be the effect and the one at the beginning is assumed to be the cause (Raykov & Marcoulides, 2000). The only relation which is not assumed to be a causal relationship is the one between privacy concern and trust indicated by a curved arrow in the model by Chellapa and Sin (2005). A curved two-way arrow symbolizes covariance or a non-directional association between the connected variables (Raykov & Marcoulides, 2000). All variables depicted in ovals are latent variables (they cannot be measured directly, but are hypothesized to underlie the observed variables in the form of questionnaire items). The one variable represented by a rectangle is type of information in the model of Malhotra et al. (2004). This is a manifest variable (it is directly observable or measurable), since it was controlled for by the researchers.

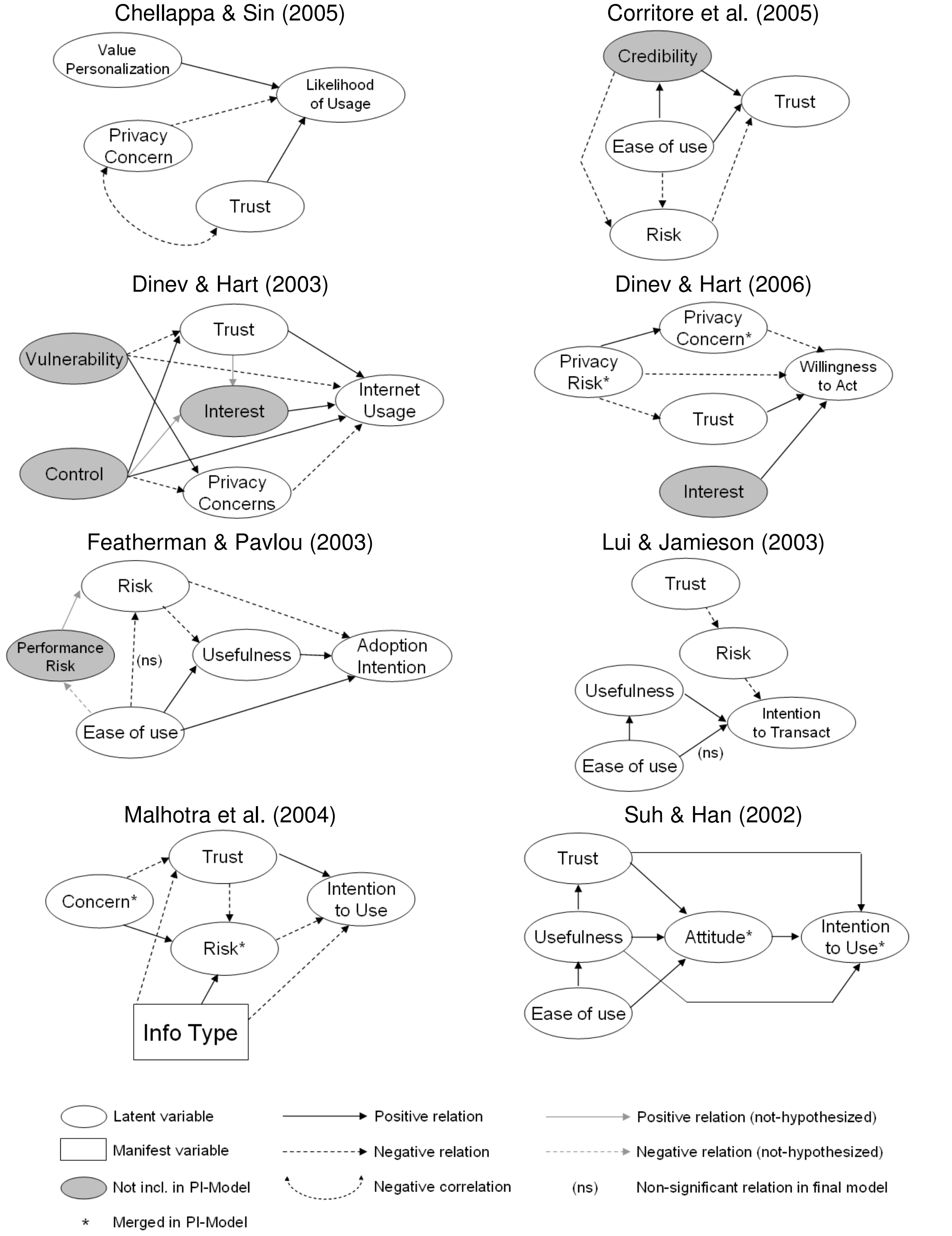
The work of Chellappa and Sin (2005) confirms the correlation between trust and privacy concern. They found a negative relation between privacy concern and intention to use, and a positive relation between trust and intention to use.

Corritore et al. (2005) present an instrument for studying trust of an individual in a given website. The model underlying this instrument hypothesizes a relation between the perception of ease of use and risk, and of both of these concepts with trust. This is the only model that does not predict some kind of intention to use.

Dinev and Hart (2003) present the development and validation of a model to assess the trade-offs between perceived personal benefits and privacy costs associated with e-commerce transactions. Their results indicate that trust influences decisions to engage in e-commerce transactions, i.e. trust is positively related to intention to use. Privacy concerns are found to have a negative relation with the use of Internet for e-commerce purposes. In a later study Dinev and Hart (2006) confirm a negative relation between perceived privacy risk and trust, and between privacy concerns and willingness to disclose information. A positive relation was found between perceived trust and willingness to disclosure information.

Featherman and Pavlou (2003) have found negative relations between perceived risk on the one hand, and usefulness and adoption intention on the other hand. They have found a positive relation between ease of use and usefulness. Positive relations were also found for usefulness and ease of use with adoption intention.

Figure 4.6. Constructs and relations in background models



Lui and Jamieson (2003) have confirmed negative relations between trust and perceived risk, and between perceived risk and intention to transact. Perceived ease of use was found to be positively related to perceived usefulness, which on its own was positively related to intention to transact.

Malhotra et al. (2004) have found a negative relationship between trusting beliefs and risk beliefs, and between risk beliefs and behavioral intention. A positive relation was found between trusting beliefs and behavioral intention.

Suh and Han (2002) have found positive relations between perceived ease of use and perceived usefulness, and between the latter and trust. Positive relations are found between both trust and perceived usefulness with intention to use.

Table 4.1 shows which constructs of the background models are included or omitted in the PI-Model. It shows the similarities in constructs between the different background models and provides the name for the construct in the PI-Model. The items used in the studies of the background models can be found in Appendix C. The constructs of (privacy) concern and (privacy) risk are combined in the PI-Model.

Table 4.1. Overview of included constructs in PI-Model and omitted background model constructs

Construct(s)	#	Background Model
Risk/Concern		
Concern & Risk	1	Mal04
Privacy concern	2	Che05; Din03
Privacy concern & Privacy risk	1	Din06
Risk	3	Cor05; Fea03; Lui03
Ease of use	4	Cor05; Fea03; Lui03; Suh02
Intention to use		
Adoption intention	1	Fea03
Attitude & Intention to use	1	Suh02
Intention to transact	1	Lui03
Intention to use	1	Mal04
Internet usage	1	Din03
Likelihood of usage	1	Che05
Willingness to act	1	Din06
Trust	7	Che05; Cor05; Din03; Din06; Lui03; Mal04; Suh02
Usefulness		
Usefulness	3	Fea03; Lui03; Suh02
Value personalization	1	Che05
Omitted		
Control	1	Din03
Credibility	1	Cor05
Performance risk	1	Fea03
Type of information	1	Mal04
Vulnerability	1	Din03

Note: The middle column indicates the amount of background models including the construct. The background models are referred to by three letters of the first author's last name and the year of publication.

Table 4.2. Overview of specified relations in background models and PI-Model

Construct1	Construct2	#	Models	Relation			PI-Model		
Trust	Intention to use	5/6	Che05	+	>		+	>	$H_{PM}1$
			Din03	+	>				
			Din06	+	>				
			Lui03	x	x				
			Mal04	+	>				
			Suh02	+	>				
Risk/Concern	Intention to use	6/6	Che05	-	>		-	>	$H_{PM}2$
			Din03	-	>				
			Din06	-	>				
			Fea03	-	>				
			Lui03	-	>				
			Mal04	-	>				
Ease of use	Intention to use	3/3	Fea03	+	>		+	>	$H_{PM}3$
			Lui03	+	>	*			
			Suh02	+	>				
Usefulness	Intention to use	4/4	Che05	+	>		+	>	$H_{PM}4$
			Fea03	+	>				
			Lui03	+	>				
			Suh02	+	>				
Risk/Concern	Trust	5/6	Che05	-	<>		-	<>	($H_{PM}5$)
			Cor05	-	>				
			Din03	x	x				
			Din06	-	>				
			Lui03	-	<				
			Mal04	-	<				
Ease of use	Risk/Concern	2/3	Cor05	-	>		-	>	($H_{PM}6$)
			Fea03	-	>	*			
			Lui03	x	x				
Ease of use	Usefulness	3/3	Fea03	+	>		+	>	($H_{PM}7$)
			Lui03	+	>				
			Suh02	+	>				
Risk/Concern	Usefulness	1/3	Che05	x	x		x	x	
			Fea03	-	>				
			Lui03	x	x				
Ease of use	Trust	1/3	Cor05	+	>		x	x	
			Lui03	x	x				
			Suh02	x	x				
Usefulness	Trust	1/3	Che05	x	x		x	x	
			Lui03	x	x				
			Suh02	+	>				

Note: # = Amount of background models specifying a relationship between both constructs out of the total background models including both constructs - = Negative relationship; + = Positive relationship; x = Not specified relationship; < Construct 1 is influenced by construct 2; > Construct 1 influences construct 2; * Relation not significant in final model. Background models are referred to by three letters of the first author's last name and the year of publication.

Table 4.2 shows for each pair of constructs which background models include both constructs and (if applicable) what relation they specify between the two constructs. Furthermore Table 4.2 shows what relation is specified in the PI-Model on the basis of these background models. This set of dependencies that is hypothesized between the five attributes trust, risk/concern, usefulness, ease of use, and intention to use on the basis of the eight background models is visualized in Figure 4.7.

Each of the hypotheses underlying the PI-Model of this study (indicated as $\mathrm{H}_{\mathbf{PM}}$) will be described in more detail below (see also Figure 4.6 & Figure 4.7 and Table 4.1 & Table 4.2). All of the constructs in the PI-model are perceived measures. This means that participants are asked to judge perceived trust, perceived risk, perceived usefulness, perceived ease of use, and perceived intention to use. However, to improve readability the word perceived will be omitted in the remainder of this chapter whenever the constructs of the PI-model are discussed.

There are six background models that include both trust and intention to use. One of these models does not specify a relation between the two constructs (Lui & Jamieson, 2003). The remaining five background models all specify a positive relation from trust to intention to use (Dinev & Hart, 2003, 2006; Chellappa & Sin, 2005; Malhotra et al., 2004; Suh & Han, 2002). Therefore the PI-Model proposes:

$\mathbf{H_{PM}1}$: A higher level of trust is related to a higher intention to use.

The constructs of risk and intention to use are included by six background models as well (Dinev & Hart, 2003, 2006; Lui & Jamieson, 2003; Chellappa & Sin, 2005; Malhotra et al., 2004; Featherman & Pavlou, 2003). All of these models specify a negative relation from risk to intention to use. Therefore the PI-Model proposes:

$\mathbf{H_{PM}2}$: A lower level of risk/concern is related to a higher intention to use.

Three background models include both ease of use and intention to use. Both extensions of the Technology Acceptance Model include a positive relation from ease of use to intention to use (Featherman & Pavlou, 2003; Lui & Jamieson, 2003), although this relation is not significant in the latter final model. Furthermore, if attitude and intention to use are combined into one construct, then the model by Suh and Han (2002) also specifies a positive relation between ease of use and intention to use. Therefore the PI-Model proposes:

$\mathbf{H_{PM}3}$: A higher level of ease of use is related to a higher intention to use.

All three background models that include both usefulness and intention to use assume a positive relation from usefulness to intention to use (Featherman & Pavlou, 2003; Lui & Jamieson, 2003; and Suh & Han, 2002). Therefore the PI-Model proposes:

$\mathbf{H_{PM}4}$: A higher level of usefulness is related to a higher intention to use.

There are in total six background models that include both risk and trust. Only one of these models does not specify a relation between the two constructs (Dinev & Hart, 2003). Chellappa and Sin (2005) have specified a non-directional association between risk and trust, whereas in four models a negative causal relationship is specified between the two constructs. Some models assume trust to be the cause and risk to be the effect of this relation (Malhotra et al., 2004; Lui & Jamieson, 2003), whereas others assume the opposite to be true (Corritore et al., 2005; Dinev & Hart, 2006). Therefore the PI-Model proposes:

H_{PM}5: Risk/concern is negatively associated with trust.

Three background models include both ease of use and risk/concern (this will be referred to as risk from now on). One of these models does not specify a relation between the two constructs (Lui & Jamieson, 2003). The other two specify a negative relation from ease of use to risk (Corritore et al., 2005; Featherman & Pavlou, 2003), although in the latter final model this relation was not significant. Nevertheless, the PI-Model proposes:

H_{PM}6: A higher level of ease of use is related to a lower level of risk.

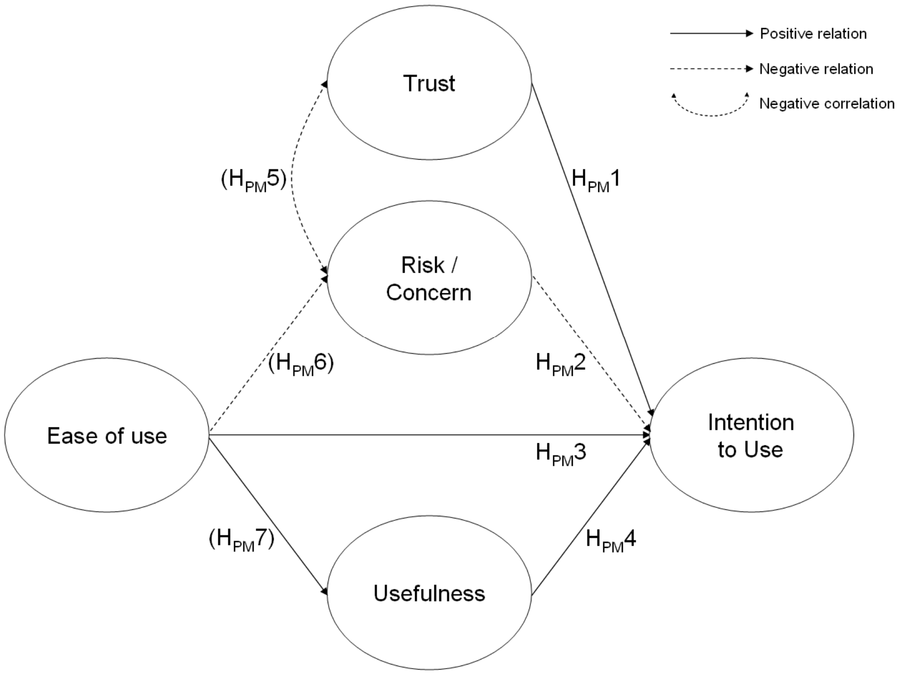
Of the three background models that include both ease of use and usefulness, all specify a positive relation from ease of use to usefulness (Featherman & Pavlou, 2003; Lui & Jamieson, 2003; Suh & Han, 2002). Therefore the PI-Model proposes:

H_{PM}7: A higher level of ease of use is related to a higher level of usefulness.

No relations are specified in the PI-Model between the constructs of trust and ease of use, trust and usefulness, and risk and usefulness. For these pairs of constructs there are three background models each that include both constructs, whereas there is only one background model that specifies a relation between the two.

Since the aim is to explain the relative importance of the four factors on intention to use, hypotheses H_{PM}5, 6 and 7 will not be tested in this study.

Figure 4.7. Hypothesized acceptance model for privacy interfaces (PI-Model)



Note: Hypotheses in parentheses are not explicitly tested in this study.

The proposed PI-Model (see Figure 4.7) is different from the models it is based on with respect to included model elements and context of investigation. The PI-model incorporates both trust and risk besides the technology acceptance elements usefulness and ease of use in an attempt to predict intention to use.

In terms of model elements the PI-Model is most similar to the model by Lui and Jamieson (2003). Even though the models include the same elements, they specify different relations between the elements. Besides, the model by Lui and Jamieson focuses on Internet-based business-to-consumer electronic commerce instead of Ambient Intelligence applications.

The context of the PI-model is different from all studies and background models described above. The background models investigate user behavior or intentions on the internet, yet the PI-Model of this study focuses on user intentions in an Ambient Intelligence environment. The context of Ambient Intelligence is provided by scenarios in this study. The domain of the model by Chellapa and Sin (2005) is closest to the PI-Model, since it focuses on personalization. The difference between these models is in the included elements.

4.1.3 Individual differences in privacy perception

Privacy is known to be perceived differently among people. Groups of people can be distinguished with varying privacy attitudes. The studies described in the previous chapters have found individual differences in the perception of privacy. In the Music Recommender study described in chapter 2 individual differences were found, in the sense that some participants strongly favored their anonymity, whereas for others this was less important. The fourth study described in chapter 3 discerned four different groups of people. One group was mainly concerned about Purpose of Use, and another had a desire for Guarantees. The third required User Control, and the last group especially cared about the type of data that is collected, and wanted to be able to inspect that data.

Many categorizations are based on Westin's typology of privacy unconcerned, privacy pragmatists and privacy fundamentalists (Harris Interactive, 2002), such as the work of Consolvo et al. (2005). Also Ackerman et al. (1999) have distinguished three groups of individuals based on general attitudes about privacy and responses to specific scenarios. The groups are: privacy fundamentalists (very concerned about any use of their data, generally unwilling to provide their data to Web sites), pragmatists (concerned about data use, but to a lesser extent), and the marginally concerned (generally willing to provide data to Web sites, although they still value their privacy under some conditions).

Berendt et al. (2005) found four different groups of users based on a clustering of the answers to privacy-related questions. They distinguished a group of privacy fundamentalists and a group of marginally concerned users as well. The remaining participants were differentiated by the focus of their privacy concerns: some are more concerned about revealing information like their name, email, or address (identity concerned users), while others are more concerned about disclosing such information as their interests, hobbies, and health status (profiling averse users).

Sheehan (2002) provides a more detailed categorization, and distinguishes four groups of people based on 15 measures for privacy concern. These groups are: unconcerned (minimal concern with privacy online, somewhat older than average, low education), circumspect (minimal concern with privacy online overall, although some situations may cause them to have higher levels of concern, younger than average, low education), wary (moderate level of concern with their privacy in many situations, and several situations cause them to experience higher than average concern with privacy, younger and better educated), and alarmed Internet users (highly concerned about privacy online, older and high level of education).

In this study, an attempt is made to check whether there are individual differences with regard to the perception of the three conceptual models for privacy interfaces. A comparison of the privacy classifications of people described in this section is difficult due to the limited amount of information provided in the papers. Therefore, it can not be concluded that any one of the classifications is superior to the others and thus more research is needed. Furthermore, the music recommender study, described in chapter 2, indicated the need to check and assure that privacy research participants represent a range of privacy attitudes. The more accurate specifications of user samples can be, the better this is for future research. In conclusion, it remains relevant to produce a more reliable classification of people with regard to privacy perception.

4.1.4 Anticipated effects of the three interfaces

The Profiles UI was expected to be intuitive, versatile and flexible, because it allows people to specify different combinations of recipients, purpose of use, and type of information. Besides, it allows varying levels of precision for each type of information. It was expected that due to these extensive possibilities people would experience more control, and hence the interface would be perceived to be more trustworthy. Control is not explicitly incorporated in the PI-Model, but it is indirectly represented by the absence of risk. Its wide possibilities would make it easier for people to set the interface according to their privacy preferences. In comparison with the other two interfaces it was expected that the Profiles UI would be perceived to provide high ease of use, low risk or concern, and high trust. Consequently, usefulness and intention to use were expected to be high as well.

The Use UI was expected to be perceived as very straightforward, because of its available defaults. Users do not have to think of their own preferences, but they can use the defaults to create their own opinion. A system with defaults settings is faster, since it allows users to recognize a default and accept it, rather than having to specify a value or option (Nielsen, 1993). Besides, default settings help novice users to learn the system since they reduce the number of actions users need to make before using the system, and the default values provide an indication of the kind of values that can be specified in the system (Nielsen, 1993). Due to these defaults it was expected an easy interface for people to use. And since only purpose of use and type of information are combined, it was expected to be fairly easy for people to see what settings are made. On the contrary, due to the absence of the recipient dimension, the interface was expected to be less trustworthy and provide less control. Besides, control was also expected to be limited due to only three levels of disclosure. Due to the more restricted possibilities in comparison to the Profiles UI it would be slightly more difficult for people to set the interface according to their privacy preferences. Overall, in terms of the model measures, it was expected that the Use UI would be perceived to provide medium levels of trust, risk, usefulness, ease of use, and intention to use.

The Split UI was expected to be perceived as very straightforward, since a level of disclosure could be chosen for each dimension separately. Related to that it was expected to be easy to learn, and easy to see what settings are chosen. The Split UI allows varying levels of disclosure for each element, and recipient related preferences can be specified. However, the Split UI does not support the explicit specification of combinations of privacy preferences, and as such the interface may be regarded as more difficult for people to set according to their preferences. Overall, in comparison with the other two interfaces, in terms of the model measures, it was expected that the Split UI would be perceived to provide medium levels of trust, risk, usefulness, ease of use, and intention to use.

4.2 METHOD

4.2.1 Design

For this study a within subject design was chosen. Thus, participants were exposed to all three interfaces and this allowed them to make comparisons between all of them. The order in which participants used the systems was counterbalanced. With three interfaces, there are six different sequences possible in which participants can use each of these models. Participants were assigned to one of these sequences in a balanced manner.
The main evaluation of interfaces was performed in pairs (see measures section for the reasoning behind this approach). Participants compared two interfaces at a time on the basis of three different measures. The evaluation order of the pairs of interfaces (Profiles vs. UI; Use vs. Split; Split vs. Profiles) was counterbalanced, and the position of each interface within a pair (first or second interface, i.e. left or right side of the screen) was controlled for as well.

4.2.2 Participants

For this study persons between 17 and 60 years of age were contacted and informed about the general purpose and approach of the study. Only participants who indicated to feel both confident using a PC including some new programs and comfortable reading/writing English were invited to participate in the study. This group of participants was chosen to represent a potential user group of Ambient Intelligence environments, yet to prevent that participating would be too demanding or difficult for people due to low or high age.

Potential participants were contacted in various ways: via a database of people who have registered themselves to be interested to participate in research experiments from the University, via colleagues, friends and family and by addressing people who were present at the University campus at the time of the experiment. Participants were informed in advance that they would receive a gift coupon of 20 euros after completing the study. In total 78 participants completed the study.

4.2.3 Apparatus and materials

The experiment was conducted in the Psychology Laboratory at the University with individual booths for each participant (see Figure 4.8). Each booth contains a PC connected to the Internet, which was used for presenting the interfaces and administering the questionnaire. The laboratory enabled to run experimental sessions with multiple participants at once. Participants' progress could be monitored from the observation booth.

Figure 4.8. Impression of the Psychology Laboratory where the experiment was conducted

An experimental system was built which included participant instructions, the questionnaire and the activation of interfaces. The system took care of the randomization of interface sequences for both use and evaluation. The interfaces for each of the conceptual models were built in Flash (see Figure 4.2, Figure 4.4, and Figure 4.5).

Five scenarios were used to describe situations in which participants would be using a profile manager to express their privacy preferences. Participants were exposed to all five scenarios. These scenarios were chosen to provide a wide variety of contexts: picture sharing, smart shopping, location tracking, personal movie record, and health monitoring. An example of such a scenario text is presented in Figure 4.9, the other scenarios can be found in Appendix D2.

The picture sharing scenario is derived from mobile blogging such as Nokia Mobilize and Share (MOSH) or Buzznet which are examples of communities where users can easily share (self-created) content. The smart shopping scenario is based on the paper by Günther and Spiekermann (2005), which uses a film about future shopping environments in which RFID technology is used. Location tracking is known to be privacy sensitive (Consolvo et al., 2005) and is used in one of the scenarios as well. A personal movie record is derived from digital video recorders such as TiVo (Barton, 2006). The health monitoring system is based on systems for remote patient monitoring or in home health monitoring such as Motiva by Philips, IBM's Personal Care Connect or Elite Care (Stanford, 2002). All scenarios included a description of the main user, the personalized system involved and some of the potential trade-offs a user faces between effective use of such a system and protecting one's privacy.

In the next stage of the experiment, participants were asked to use the interfaces for the second time and set a few specified privacy preferences with each interface. An example of such an instruction is shown in Figure 4.10, the other task instructions are included in Appendix D3.

Figure 4.9. An example of a scenario text

Bob Conner is a 25-year old law-student. He lives with four other students in a house on campus. Bob got a new cell phone for his birthday last week, and he wants to set it up and connect it to his smart living environment.

Bob's cell phone has a camera, which he uses to take pictures where-ever he goes. The camera makes use of a new service that helps him automatically share his pictures with friends or family, and his own photo-collection stored at his PC back home. More than this, pictures are automatically annotated with information regarding the time and location where they were taken. Bob really appreciates this automatically sharing of pictures since it saves him a lot of trouble searching for the right pictures, adding context information and then sending them to some of his relatives. Also, he enjoys using the location and time information to find pictures in his collection. On the other hand, he feels it maybe somewhat risky if his parents get to see all the pictures from his last holiday with his mates.

Task:
You may want to share your pictures with some people who are close to you to share your experiences. However, there may be some people whom you don't want to have access to your pictures. You may want to have your pictures available on other devices, to be able to view them from other places or in other modes as well, or maybe you prefer to keep them on your cell phone. Maybe you want your pictures only to be used for certain purposes. Possibly you want the additional time and location information only to be accessible by some people or for some purposes.
Please take some time to think about this situation.

Note: Text for Scenario 1 - Picture sharing.

The tasks related to three different contexts, namely a health-monitoring program, a cell phone with location tracking for others, and a mobile device that allows automatic sharing of pictures, messages and location information. The actual settings to be performed with each interface were adapted according to the underlying conceptual model. For instance, in the tasks for the Use UI no reference was made to a particular recipient, since the interface does not allow prevention of disclosure to particular recipients.

Participants' answers to the questions were automatically stored in a database. Throughout the whole experiment a capture was made of each participant's screen and thus their mouse movements by use of Camtasia. This was done in order to investigate

Figure 4.10. An example of an instruction text for second use

You are participating in a health-monitoring program that allows various people, like your doctor or insurance company, to have remote access to your personal information while you are able to stay at home.
In the light of this program you decide to make all of the following settings:

- You want your medical information to be available for insurance coverage.
- You do not want your medical information to be used for identifying people at high-risk for specific health problems, or for marketing purposes.
- You do not want your entertainment information to be used to decide about future health care services.
- You want your financial information to be used for insurance coverage.

Note: Text for Task 1 - Use UI.

afterwards in what way the interfaces were used by participants and what settings were made with each interface. These settings made by participants were recorded manually on the basis of the Camtasia recording. Any comments made or questions posed by participants throughout or at the end of the experiment were written down as well.

4.2.4 Procedure

The procedure followed in this study is shown in Figure 4.11 and will be explained below. For clarification of the procedure this section indicates at what points certain measures were used. For the exact focus and phrasing of the measures used, please consult the relevant section 4.2.5 on Measures.

Potential participants were invited to participate in a research concerning “the evaluation of interfaces for managing privacy preferences”. When people met the criteria for age, confidence in using a PC, and language, an appointment was scheduled. For efficiency reasons, appointments were made with multiple participants at once. However, care was taken that enough time was available to answer individual questions.

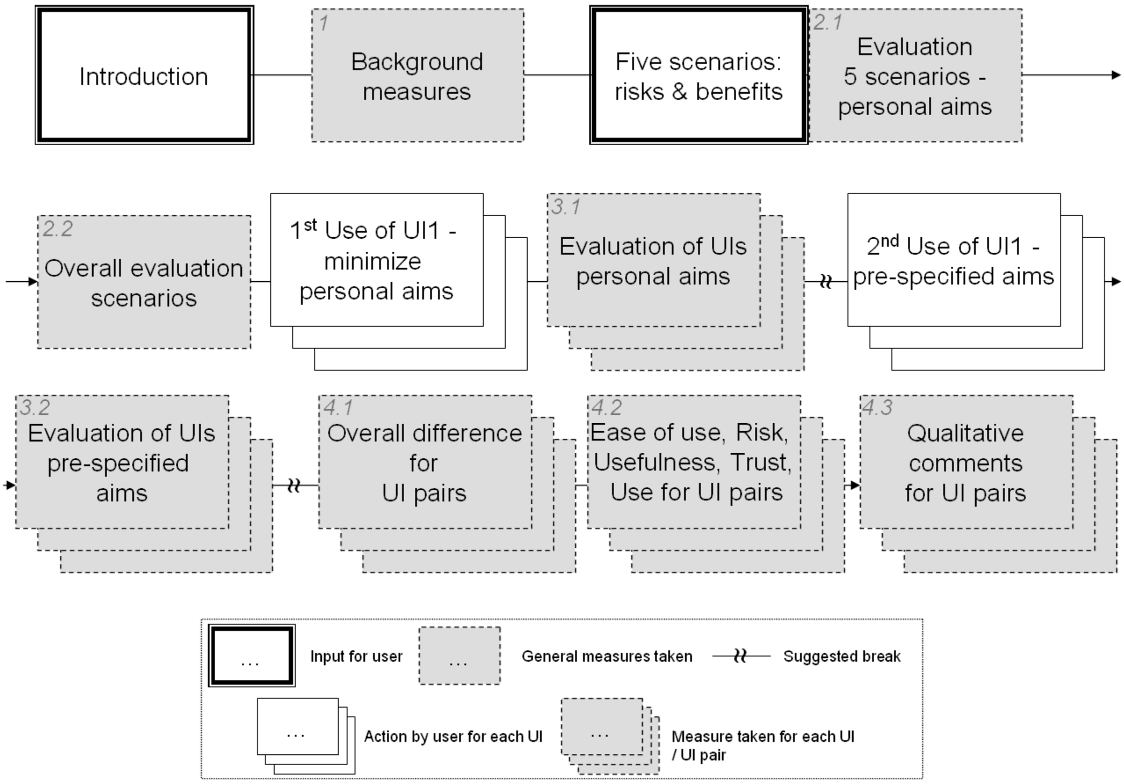
Once in the lab, participants were given some information about the study and the procedure (see Appendix D1). They were told that questions could be asked throughout the study; however little information could be given about how to operate the interfaces they would use, since the aim of the study was for participants to find out for themselves how to use these interfaces.

First of all, participants were asked to provide some background information (measure 1 in Figure 4.11 and section 4.2.5). Then, participants were shown five specific scenarios that illustrate potential risks and benefits of a personalized environment (picture sharing, smart shopping, location tracking, personal movie record, health monitoring). The scenarios served to provide participants with a context of reference for the privacy interfaces, because privacy concerns and preferences are known to be context specific (Consolvo et al., 2005; Lederer, Mankoff, et al., 2003; Sheehan, 2002). After each scenario participants were asked to indicate their (privacy) concerns with regard to possible recipients, purpose of use, and type of information (measure 2.1). This was done as a manipulation check to confirm that the scenarios indeed provided some level of concern, and thus participants had a purpose to use the interfaces for setting their privacy preferences. And finally they were asked to rate the level of risk involved in a situation encompassing all five scenarios (measure 2.2).

Next, participants were asked to use all three interfaces for minimizing their privacy concerns (as expressed before) in light of a situation encompassing all five scenarios. This was done to ensure that participants have a personal interest in setting the interfaces correctly. Then participants were asked to evaluate the systems with regard to their level of concern after this first use (measure 3.1).

Subsequently participants were asked to make with each interface a few privacy settings that were pre-determined by the experimenter. These fixed tasks were provided in order to allow participants to fully experience the possibilities and limitations of an interface. This was done since it was expected that participants might not discover the possibilities and limitations based on the first free use of the interfaces. Afterwards they had to rate the complexity of each interface for this second use (measure 3.2).

Figure 4.11. Flowchart of procedure followed in experiment


Introduction
1
Background measures
Five scenarios: risks & benefits
2.1
Evaluation 5 scenarios - personal aims
2.2
Overall evaluation scenarios
1st Use of UI1 - minimize personal aims
3.1
Evaluation of UIs personal aims
2nd Use of UI1 - pre-specified aims
3.2
Evaluation of UIs pre-specified aims
4.1
Overall difference for UI pairs
4.2
Ease of use, Risk, Usefulness, Trust, Use for UI pairs
4.3
Qualitative comments for UI pairs
Input for user
General measures taken
Suggested break
Action by user for each UI
Measure taken for each UI / UI pair

Then, the final evaluation of the interfaces was performed, which consisted of a paired evaluation of the interfaces. First, participants were asked to rate the overall difference between each pair (measure 4.1). Second, they were asked to compare each pair on the basis of statements relating to trust, risk, usefulness, ease of use and intention to use (measure 4.2). Finally they were invited to express open comments with regard to each pair of interfaces (measure 4.3).

It took participants approximately two hours (with a maximum of three hours) to complete the study. Participants were allowed to take small breaks during the study in order to keep focused and concentrated. By means of the experimental system participants were pointed to two suitable moments for a break, namely right after the evaluation of both the first and second use of the interfaces. In principle it could have been possible for participants to speak to each other during the breaks; however, in practice participants took their breaks at different times due to different work paces.

4.2.5 Measures

Measure 1: General background data (see Appendix D1)

The background measures taken in this study were:
1.1 Demographics (Gender, age, education level)
1.2 Experience with technology (Use of Internet, use of communication technologies, and use of Internet specific technologies).
1.3 Personality traits (Ten Item Personality Inventory, TIPI by Gosling et al., 2003).

1.4 Concern for privacy (the Privacy Segmentation Index, PSI by Harris Interactive, 2002).

All of these various background measures were included in order to check for representativeness of the sample. Furthermore, it allowed the investigation of whether or not possible differences in interface evaluation between participants can be explained by differences in demographics.

Measure 2: Evaluation scenarios (see Appendix D2)

2.1 For each scenario separately:

- Extent of realism (on a scale from 1: not at all realistic, to 7: extremely realistic)
  "To what extent do you feel that the described situation could be realistic for you?"
  This question was included to check whether participants could imagine being involved in a situation as described. In case participants would not be able to relate to the situations described, one could argue that their usage of the privacy interfaces would be vacuous or that their ability to empathize with the actors of the scenario would be impeded.
- Extent of privacy concern (on a scale from 1: not at all concerned, to 7: extremely concerned)
  "Now imagine that you are in such a situation yourself. Please indicate to what extent you would be concerned about your privacy."
  This question was included to check whether participants did indeed perceive concerns about their privacy when being involved in a situation as described. If the situation would be rated as non-privacy-sensitive, then one would argue that the potential benefit of the system is absent. Besides, knowing how participants perceive the privacy threat helps to understand the impact of the system to protect their privacy.
- List two main concerns
  "Please describe concisely what would be your two main concerns when being in such a situation as described before."
  This open question was included to make an inventory of the (privacy) concerns participants may have in a situation as described, as well as to provide a potential explanation for preference of one interface over another.

2.2 For an environment encompassing all scenarios together (participants were asked to imagine a smart environment where all the technologies described in the scenarios - picture sharing, smart shopping, location tracking, personal movie record, and health monitoring - are available to them):

- Level of risk involved (on a scale from 1: strongly disagree to 7: strongly agree; Corritore et al., 2005). Participants had to indicate the extent to which they agree or disagree with seven statements. This measure is a relative measure contrary to many other measures used in the empirical studies reviewed in the section 4.1.2. It is a relative measure in the sense that it measures risk perception in relation to a particular application or system (the profile manager in this study). Many other measures for risk provide an indication of the tendency of people to perceive risk in general, more like a personal characteristic. Such a measure was considered less useful in this experiment, since the interest was in measuring changes in risk perception due to the use of different profile managers. Even though at this point a relative measure was not needed, it was needed at a later stage of the experiment (see risk measure 4.2). For ease of comparison the same relative measure was used in both stages.

Measure 3: Separate evaluation interfaces (see Appendix D3)

3.1 After first use

- Level of concern (on a scale from 1: very much less concerned than before, to 7: very much more concerned than before)
  "Please indicate for each interface to what extent you felt more or less concerned after the actual use of that interface compared to before."
  This question was included to see whether using each of the interfaces reduced or increased participants' concerns.

3.2 After second use

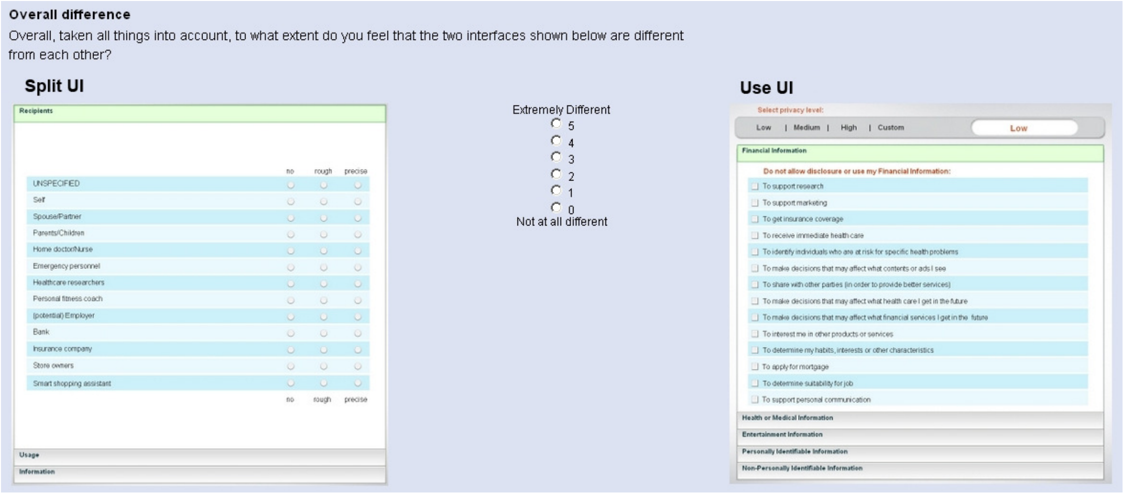
- Ease of use (on a scale from 1: extremely easy to 7: extremely difficult)
  "Please indicate for each of the interfaces to what extent you felt that it was easy or difficult to make the required settings with that interface."
  This question was included to measure participants' perceived complexity of each of the interfaces. A single measure was used in order to obtain some feedback of users about their experiences with the interfaces without burdening them.
- Comprehension (objective measure). Participants' settings with each interface were compared to the correct settings based on the task instructions. This measure was derived to see how complex performing the tasks with each of the interfaces actually were, and provides an indication of how successful participants were at obtaining the required settings with each interface.

Measure 4: Paired evaluation interfaces (see Appendix D4)

For the last part of the study participants were asked to evaluate interfaces in pairs. Participants compared two interfaces at a time on the basis of three different measures: overall difference, experience and acceptance measures, and qualitative comments. Each of these measures will be explained in more detail below.

4.1 Overall difference (see Figure 4.12; on a scale from 0: not at all different to 5: extremely different). This measure is also referred to as dissimilarity scaling (Martens, 2003), or (overall) dissimilarity judgment (Erickson, 2008; Donthu & Cherian, 1993). In dissimilarity scaling participants scale the dissimilarity or

Figure 4.12. Screenshot of question about overall difference



Overall difference

Overall, taken all things into account, to what extent do you feel that the two interfaces shown below are different from each other?

Split UI

Recipients

	no	rough	precise
UNSPECIFIED	○	○	○
Self	○	○	○
Spouse/Partner	○	○	○
Parents/Children	○	○	○
Home doctor/Nurse	○	○	○
Emergency personnel	○	○	○
Healthcare researchers	○	○	○
Personal fitness coach	○	○	○
(potential) Employer	○	○	○
Bank	○	○	○
Insurance company	○	○	○
Store owners	○	○	○
Smart shopping assistant	○	○	○
	no	rough	precise

Usage

Information

Extremely Different
○ 5
○ 4
○ 3
○ 2
○ 1
○ 0
Not at all different

Use UI

Select privacy level:

Low | Medium | High | Custom   Low

Financial Information

Do not allow disclosure or use my Financial Information:

- □ To support research
- □ To support marketing
- □ To get insurance coverage
- □ To receive immediate health care
- □ To identify individuals who are at risk for specific health problems
- □ To make decisions that may affect what contents or ads I see
- □ To share with other parties (in order to provide better services)
- □ To make decisions that may affect what health care I get in the future
- □ To make decisions that may affect what financial services I get in the future
- □ To interest me in other products or services
- □ To determine my habits, interests or other characteristics
- □ To apply for mortgage
- □ To determine suitability for job
- □ To support personal communication

Health or Medical Information

Entertainment Information

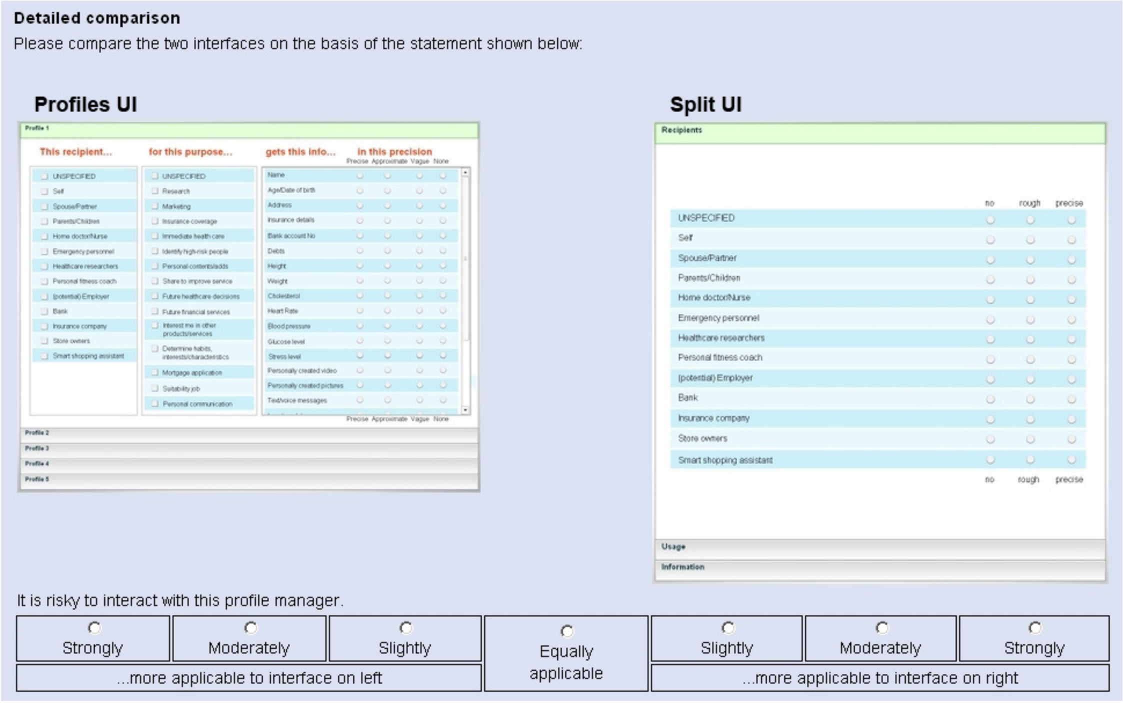
Personally Identifiable Information

Non-Personally Identifiable Information

difference between two objects. Any aspect that contributes to the dissimilarity can be taken into account (Martens, 2003). The overall difference measure is included since it provides information on whether or not the interfaces are perceived to be different from one another. Furthermore, it will allow investigation whether or not this overall difference is in accordance with the differences found by the five attributes described below. If the overall difference between two interfaces would be large, yet the difference between these models on the basis of the five attributes would be small, then this could be considered an indication that participants take other factors besides these five attributes into account.

4.2 Experience and acceptance measures, i.e. difference scaling (an example of a measure is shown in Figure 4.13; all measures are listed in Table 4.3). In difference scaling participants scale the difference between two stimuli with regard to a specific attribute (Martens, 2003). This is also referred to as difference judgments or comparison scaling (De Ridder, 2001). An advantage of rating two stimuli at a time is that it is expected to be more sensitive to differences between stimuli than designs with single stimuli evaluation. As Gabrielsen (2000) and Scheffé (1952) explain for difference scaling of preferences (i.e. paired comparison): if a participant may independently give two stimuli the same score in separate evaluations, he or she might still find a slight preference for one of them. Another advantage of difference scaling over scaling where individual stimuli are rated is that the latter is more easily influenced by contextual effects (De Ridder, 1996). The response to a stimulus depends not only on the stimulus itself but also on the other stimuli to be judged in a session (De Ridder, 1996).

Figure 4.13. Screenshot of question about attribute comparison



Detailed comparison

Please compare the two interfaces on the basis of the statement shown below:

Profiles UI

Profile 1

This recipient...	for this purpose...	gets this info...
□ UNSPECIFIED	□ UNSPECIFIED	Name
□ Self	□ Research	Age/Date of birth
□ Spouse/Partner	□ Marketing	Address
□ Parents/Children	□ Insurance coverage	Insurance details
□ Home doctor/Nurse	□ Immediate health care	Bank account No
□ Emergency personnel	□ Identify high-risk people	Debts
□ Healthcare researchers	□ Personal contents/adds	Height
□ Personal fitness coach	□ Share to improve service	Weight
□ (potential) Employer	□ Future healthcare decisions	Cholesterol
□ Bank	□ Future financial services	Heart Rate
□ Insurance company	□ Interest me in other products/services	Blood pressure
□ Store owners	□ Determine habits, interests/characteristics	Glucose level
□ Smart shopping assistant	□ Mortgage application	Stress level
	□ Suitability job	Personally created video
	□ Personal communication	Personally created pictures
		Text/voice messages

in this precision: Precise ○ Approximate ○ Vague ○ None ○

Profile 2

Profile 3

Profile 4

Profile 5

Split UI

Recipients

	no	rough	precise
UNSPECIFIED	○	○	○
Self	○	○	○
Spouse/Partner	○	○	○
Parents/Children	○	○	○
Home doctor/Nurse	○	○	○
Emergency personnel	○	○	○
Healthcare researchers	○	○	○
Personal fitness coach	○	○	○
(potential) Employer	○	○	○
Bank	○	○	○
Insurance company	○	○	○
Store owners	○	○	○
Smart shopping assistant	○	○	○
	no	rough	precise

Usage

Information

It is risky to interact with this profile manager.

○ Strongly	○ Moderately	○ Slightly	○ Equally applicable	○ Slightly	○ Moderately	○ Strongly
...more applicable to interface on left				...more applicable to interface on right		

Table 4.3. Experience & acceptance measures

Code	Description
Trust	
Tru1	I expect this profile manager will not take advantage of me.
Tru2	I believe this profile manager is trustworthy.
Tru3	I believe this profile manager will not act in a way that harms me.
Tru4	I trust this profile manager.
Risk	
Ris1	I feel vulnerable when I interact with this profile manager.
Ris2	I believe that there could be negative consequences from using this profile manager.
Ris3	I am taking a chance interacting with this profile manager.
Ris4	I feel it is unsafe to interact with this profile manager.
Ris5	I feel that the risks outweigh the benefits of using this profile manager.
Ris6	I feel I must be cautious when using this profile manager.
Ris7	It is risky to interact with this profile manager.
Usefulness	
Val1	Using this profile manager improves my performance to use personalized services while protecting my privacy.
Val2	Using this profile manager increases my productivity to use personalized services while protecting my privacy.
Val3	Using this profile manager enhances my effectiveness to use personalized services while protecting my privacy.
Val4	I find this profile manager to be useful to use personalized services while protecting my privacy.
Ease of use	
Eas1	Learning to operate this profile manager was easy for me.
Eas2	I found it easy to get this profile manager to do what I wanted it to do.
Eas3	I found it easy for me to become skillful at using this profile manager.
Eas4	I found this profile manager easy to use.
Intention to use	
Use1	Assuming I have access to this profile manager, I intend to use it.
Use2	Given that I have access to this profile manager, I predict that I would use it.
Use3	It is likely that I will use this profile manager in the near future.

All of the 8 background models described in the introduction contain some of the five attributes that need to be measured in this study. Most other models that include one or more of the concepts included in this study propose general measures for each concept, i.e. the measures do not refer to a particular application or interface, but they serve as an indication of the tendency of people to trust or perceive risk in general as a personal characteristic. Since the aim of this study is to compare users' perception of different interfaces for setting privacy preferences, these measures are less applicable.

Instead, the measures in this study are taken from Corritore et al. (2005) and from Lui and Jamieson (2003), who use relative measures depending on the application involved. The model by Suh and Han (2002) includes similar measures for some of the attributes. Originally these attributes were measured in a direct response design by 7-point Likert scales ranging from 1 (Strongly disagree) to 7 (Strongly agree). For the purpose of this study the scales have been adapted to allow difference scaling between the UIs on a scale from -3 (Strongly more applicable for interface on left) to +3 (Strongly more applicable for interface on right). A negative score indicates that the left hand interface was rated higher on a particular attribute, whereas a positive score indicates that the right hand interface was rated higher. For example a score of -2 for UI pair 1 (Profiles - Split) would indicate that the Profiles UI rated higher. The zero category can be used in case both interfaces are judged to have equal attribute strength. For all of the measures used, the items loaded on the construct represented in the original model.

The model evaluation will be performed on the paired data. This implies that the model will not predict an absolute intention to use of privacy interfaces, but instead the model will explain differences in intention to use between privacy interfaces by difference in risk, trust, usefulness and ease of use.

The included experience and acceptance measures were:

- Trust: as in Corritore et al. (2005; cronbach's alpha is 0.842), due to brevity and the focus on UIs (other sources provide more general trust measures). Similar items are included in the measure by Suh and Han (2002).
- Risk: as in Corritore et al. (2005; cronbach's alpha is 0.908), because it is based on clear statements which fit the context well.
- Usefulness: as in Lui and Jamieson (2003; composite reliability 0.891) because it fits the context well. It contains similar measures as proposed by Suh and Han (2002).
- Ease of use: as in Corritore et al. (2005; cronbach's alpha is 0.950) and Lui and Jamieson (2003; composite reliability 0.942) due to its brevity. The items used are also included in other measures, such as by Suh and Han (2002).
- Intention to use: as in Lui and Jamieson (2003; 0.925) due to its brevity and because it fits the context. Similar items are included in the Use measures by Suh and Han (2002).

4.3 Qualitative comments (open question).

Participants were asked for additional comments regarding each pair of interfaces.

4.3 RESULTS

4.3.1 Background measures

As indicated before, the background measures were only included to check for representativeness of the sample and to test whether or not possible differences in interface evaluation between participants can be explained by differences in their background. Therefore, only the main results for the background measures will be presented in this section, for more detailed results please refer to Appendix E.

In total 78 participants started and completed the study, of which 29 were female (37%), and 49 were male (63%). Participant ages ranged from 18 to 60 with an average age of 32. For 95% of the participants education level was between high school and a doctoral degree.

This means that the sample is more male and more educated than the general population (For the Dutch population in 2008, 49.4% is male and 50.6% is female; CBS, 2008. In this study 22% of the participants had high school education or less, compared to 69% for the labor force in Holland aged between 15 and 64; CBS, 2006). The fact that the sample is more male may lead to lower privacy concerns overall (Garbarino & Strahilevitz, 2004; Sheehan, 1999; GVU Center, 1998; Harris Interactive, 2002). The effect of education level on privacy concern is not univocal, some find that higher education levels increases privacy concern (Sheehan, 2002), while others find the opposite (Harris Interactive, 2002). However, in the sample of the current study it turned out that out of the 12 questions regarding concern (measure 2.1) and risk (measure 2.2) there were only a few cases where the male and more educated participants rated the concern or risk higher compared to the other participants.

Based on the experience with technology measures it could be concluded that the participants are experienced with and aware of the current technological landscape. Therefore, they will be able to appreciate the privacy concerns and information disclosure choices presented to them in this study.

Overall the sample of this study is not particularly skewed towards any specific personality trait if compared to the norm provided by Gosling et al. (2003). Compared to the Harris Interactive sample (Harris Interactive, 2002) the sample of this study contains more pragmatists and less fundamentalists. This could have led to fewer privacy concerns in the sample of this study. However, it turned out that the level of privacy concern based on the scenarios is not significantly different for fundamentalists and pragmatists.

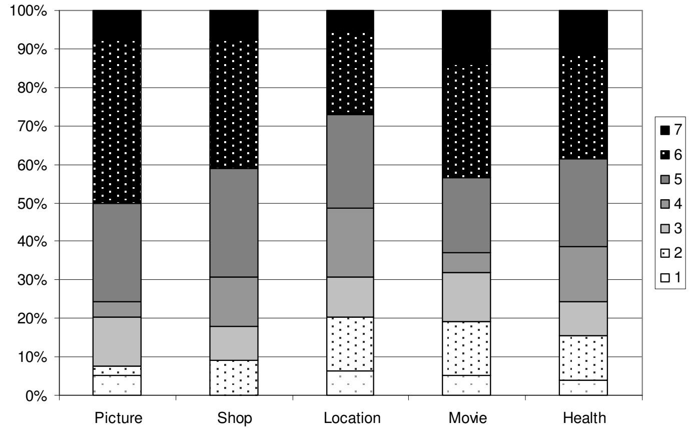
4.3.2 Evaluation scenarios

Realism of scenarios

Participants were asked to rate the level of realism on a scale from 1 (not at all realistic) to 7 (extremely realistic) of the situations regarding the first use of the interfaces. Most participants felt the situations described were quite realistic (see Figure 4.14). Median answer for all 5 situations is 5. So, it can be concluded that overall the scenarios were perceived to be realistic, and hence it may be assumed to have provided some sensible context of use to participants.

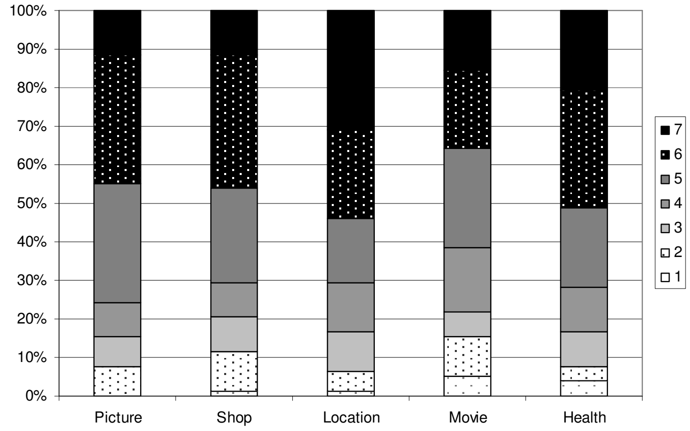
Many of the participants who indicated that the scenarios were not realistic to them explained that they did not appreciate the service, or that they wanted to be in control themselves and did not want to give away their control to some automated service. For example, one participant commented on the smart shopping scenario: "*I can think by myself what I want. I don't need a computer to tell me what things I should buy!*" Another commented on the movie recommender scenario: "*This movie and website record would not be desired by me to use, let alone used by others to gather information about me. I do not want to be bothered with thinking about if I want to hide movies/websites I saw.*" And yet another participant commented about the health monitoring scenario: "*I would prefer to be able to talk to my doctor instead of allowing something else to tell him how I feel.*" These comments do indicate acceptance problems for personalized services. However, even these users appreciate the privacy trade-offs involved and the technological feasibility of the scenarios. Even though the scenarios are not desirable to them, they can be considered realistic.

Figure 4.14. Extent of realism of scenarios



Note: Low scores represent absence or low levels of realism, high scores represent high levels of realism.

Figure 4.15. Extent of concern about privacy in such a situation



Note: Low scores represent absence or low levels of realism, high scores represent high levels of realism.

Extent of privacy concern

Participants were also asked to rate the level of concern about their privacy in a situation as described by each scenario on a scale from 1 (not at all concerned) to 7 (extremely concerned). The results are shown in Figure 4.15. Most participants indicated that they would be concerned about their privacy in situations such as those described by the scenarios. Median answer for the situations involving picture sharing, smart shopping and personal movie record is 5, for the other two 6, indicating a slightly higher concern for location tracking and health monitoring. Overall this shows that participants were indeed quite concerned about their privacy in the situations presented to them, and hence there was a convincing justification for them to manage their profile information.

Participants were asked to list their two main concerns about each situation. Only concerns (i.e. negative feelings) were taken into account, since participants were not

explicitly asked to mention positive impressions regarding the scenarios presented to them. Therefore, the comments do not imply absence of positive judgment.
For analysis of participants' comments open coding was used. This means that the categories emerge from the data itself (Strauss & Corbin, 1990). Over 950 concerns were mentioned by participants with regard to the 5 situations. On average 196 concerns were raised per situation. In total 32 categories of concerns were distinguished. Half of these concerns were mentioned by at least 10 participants in one of the situations (see Table 4.4). The other 16 concerns were mentioned by fewer than 10 participants per situation.

The four most frequently mentioned concerns (see Table 4.4) regard disclosure to certain recipients, control over the system, and general privacy issues. Concerns about the restriction of the disclosure to certain recipients (Recipient) were addressed 75 times for all situations together. For example one participant indicated: "*I would like to share my pictures only with the people I choose*" (scen1), and another: "*I want to be able to decide who can track me and who can't*" (scen3).

Even more frequently this restriction of the disclosure to certain recipients was mentioned in relation to the type of information to be disclosed (Recipient_Info), namely 115 times in total. Examples of such concerns are: "*Certain pictures may be really private, only for family and close friends, while other pictures I may want to share with colleagues etc.*" (scen1) and: "*I guess I would not want my kids to see that ;) Partner yes, but kids... I don't know why exactly, perhaps a different generation might misunderstand some things? And I think I would not share everything with my kids, some things are private or between me and my partner*" (scen4).

Control was mentioned 77 times, and privacy issues in 73 occasions. With regard to concerns about control one participant stated: "*I want to be 100% sure that I am the only one who can control these access rights*" (scen5), and another said: "*I'm not concerned, as long as I have the control over an advertisement system. I want the system to be reactive rather than pro-active and yelling at me*" (scen2). With regard to privacy concerns one participant indicated: "*I'm concerned about my privacy, the shopkeeper gets too much personal information about my food/living habits*" (scen2), and another said: "*If really every picture I take is automatically being shared, I would be much more worried about my privacy*" (scen1).

The concerns that were most frequently mentioned in this study do resemble a lot of concerns reported by Cranor (2004), such as unsolicited marketing (SPAM), a computer "figuring things out" about me (BigBrother), information revealed to other users of same computer, and unauthorized access to accounts (both: Others and Security).

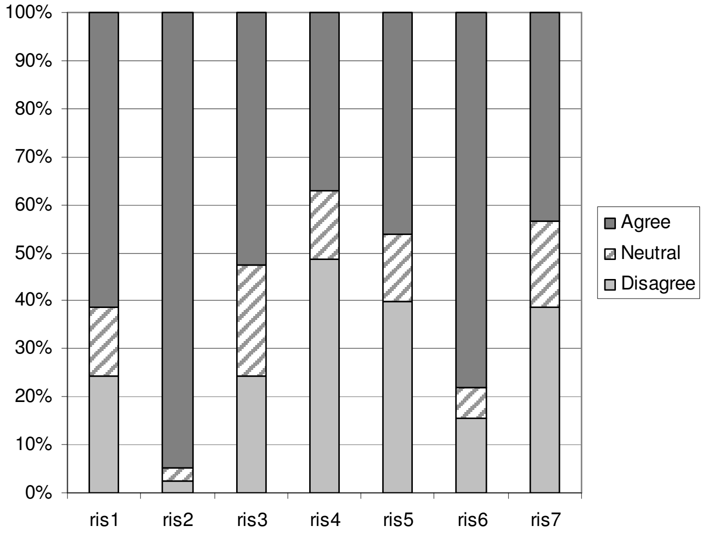
Overall, it is felt that the scenarios presented a credible and realistic level risk or concern for participants. The concerns mentioned by participants in this study do reflect concerns with regard to Ambient Intelligence in general: the feeling of always being monitored, general privacy and security issues and loss of control (see also potential downsides of Ambient Intelligence in section 1.1.3). Many of these concerns could be addressed by interfaces for privacy preferences, since a lot of concerns regard issues of control (wanting to restrict the flow of certain information to certain individuals, for certain purposes, or in specific circumstances).

Table 4.4. Most frequently mentioned concerns

		# of comments per situation					
		1	2	3	4	5	-
Code	Concerned about…	Picture	Shop	Location	Movie	Health	ALL
Recipient_Info	Wanting to restrict disclosure of certain information to certain recipients.	22	17	17	31	28	115
Control	Wanting to be in control of the system / data sharing. Disliking automatic disclosure, demanding a personal decision / choice / permission / approval.	26	10	14	14	13	77
Recipient	Wanting to restrict disclosure to certain recipients.	28	1	21	10	15	75
Privacy	Maintaining privacy, keeping things private/personal/to yourself. It is my business, not for anyone else to know.	18	16	12	12	15	73
Service disliked	Service is (partly) disliked/not appreciated.	7	4	13	17	28	69
Purpose	Allowing use of data only for certain purposes. Questioning what happens with the data?	13	18	8	8	19	66
Info type	Controlling info type (or being able to eliminate certain items within one info type from disclosure).	18	6	5	21	3	53
Spam	Being contacted / spammed / advertised with unwanted services/marketing.	1	41	0	2	2	46
OwnFreedom	Not feeling free/being limited. Being able to choose/decide yourself / being controlled by a system.	1	22	9	6	3	41
Others	Unwanted access of data by others.	21	11	4	2	2	40
Context	Availability of data outside original context/situation, wanting to share data depending on situation/context.	8	4	11	6	9	38
AlwaysOn	Having a system that constantly monitors what you're doing, not being able to / demanding possibility to switch off the system.	0	0	20	1	10	31
Security	Security issues with data stored / used by system.	4	5	2	8	10	29
StorageLocation	The storage location of the data.	12	0	1	4	0	17
BigBrother	Having the impression / feeling of constantly being watched / tracked / monitored.	0	3	10	2	0	15
ScopeService	Service is only perceived to be useful / interesting in certain contexts.	0	0	3	0	11	14
# frequent comments		179	158	150	144	168	799
Total # comments		215	192	201	171	188	967

Note: Concerns mentioned by at least 10 participants; Description for each concern and the number of times a concern is mentioned per situation.

Figure 4.16. Extent of agreement with various risks in an environment including all 5 scenarios



Note: Ris1: Would feel vulnerable, Ris2: Negative consequences, Ris3: Taking a chance, Ris4: Feel it is unsafe, Ris5: Risks outweigh benefits, Ris6: Must be cautious, Ris7: Would be risky.

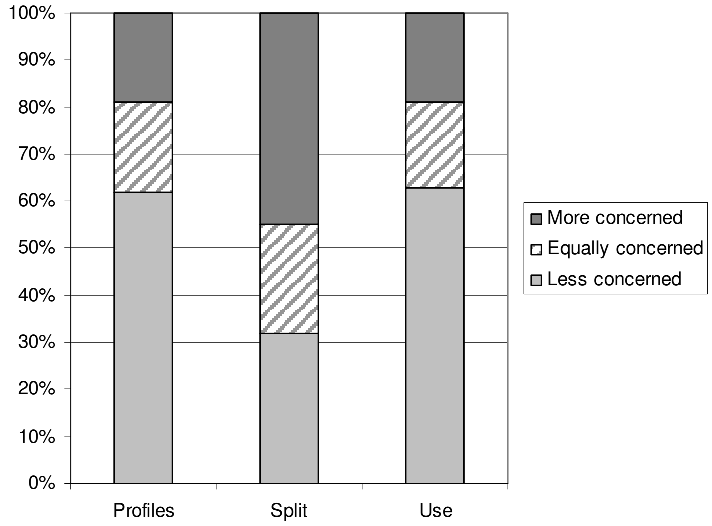
Participants were asked to imagine a smart environment encompassing all 5 scenario technologies of picture sharing, smart shopping, location tracking, personal movie record, and health monitoring together. For this overall environment participants were asked to rate the level of risk involved, by indicating the extent to which they agree or disagree with seven statements relating to risk on a scale from 1 (strongly disagree) to 7 (strongly agree) following Corritore et al. (2005). Figure 4.16 shows the results. Most participants would feel that they were somewhat vulnerable in such a situation (ris1, 30% rated 5), that there could be negative consequences (ris2, 41% rated 6), that they are taking a chance (ris3, 34% rated 5), that the risks outweigh the benefits (ris5, 22% rated 5), and that they must be cautious (ris6, 28% rated 5). However, most participants felt that such a situation is safe (ris4, 30% rated 3) and not risky (ris7, 27% rated 3). Thus, participants indeed perceived a sense of risk with regard to the scenarios presented to them.

4.3.3 Separate evaluation interfaces

Level of concern (after first use of interfaces)

Participants were asked to rate their level of concern after using the interfaces for the first time compared to their level of concern before use. The level of concern after using the Profiles or the Use UI was almost the same (see Figure 4.17). Over 60% of the participants indicated to feel less concerned after using one of these interfaces compared to before using them. Almost 20% of the participants indicated to feel more concerned after use of either the Profiles or Use UI. Concerns after using the Split UI were somewhat higher; only 32% of the participants indicated to feel less concerned and 45% indicated to feel more concerned then before.

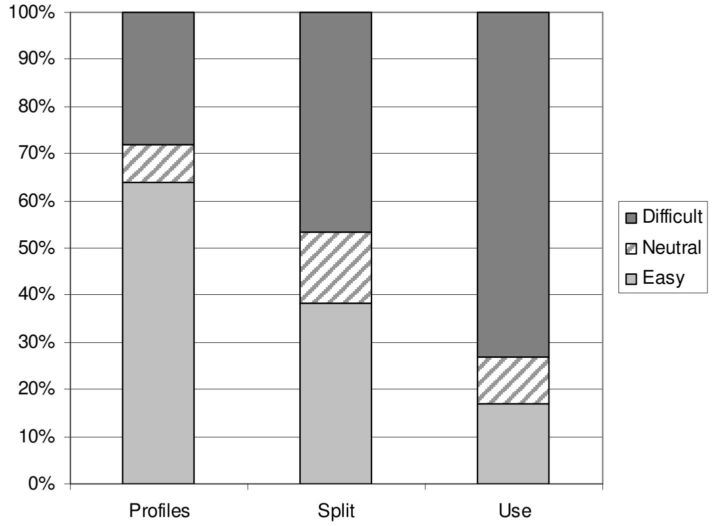
Figure 4.17. Level of concern compared to before use



Ease of use (after second use of interfaces)

Participants were asked to rate the difficulty of performing the task for second use with each of the interfaces. This time there was more difference between the evaluations of the three interfaces. The Profiles UI was considered easiest (2nd use was rated as easy by 64%, and difficult by 28%), the Use UI was considered most difficult (2nd use was rated as easy by only 17%, and difficult by 73%) and the Split UI was considered neither easy or difficult (easy by 38%, and difficult by 46%). See Figure 4.18.

Figure 4.18. Subjective complexity second use of interfaces



The recording of participants' use of the interfaces showed that participants did not correctly read the text provided by the interfaces. For example participants did not notice that in the Use UI situations of information disclosure need to be disallowed instead of allowed, and quite some participants did not notice the multiple sections provided by an interface. This caused participants to make assumptions about the interfaces without proper protection of their privacy. Despite the fact that the consequences of this careless behavior were not explicitly investigated in this study, it can be concluded that people may experience privacy violations in real situations due to improper settings of their privacy preferences as a result of careless reading.

4.3.4 Paired evaluation interfaces

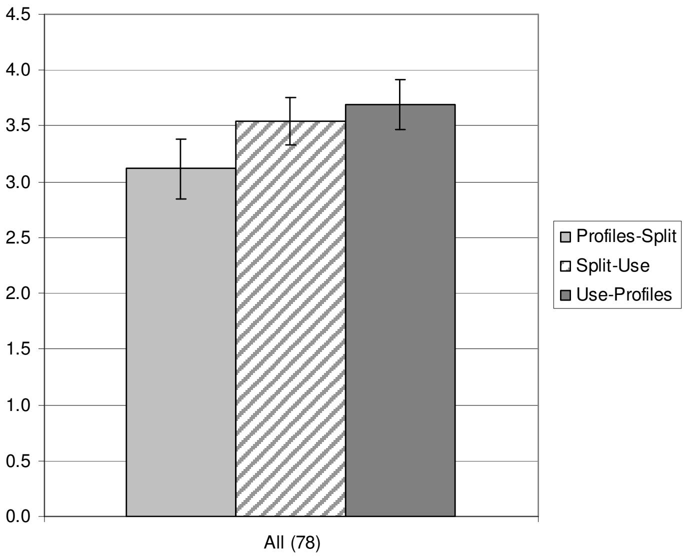
Overall difference

Participants were asked to rate the overall difference between two interfaces at a time on a scale from 0 (not at all different) to 5 (extremely different). An example of this question is shown in Figure 4.12 at page 116. Figure 4.19 shows the results of the overall difference between the interface pairs. The differences between the three pairs of interfaces are quite similar. The difference between the Profiles and the Split UI is on average rated 3.12. The difference between the Split UI and the Use UI is on average rated 3.54, and the difference between the Use and the Profiles UI is on average rated 3.69. Each of these is significantly different from 0 (p<0.0001), i.e. for all three pairs the interfaces are indeed perceived to be different from each other. Based on the overall difference it seems that the Profiles and Split UI are slightly more alike than the other interfaces are among each other.

Experience & acceptance measures

Participants were also asked to rate the extent to which each pair of interfaces differed from each other with regard to 5 specific attributes (based on 22 items, namely trust: 4 items; risk/concern: 7 items, usefulness: 4 items, ease of use: 4 items; and intention to

Figure 4.19. Overall difference between the three interface pairs for total sample

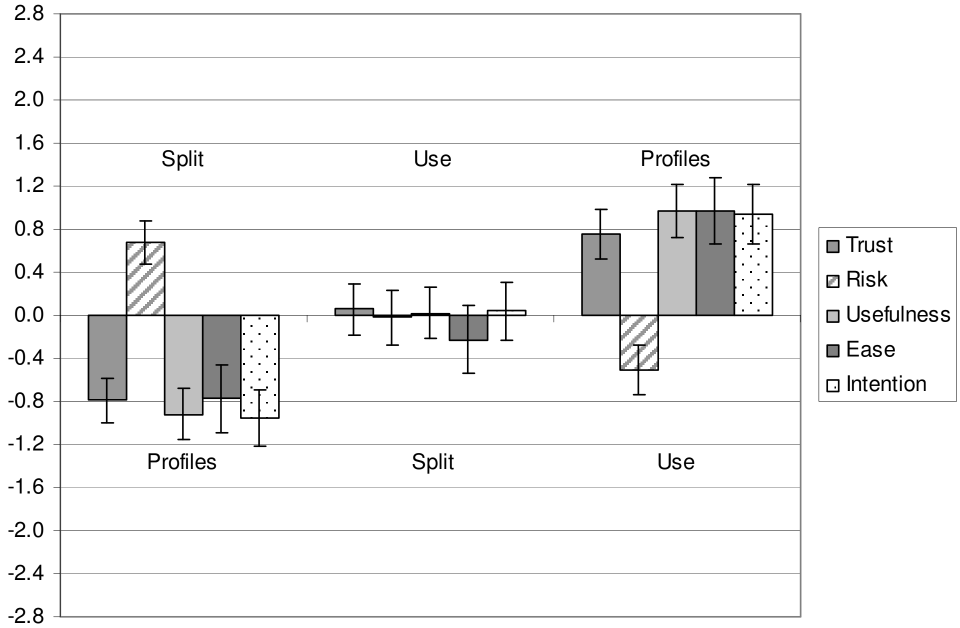


Note: Including 95% confidence interval.

use: 3 items). See also the section about measure 4.2. Participants could give a score ranging from -3 (strongly more applicable for interface on left), through 0 (equally applicable to both interfaces), to +3 (strongly more applicable for interface on right). In other words, negative scores indicate that the UI on the left is scoring higher on the specific attributes, whereas positive scores indicate that the UI on the right scores higher. Scores close to zero indicate that there is practically no difference between the two UIs with regards to the specific attribute. A screenshot of one of these attribute questions is shown in Figure 4.13 at page 117.

The average ratings of each interface pair on the five attributes are shown in Figure 4.20. This figure shows that the interfaces of UI pair 1 (Profiles-Split) and those of UI pair 3 (Use-Profiles) are considered to be quite different from one another. The Profiles UI scores higher on trust, usefulness, ease of use and intention to use in comparison to both the Split and Use UI. The interfaces of UI pair 2 (Split-Use) could not be distinguished from each other, except for the attribute ease of use, though this difference is not significant. The Split UI was rated slightly easier to use (negative score). The Split UI and Use UI score low on the features trust, usefulness, ease of use and intention to use, and high on risk in comparison to the Profiles UI. In the remainder of this chapter whenever the four features trust, usefulness, ease of use and intention to use are mentioned together the term desirable features will be used to enhance readability. This term was chosen for these four features since they were initially expected to relate positively to intention to use.

Figure 4.20. Average attribute rating of each interface pair for total sample



Note: Figure shows rating for the following pairs: Profiles-Split; Split-Use; Use-Profiles. Negative or positive scores indicate that the first or respectively the second interface of a pair is scoring higher on a particular attribute, in accordance with the interface labels in the graph (score max: +3; min: -3). Including 95% confidence interval.

This means that, overall, the Profiles UI was rated highly by participants, and that little difference was found between the Split UI and Use UI in terms of the attributes measured.

For the comparison of UI pair Profiles-Split (overall diff. 3.12) all attributes are significantly different from 0, meaning there is a difference between the Profiles and Split UI with regard to the five attributes trust, risk, usefulness, ease of use, and intention to use. For the comparison of UI pair Split-Use (overall diff. 3.54) none of the attributes are significantly different from 0, indicating that there is no difference between the Split and Use UI with regard to any of the five attributes. For the comparison of UI pair Use-Profiles (3.69) all attributes are significantly different from 0, indicating that there is a difference between the Use and Profiles UI with regard to the five attributes.

Alternative analysis and presentation

There is a possible alternative approach for the analysis and presentation of the paired evaluation of privacy interfaces to the one described before in this section. This alternative approach is based on a combination of Multi Dimensional Scaling (MDS) and multiple regression. This alternative analysis was performed as well, but the results are not presented in this chapter. Even though the two approaches may seem to provide different information, in principle the conclusions that can be drawn on the basis of both forms of analysis are the same. Therefore, the results of the alternative analysis are only presented for the total sample in Appendix E1.

Qualitative comments

Participants were finally asked for additional comments about each pair of interfaces to the extent they did not provide this information before. Only 8 participants chose to answer some questions in Dutch. These comments were translated into English.
Then open coding was used (Strauss & Corbin, 1990), meaning that the categories emerge from the data itself. Over 750 comments were provided by participants with regard to interfaces. Comments were split in negative, positive or neutral comments.

The presence of default settings was perceived differently by different participants. The most frequently mentioned comments (mentioned by more than 10 participants for at least one interface) are listed in Table 4.5. The first two columns show the explanations for the comments, and the columns to the right show the amount of participants mentioning a particular feature (or the absence of it) as being positive or negative for each specific interface. These frequencies are given as an indication of the salience of this feature to users, since they reported these comments as answers to an open question.
For example, the first row "availability default" indicates that 7 participants missed having default settings in the Profiles UI (e.g. "*there is no way to have an easy default choice*", or "*you might want to give some presets like available in the Use UI interface*", whereas for the Use UI 13 participants felt that the availability of default settings was a good feature (e.g. "*makes it easier to set everything to a high privacy level using a single mouse click*") and 3 participants felt it was not (e.g. "*If you use high level it automatically gives high level in every situation. It is a lot of work to put it in your own personal style*").

Overall, the Profiles UI was considered to be the only clear interface. The second row of Table 4.5, labeled "Clear", shows that the Profiles UI was perceived as clear by most

Table 4.5. Most frequently mentioned comments

	Profiles		Split		Use		Total	
Code Comment regarding	N	P	N	P	N	P	N	P
Availability default								
Availability of presets	7	0	0	0	3	13	10	13
Clear								
Negative: Confusing, unclear, messy, vague. Positive: Clear, orderly, clean, transparent, straightforward, obvious	2	13	15	5	20	4	37	22
Combinations								
Ability to make different combinations dependent on recipient / purpose / information	4	25	18	2	7	4	29	31
Consequences settings								
Knowing how settings will be interpreted	14	6	23	1	14	5	51	12
Easy to use								
Easy (to use / handle / choose)	2	23	2	25	5	10	9	58
Easy to understand / learn								
Easy to understand/learn (use at first)	4	4	11	1	11	0	26	5
Foolproof								
Easily make mistakes/careful not to make mistakes	1	0	8	1	8	0	17	1
General								
General expression about appreciation. In case positive: Like, good / better, handy, nice, prefer / my choice	0	32	7	9	10	9	17	50
Meaning elements								
Meaning of some UI elements unclear	4	0	4	0	15	0	23	0
Overview								
Overview, good view, one screen, see everything	2	24	8	0	6	4	16	28
Possibilities								
Number of options, functions, possibilities (profiles), extent of freedom	9	13	7	3	23	7	39	23
Precision								
Precision, detail	0	9	4	1	2	3	6	13
Safety								
Negative: Concerns, uncertainty. Positive: Safety, security, protection	1	2	3	0	8	8	12	10
Specificity								
Specificity, being able to specify answers / choices	1	10	7	0	4	1	12	11
Speed								
Amount of work, time, settings needed	22	1	0	6	2	6	24	13
# frequent comments	73	162	117	54	138	74	328	290
% frequent comments	31.1	68.9	68.4	31.6	65.1	34.9	53.1	46.9
Tot # freq. comments	235		171		212		618	
Total # comments	283		218		256		757	

Note: Description and number of times mentioned per interface. N: negative comment; P: positive comment.

participants (14/20; e.g. "*the interface is set up clearly*", or "*very transparent*"), whereas the other two UIs were regarded as confusing by most participants (15/20, 20/24; e.g. for Use UI: "*really vague*" or "*Not very clear. Confusing*" and for Split: "*Not clear how 'Recipients', 'Usage' and 'Information' are linked to each other*", or "*kind of confusing*").

The ability to make combinations based on recipient, purpose of use and type of information was appreciated for the Profiles UI (25/29; e.g. "*you can make profiles for each type of information, or for each recipient*"), and disliked for the Split UI (18/20; e.g. "*Different combinations depending on recipient not possible. That is not so convenient.*"). The way the Profiles UI allowed one to specify combinations, i.e. in different profiles, seemed to be appreciated.

For all three interfaces participants were negative about their understanding or comprehension of what consequences their settings would have (51/63; e.g. "*I am worried that I don't actually know how my information is used*" regarding Split UI). Participants felt that all three interfaces were quite easy to use, though the Use UI scored most negative comments on this point (5/15; e.g. "*hardest one to use*"). The Split and Use UI were mainly rated as difficult to understand or start using and also prone to errors, whereas for the Profiles UI these comments were balanced.

In general only appreciation was mentioned about the Profiles UI (32), whereas for the Split and Use UI an equal amount of positive and negative comments were made with regard to general appreciation.

The vagueness of some UI elements was mentioned as a negative feature for all UIs, though most comments were made about the Use UI (15 compared to 4 for the other UIs; e.g. "*not clear, because of the LOW MEDIUM HIGH and CUSTOM*" or "*unclear to me under which heading all the different types of information would fall*"). Based on the amount of comments made, the overview provided by each interface was best for the Profiles UI (24/26), somewhat neutral for the Use UI (4/10) and weak for the Split UI (0/8).

The amount of possibilities, such as the number of options or functions and the extent of freedom provided, was rated very low for the Use UI (23/30). The Profiles UI was indicated to be most precise and specific. Safety was mainly mentioned as an issue for the Use UI, but both in the positive and negative sense. Finally, time and effort it may take to set up the Profiles UI was mentioned as a negative feature.

Per interface this gives the following impression. The Profiles UI was generally appreciated, among other things because it was considered to be a clear interface, with the best overview, and most precise and specific, and it allowed people to make combinations between recipient, purpose of use and type of information (it is the only interface where combinations are directly visible to users). However, participants were somewhat less enthusiastic about the Profiles UI because it did not have any default settings such as the Use UI, and participants were aware that it may take a lot of time and effort to fully set the interface. Note that the conceptual model supported by this user interface does not prohibit having some default settings to guide users. So, in practice one could expect that a redesigned interface including defaults would be the most appropriate one for specifying privacy preferences.

The Use UI and the Split UI were both considered to be confusing, difficult to understand or start using, prone to errors and the general appreciation for these interfaces was neutral. Furthermore, the Use UI was considered hard to use and many comments were made about the unclear meaning of some UI elements. Its overview was considered to be mediocre and the amount of possibilities were perceived to be limited. However, the interface was appreciated for the availability of default settings. It should be noted that most privacy settings using current browsers for the Internet use one or another adaptation of the Use UI. The results of this experiment suggest an interesting opportunity for improvement in prevalent contemporary Internet browsers.

Besides comments made with regard to both the Use UI and the Split UI, specific comments for the Split UI were its poor overview, and participants indicated to miss or dislike its ability to make combinations between recipient, purpose of use and type of information.

4.4 CLUSTER ANALYSIS

4.4.1 Approach

As noted earlier, it is interesting to see if distinctions can be made among participants with respect to their evaluation of the three interfaces. Different cluster analysis techniques can be used to distinguish groups of participants with similar answering patterns. This study aimed to find groups of participants who rated the pairs of interfaces in a similar fashion yet different from other participants. The cluster analysis is based on the overall difference score plus the 22 attribute items for each of the 3 interface pairs (see Table 4.3). This means that in total 69 scores will be used for the cluster analysis.

Except for slight variations, similar results were obtained after using multiple techniques for cluster analysis. This confirmed the existence of fairly stable groups of participants regarding their evaluation of the three interface pairs. Before performing further analysis of the identified groups of participants one single cluster analysis technique was chosen. The rationale behind this chosen technique is described below.

In this case a hierarchical clustering based on Ward's method and the Squared Euclidean distance between cases was applied. Among the agglomerative hierarchical clustering methods Ward's method is most commonly used (Everitt, 1993). Ward's method tries to minimize the loss associated with each grouping of cases. Loss is defined by the error sum of squares (ESS). In the first step of the clustering process, each case is in its own cluster and the ESS is 0 (Aldenderfer & Blashfield, 1985). Then, union of each possible pair of clusters is considered, and the two clusters whose fusion will lead to a minimum increase of ESS will be combined (Everitt, 1993). Squared Euclidean distances are commonly used with Ward's method (SPSS, 2005).

The number of clusters can be determined by looking at the dendrogram. This is a graph, resulting from the cluster analysis, displaying the distances between clusters. It provides information on the cohesiveness of the clusters formed. The number of clusters can be reduced by merging clusters that are close together. Whenever there is a big distance between two consecutive groups of clusters, then this indicates the appropriate number of clusters. In this case a solution based on 4 clusters was chosen (see dendrogram in Appendix E1). The fourth cluster turned out to be a heterogeneous cluster. Therefore, the results for this cluster are not presented in the main text of this chapter, but can be found in Appendix E2.

Table 4.6. One-way analysis of variance for variable scores between cluster

		SS	df	MS	F	Sig.
ris3_P-S	Between Groups	6.939208	3	2.3131	1.3251	0.2727
	Within Groups	129.1762	74	1.7456		
ris5_P-S	Between Groups	10.72229	3	3.5741	1.9053	0.1361
	Within Groups	138.8162	74	1.8759		
ris3_S-U	Between Groups	3.870664	3	1.2902	0.8897	0.4506
	Within Groups	107.3088	74	1.4501		
ris5_S-U	Between Groups	9.379148	3	3.1264	1.8509	0.1454
	Within Groups	124.9926	74	1.6891		
ris3_U-P	Between Groups	3.042232	3	1.0141	0.5374	0.6581
	Within Groups	139.6373	74	1.8870		
ris5_U-P	Between Groups	5.52184	3	1.8406	0.8124	0.4910
	Within Groups	167.6576	74	2.2656		
dif_S-U	Between Groups	1.73687	3	0.5790	0.6526	0.5838
	Within Groups	65.64775	74	0.8871		
dif_U-P	Between Groups	3.539698	3	1.1799	1.1630	0.3297
	Within Groups	75.07569	74	1.0145		

To see whether or not there is any evidence that the clusters indeed are different with regard to some of the measured attributes a one-way analysis of variance was performed on the 69 variables used in the cluster analysis. With regard to the following 8 variables the clusters do not differ from each other (see also Table 4.6):

- 2 difference scores (for the pairs Split-Use & Use-Profiles);
- 2 risk items (ris3 and ris5 for all three pairs).

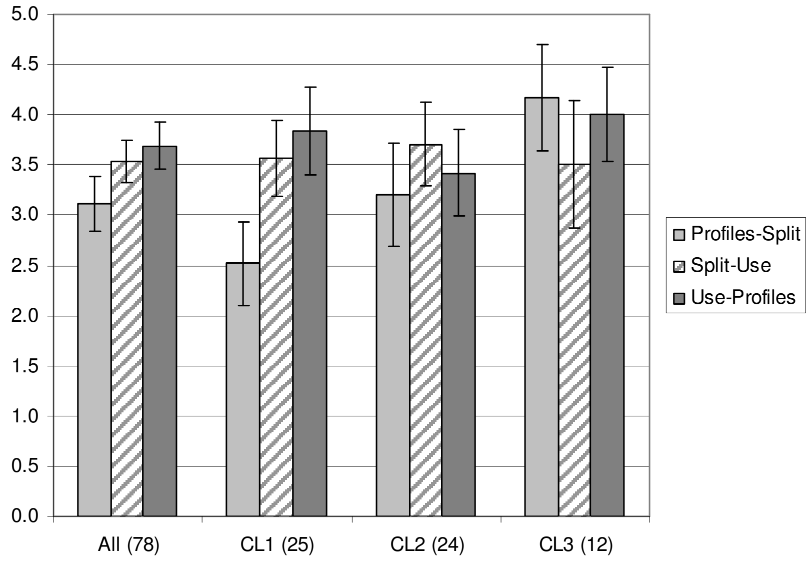
For the remaining 61 variables there is evidence that the four cluster means are not equal (i.e. the mean of at least one cluster is different from another cluster).

In Figure 4.21 the difference scores for the three interface pairs are shown for the whole sample and for the distinguished clusters. The answering patterns for the overall perceived differences between the three interface pairs are similar for cluster 1 and the total sample of participants.

For cluster 1 the overall difference between the Profiles UI and the Split UI is considered to be much smaller (2.52) compared to the difference between the other two interface pairs (3.56 and 3.84). Apparently, for this cluster the Use UI is perceived to be least similar to the other two interfaces.

For the remaining clusters there is hardly any variation in overall difference between the three interface pairs. Participants of cluster 2 on the other hand find the overall difference between the three pairs fairly similar, yet they perceive a somewhat larger difference between the Split UI and the Use UI (3.71 compared to 3.21 and 3.42). On the contrary, participants of cluster 3 perceive the overall difference between this particular pair of interfaces (Split UI and the Use UI) to be smallest (3.50 compared to 4.00 and 4.17).

Figure 4.21. Overall difference between interface pairs for total sample and separate clusters



Note: Including 95% confidence interval. All = Total sample. CL = Cluster. The number in parentheses shows the number of participants in each group.

4.4.2 Experience and acceptance measures per cluster

For the first three clusters a graph will be presented showing the average scores for the five attributes trust, risk, usefulness, ease of use and intention to use. These graphs show the extent to which a particular attribute was rated to be more or less applicable to a particular interface in comparison to one of the other interfaces. As will become clear, these clusters or groups of participants are very different from each other in terms of the interface being 'preferred', in terms of relatively high scores on intention to use. The results for the fourth cluster can be found in Appendix E2.

Cluster 1

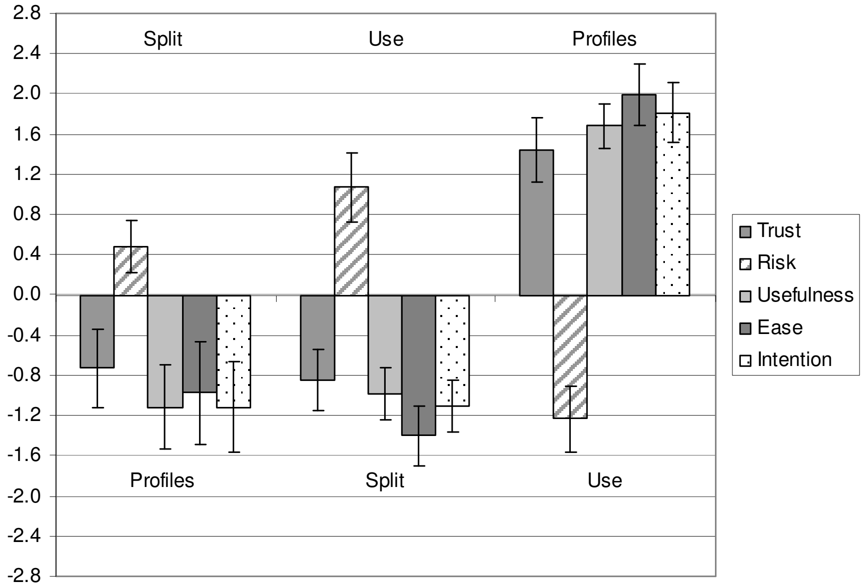
The first cluster (see Figure 4.22), consisting of 25 participants, perceives the differences between the interfaces in terms of the five attributes measured to be quite large. This cluster has a quite strong positive opinion about the Profiles UI (scoring higher on desirable attributes and lower on risk in comparison to both other interfaces). The Use UI is quite strongly disliked (low scores on desirable attributes and high score on risk in comparison to both other interfaces). The Split UI is perceived to be in between these two extremes (high score on risk when compared to Profiles UI, but low when compared to Use UI and vice versa for desirable attributes).

For this first cluster all paired comparison scores are significantly different from zero, indicating that participants perceived the pairs of interfaces to be different on the five attributes trust, risk, usefulness, ease of use and intention to use.

Cluster 2

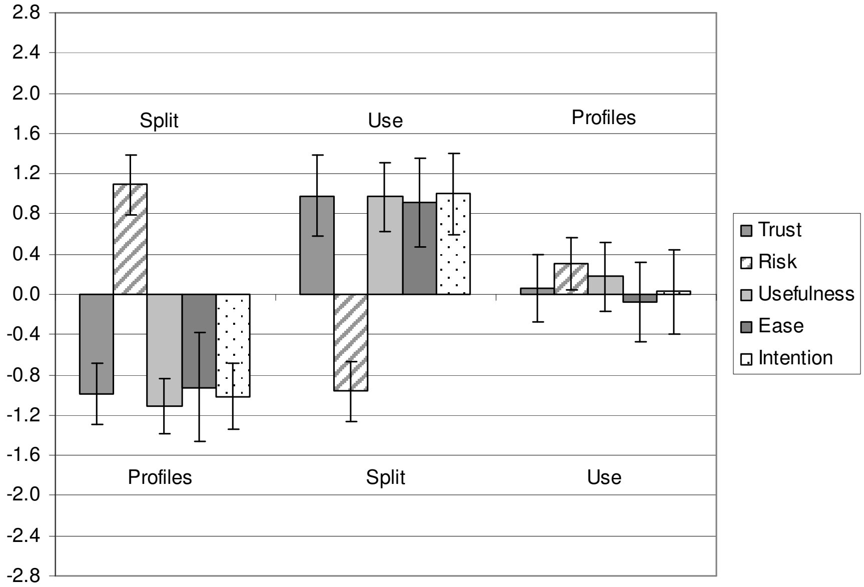
The second cluster (see Figure 4.23) consists of 24 participants who perceive small differences between the interfaces in terms of the five attributes. Both the Profiles UI and

Figure 4.22. Relative attribute rating of each interface pair for Cluster 1



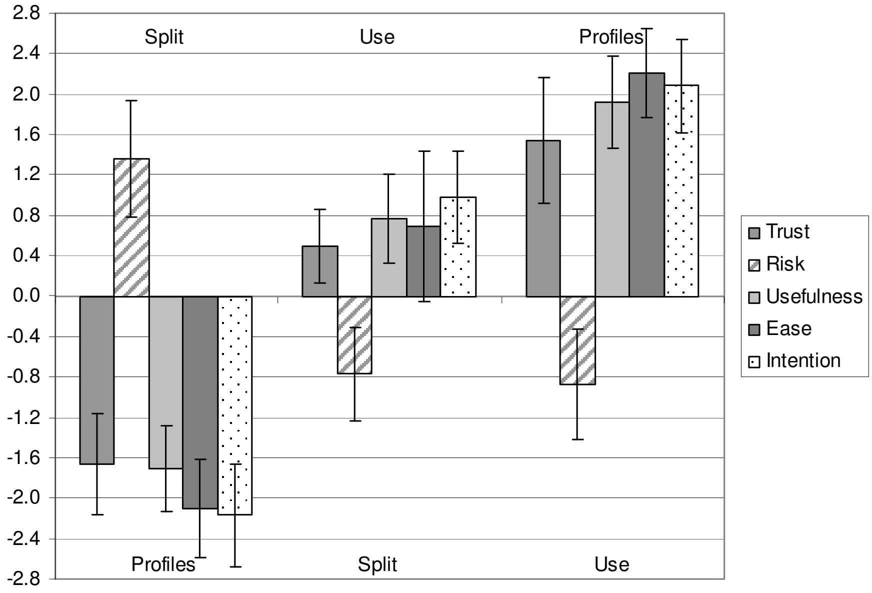
Note: n=25. Figure shows rating for the following pairs: Profiles-Split; Split-Use; Use-Profiles. Negative or positive scores indicate that the first or respectively the second interface of a pair is scoring higher on a particular attribute, in accordance with the interface labels in the graph (score max: +3; min: -3). Including 95% confidence interval. Quite strong preference Profiles UI & quite strong dislike Use UI.

Figure 4.23. Relative attribute rating of each interface pair for Cluster 2



Note: n=24. Figure shows rating for the following pairs: Profiles-Split; Split-Use; Use-Profiles. Negative or positive scores indicate that the first or respectively the second interface of a pair is scoring higher on a particular attribute, in accordance with the interface labels in the graph (score max: +3; min: -3). Including 95% confidence interval. About equal preference Profiles UI & Use UI, dislike Split UI.

Figure 4.24. Relative attribute rating of each interface pair for Cluster 3



Note: n=12. Figure shows rating for the following pairs: Profiles-Split; Split-Use; Use-Profiles. Negative or positive scores indicate that the first or respectively the second interface of a pair is scoring higher on a particular attribute, in accordance with the interface labels in the graph (score max: +3; min: -3). Including 95% confidence interval. Strong preference Profiles UI, strong dislike Split UI, dislike Use UI.

Use UI are positively perceived (high scores on desirable attributes; and low score on risk), whereas the Split UI is negatively perceived in comparison to the other interfaces (low scores on desirable attributes and high score on risk).

For this cluster all paired comparison scores between the pair of the Profiles UI and Split UI and the pair of the Split UI and the Use UI are significantly different from zero. The differences between the Profiles UI and the Use UI are not significantly different from zero except for risk. This is visible in Figure 4.23 as well.

Cluster 3

The third cluster (see Figure 4.24) consists of only 12 participants. This group of participants perceives the largest difference between the three interfaces in terms of the five attributes measured. The Profiles UI is very strongly preferred (high scores on desirable attributes and low score on risk), the Split UI is strongly disliked (low scores on desirable attributes and high score on risk), and the Use UI is somewhere in between (It scores higher on risk when compared to Profiles UI, but lower when compared to Split UI, and vice versa for desirable attributes).

For this cluster all paired comparison scores are significantly different from zero, except ease of use for the comparison between the Split UI and the Use UI. This indicates that participants perceived the pairs of interfaces to be different.

4.4.3 Remaining measures per clusters

This section will provide an overview of the main differences between the clusters (see also (Table 4.7). Please note that each cluster description is relative and should therefore be interpreted in comparison to those of the other clusters. More information regarding the differences between the clusters can be found in Appendix E.

Cluster 1 is fairly young (30.9 years on average), is balanced with respect to gender (48% females), has a medium education level in comparison to the other clusters, uses somewhat outdated communication technologies, but has relatively high experience on the Internet.
The participants of this cluster consider themselves as not very conscientious and based on the PSI they have a neutral privacy attitude. They raised concerns related to privacy, recipient and control. In comparison to other clusters particularly privacy and security seem to be important. This cluster values an interface that is (initially) ease to use and that provide a lot of options.

Cluster 2 is fairly young (29.2 years on average), has few females (29%), and is highly educated in comparison to the other clusters. This cluster is a low user of communication technologies and has relatively short experience on the Internet. The participants of this cluster rate themselves as slightly introvert. Based on the PSI Index they have a quite neutral attitude with regard to privacy. Concerns frequently raised by this cluster are service disliked, recipient, and control. In comparison with other clusters specifically the downsides of services are mentioned. This second cluster values to have an interface with a lot of options and a quick/fast interface as well.

Table 4.7. Summary of differences between the clusters

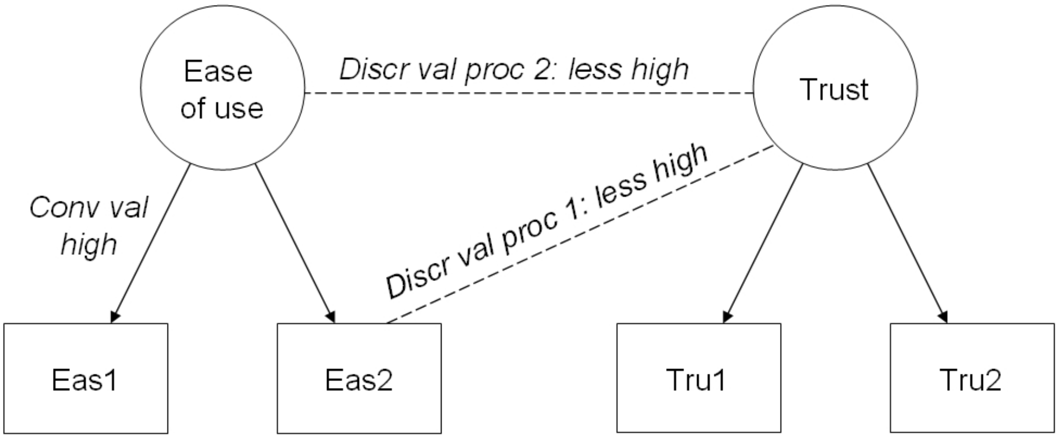
	CL1	CL2	CL3
Age	Low	Low	High
Proportion females	High	Low	High
Education level	Intermediate	High	Intermediate
Internet experience (yrs)	High	Low	High
Personality	Least Conscientious	Least Extravert	Most Conscientious
Privacy concern (PSI)	Intermediate	Intermediate	High
Realism & Concern scenarios	Intermediate	Intermediate	High
Concern & Difficulty UIs	Low: Profiles	High: Split	Low: Profiles
Main concerns	Privacy & Security	Downsides of services	Purpose of use Own freedom
Evaluation Profiles UI	Positive	Positive	Positive
Evaluation Use UI	Negative	Positive	Negative
Evaluation Split UI	Neutral	Negative	Negative
Main characteristics	Easy to use Options	Combinations Quick to set interface	Easy to use Clarity Control/Safety Level of Detail

In comparison to the other clusters, cluster 3 is older (37.3 years on average) and consists of quite some females (42%). The education level of this cluster is medium in comparison to other clusters. This cluster is a high user of fax, cell phone and to some extent voice mail in comparison to the other clusters. Most participants in this cluster have a long experience with the Internet. They consider themselves to be somewhat conscientious and are most concerned about privacy based on the PSI index. This cluster particularly raised concerns about purpose, service disliked and control. In comparison to other clusters purpose and own freedom are important. This clusters rated the scenarios as more concerning and realistic than the other clusters. For this cluster an interface that is easy to use and clear is important, as well as control/safety and the level of detail available.

4.5 MODEL EVALUATION

In section 4.1.2 the PI model for the acceptance of privacy interfaces was introduced. In this section the relations between the various factors and intention to use are explored in more detail. The relations of the proposed PI model were investigated using the Partial Least Squares (PLS) approach (with PLS-Graph version 3.0). Only the relation between each of the four factors trust, risk, ease of use, and usefulness with intention to use was investigated, since the aim was to study their relative importance in explaining intention to use. PLS performs a Confirmatory Factor Analysis (CFA) as opposed to an Exploratory Factor Analysis. In a CFA the pattern of loadings of the indicators on the latent variables is specified explicitly in a model. Then, the fit of this model is examined to determine factorial validity, in other words, whether the patterns of loadings of the measurement items correspond to the theoretically assumed factors (Gefen & Straub, 2005).

Figure 4.25. Schematic overview for assessment of model validity



Note: Convergent validity is obtained when each of the attribute items loads significantly on its latent construct (i.e. Eas1 and Eas2 should load significantly on “ease of use”). Procedure 1 to examine discriminant validity requires that attribute items load highly on their theoretically assigned factor and not highly on other factors (i.e. item eas1 should load higher on “ease of use” than on “trust”). Procedure 2 to examine discriminant validity requires an AVE analysis (the correlation of the construct with its attribute items should be larger than its correlation with the other constructs, (i.e. the correlation of “ease of use” with the item eas1 and eas2 should be higher than its correlation with “trust”).

First of all, convergent validity needs to be examined. Convergent validity occurs when items aimed to reflect one construct converge (or show significant high correlations with one another), particularly when compared to the convergence of items relevant to other constructs (Straub et al., 2004). Convergent validity is obtained when each of the attribute items loads significantly on its latent construct (see Figure 4.25). In other words, the t-value of the relationships between constructs and their indicators (Outer Model Loadings) should be above 1.96. The model contained 22 items and 5 constructs.

The data set consisted of 234 cases (78 participants times 3 interfaces). For one risk item (ris3), the t-value of the Outer Model Loadings was not above 1.96, so it was decided to drop this item from further analysis. Once this item was removed convergent validity was obtained, as all t-values for the Outer Model Loadings were above 1.96 (see Table 4.8).

Table 4.8 shows that the means of all responses are close to neutral (i.e. zero). Standard deviations for all responses are in the range 1.22 to 1.78 indicating that there were no problems with floor or ceiling effects. All indicator loadings were significant (p<.01). The t-statistic of the loading as listed in Table 4.8 was generated from the Bootstrap re-sampling procedure performed on the data set. In PLS information about

Table 4.8. Descriptive statistics and psychometric properties of measurement scales

		Mean	Standard Deviation	Weight	Loading	t-statistic Loading
Trust	tru1	0.043	1.211	0.2199	0.7758	14.8263
	tru2	0.004	1.394	0.3050	0.9260	87.1061
	tru3	0.000	1.411	0.2883	0.9031	48.6128
	tru4	-0.017	1.374	0.3157	0.9076	80.0275
Risk	ris1	0.137	1.447	0.1928	0.8520	23.7482
	ris2	0.004	1.487	0.2181	0.8964	49.8088
	ris4	0.000	1.550	0.2308	0.9273	91.1712
	ris5	0.021	1.403	0.0297	0.3014	2.7004
	ris6	0.103	1.740	0.2242	0.9316	106.6758
	ris7	0.064	1.542	0.2279	0.9145	49.9896
Usefulness	val1	-0.030	1.379	0.2593	0.8742	24.5574
	val2	0.021	1.372	0.2755	0.9226	69.7603
	val3	0.068	1.501	0.2886	0.9214	102.9716
	val4	0.043	1.607	0.2822	0.8971	50.5648
Ease	eas1	-0.043	1.599	0.2498	0.9264	63.7291
	eas2	-0.017	1.728	0.2946	0.9080	55.2851
	eas3	0.060	1.609	0.2700	0.9302	93.3813
	eas4	-0.043	1.774	0.2672	0.9355	88.418
Intention	use1	0.026	1.420	0.3554	0.9647	210.8284
	use2	-0.004	1.521	0.3509	0.9620	190.1102
	use3	0.009	1.517	0.3386	0.9441	97.4531

Note: Each measurement item is explained by the linear regression of its latent construct and its measurement error.

the variability of the parameter estimates and their significance has to be generated by means of re-sampling procedures. Bootstrapping is superior to the other two re-sampling procedures: blindfolding and jackknifing for deriving valid standard errors or t-values. The bootstrap procedure approximates the sampling distribution of an estimator by re-sampling with replacement from the original sample (Temme et al., 2006). All the loadings (except ris5) are well above 0.70 (as suggested by Chin, 1998).

Then discriminant validity needs to be examined. Discriminant validity occurs when each attribute item correlates weakly with all other constructs except for the one to which it is theoretically associated (Gefen & Straub, 2005). Discriminant validity can be checked by two different procedures. First of all the correlation of the latent variable scores with the original attribute items needs to show a pattern of loadings in which the attribute items load highly on their theoretically assigned factor and not highly on other factors (Gefen & Straub, 2005). Thus item *eas1* should load higher on “ease of use” than for example on “trust” (see schema in Figure 4.25). The data meets discriminant validity in the sense of this first procedure (see Table 4.9). Even though exact thresholds have not yet been defined in related literature, Gefen and Straub (2005) suggest that all the loadings of the attribute items on their assigned latent variables should be an order of a magnitude larger than any other loading (i.e. a difference larger than .10). The data meets this criterion as well except for the 4 cells in Table 4.9 marked with an asterisk.

Table 4.9. Correlation table of latent variable scores with the original attribute items

	Trust	Risk	Usefulness	Ease	Intention
tru1	**0.7759**	-0.5781	0.5429	0.4691	0.5510
tru2	**0.9260**	-0.7422	0.7917	0.6296	0.7644
tru3	**0.9031**	-0.7590	0.7570	0.6042	0.7226
tru4	**0.9076**	-0.7671	0.8019	0.7020	0.7912
ris1	-0.6606	**0.8520**	-0.6483	-0.5304	-0.5964
ris2	-0.7502	**0.8964**	-0.7125	-0.5891	-0.6746
ris4	-0.7829	**0.9273**	-0.7585	-0.6341	-0.7138
ris5	-0.1865	**0.3014**	-0.1687	-0.0594	-0.0918
ris6	-0.7441	**0.9316**	-0.7543	-0.6728	-0.6933
ris7	-0.7480	**0.9145**	-0.7371	-0.6377	-0.7047
val1	0.7088	-0.6737	**0.8742**	0.6679	0.7488
val2	0.7493	-0.7353	**0.9226**	0.7238	0.7955
val3	0.7941	-0.7465	**0.9214**	0.7395	0.8334*
val4	0.7540	-0.7255	**0.8971**	0.7029	0.8150*
eas1	0.5863	-0.5518	0.6507	**0.9264**	0.6855
eas2	0.7053	-0.7201	0.8021	**0.9080**	0.8084*
eas3	0.6560	-0.6329	0.7170	**0.9302**	0.7407
eas4	0.5976	-0.5769	0.7185	**0.9355**	0.7330
use1	0.7897	-0.7285	0.8649*	0.7855	**0.9647**
use2	0.7799	-0.7239	0.8555	0.7726	**0.9620**
use3	0.7626	-0.6875	0.8164	0.7532	**0.9441**

Note: * Does not meet discriminant validity criterion suggested by Gefen & Straub (2005).

Table 4.10. Correlations between constructs and square root of AVE

	Trust	Risk	Usefulness	Ease	Intention
Trust	**0.880**	-0.815	0.832	0.691	0.812
Risk	-0.815	**0.835**	-0.798	-0.675	-0.746
Usefulness	0.832	-0.798	**0.904**	0.784	0.884
Ease	0.691	-0.675	0.784	**0.925**	0.805
Intention	0.812	-0.746	0.884	0.805	**0.957**

Note: AVE is represented by bold diagonal elements.

Table 4.11. Composite reliability and AVEs for the five constructs

	Composite reliability	AVE
Trust	0.932	0.775
Risk	0.928	0.697
Usefulness	0.947	0.817
Ease	0.960	0.856
Intention	0.970	0.916

The second procedure to check discriminant validity requires an AVE (Average Variance Extracted) analysis. In such an analysis the square root of every AVE (one for each latent construct) should be larger than any correlation among any pair of latent constructs. Conceptually, the AVE test is equivalent to saying that the correlation of the construct with its attribute items should be larger than its correlation with the other constructs (Gefen & Straub, 2005; also depicted in Figure 4.25). Discriminant validity is also met according to this second procedure (see Table 4.10).

Finally, the composite reliability and AVE for each construct can be used to assess the reliability of the constructs. AVE is suggested to be at least .50 (Fornell and Larcker, 1981). The accepted value for composite reliability is 0.70 and higher (Thompson et al., 1994). Thus, all constructs show a high degree of internal consistency and the overall amount of variance in the items accounted for by the latent construct is acceptable (see Table 4.11).

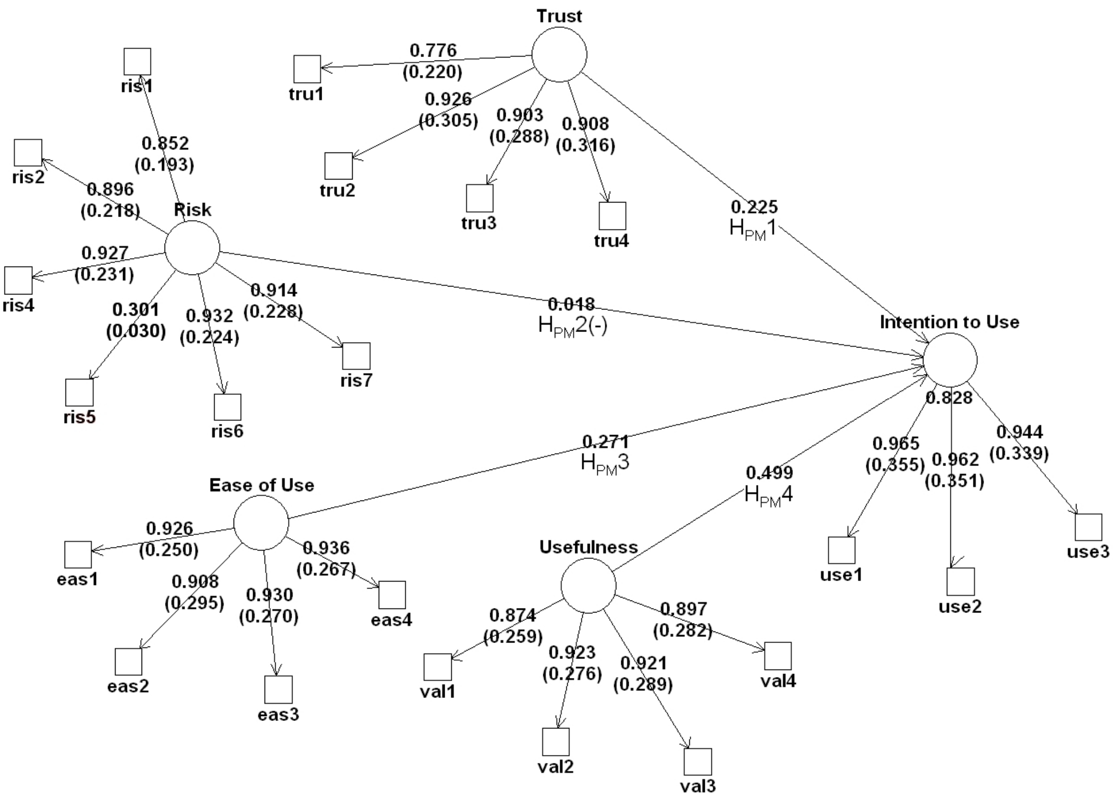
Based on the above results, convergent validity, discriminant validity and reliability of the constructs and their indicators have been demonstrated. The path coefficients for the model, generated by PLS, are shown in Table 4.12. The amount of variance in the dependent latent variable (intention to use) explained by the model was rather high, namely 83% (see Figure 4.26).

Table 4.12. Path estimates and t-statistic for each of the 4 relations tested

	Path estimate	T-statistic
Trust - Intention	0.225	3.3383
Risk - Intention	0.018	0.3306[a]
Usefulness - Intention	0.499	7.1211
Ease - Intention	0.271	5.1863

Note: [a] Not significant.

Figure 4.26. Estimated model parameters including indicators



Note: The number above each path from an indicator (in boxes, e.g. tru1) to a latent variable (in circles e.g. trust) is the indicator loading. The number below each path in brackets is the indicator weight. The number below intention to use is the construct R^2 (calculated and displayed for each variable that is a dependent variable in the model).

Chin (1998) suggests as a minimum standard for paths to be considered meaningful 0.2. In this case all the statistically significant standardized path coefficients are above this value. There was a significant, positive relationship of usefulness of the interfaces and intention to use (Path estimate=.499; p<0.001). Also the relationship between the difference in ease of use of the interfaces and the difference in intention to use was positive and significant (Path estimate=.271; p<0.001). The relationship between intention to use and risk was hypothesized to be negative ($H_{PM}2$). The path estimate however was close to zero, and not significant, thus hypothesis 2 (see paragraph 4.1.2) was not supported by the data. The relationship between the difference in trust of the interfaces and the difference in Intention to use was positive and significant (Path estimate=.225; p<0.001).

Concluding, for the total sample the effect of trust and risk on intention to use is dominated by usefulness and ease of use (path estimates of .255, .018, .499 and .271 respectively).

4.6 DISCUSSION AND CONCLUSIONS

This chapter presented a comparative evaluation of privacy interfaces based on three different conceptual models (Self-Representation, Information-Use and Split-Dimension). These privacy interfaces support the management of one's privacy preferences regarding disclosure of personal information. The types of privacy settings that can be specified with each conceptual model are as follows:

- Self-Representation: approved representations of the self that are suitable for a particular context (based on Goffman, 1959), i.e. approved disclosure instances based on combinations of recipient, purpose of use as well as type of information;
- Information-Use: disapproved disclosure instances based on both purpose of use and type of information.
- Split-Dimension: approved levels of information disclosure split across the three separate dimensions, namely recipient, purpose of use, and type of information.

For each conceptual model a privacy interface was created on the basis of existing privacy interfaces. The interfaces created for the purposes of this study are called the Profiles UI, the Use UI and the Split UI respectively:

- The Profiles UI allows users to specify multiple representations of the self, called profiles, which are different combinations of recipient, purpose of use and type of information, which are suitable in different contexts.
- The Use UI enables users to specify the purposes for which specific types of information are not allowed to be used. This interface is different from both others, since it requires users to specify which information may not be disclosed in a specific context. Furthermore, it is the only interface which allows users to start from default privacy settings.
- The Split UI is based on an even simpler and more restrictive conceptual model, since the appropriate disclosure level of information can only be specified for each dimension (recipient, purpose of use and type of information) separately. This makes it relatively easy to specify the appropriate setting for each dimension; however the user is less flexible in the combinations between the different dimensions.

An experimental comparison of the three interfaces was conducted. Participants made privacy settings with each interface both according to their own insight and corresponding to some pre-determined tasks. Scenarios were used to contextualize both user tasks. Participants were asked to rate their level of privacy concern after using the interfaces according to their own insight. Difficulty of using the interfaces was assessed after performing the pre-determined tasks. Then, participants evaluated the interfaces in pairs in terms of perceived overall difference and on the basis of the five attributes trust, risk, usefulness, ease of use and intention to use. Finally, participants were asked to provide additional comments about each of the interfaces.

The remainder of this section will discuss the results of this study. First, the research approach used for this study will be evaluated. Then the user evaluation of the three Privacy Interfaces will be discussed, including possible suggestions for future design of such interfaces. Subsequently, the results of the study for the end-user acceptance of privacy interfaces will be discussed. And finally, a discussion on possible ways to distinguish users with regard to the evaluation of privacy interfaces will be presented.

Evaluation Research Approach

In this study scenarios were used to contextualize user tasks. Users confirmed being concerned about their privacy in situations addressed by the scenarios. Furthermore, reflection on these scenarios provided valuable insights in the most important user concerns. Comments made by participants during and/or after the experiment demonstrated that participants tried to set the interfaces according to the situations described in the scenarios. In that sense the set up of this study succeeded in providing participants with a believable context of use. In contrast, in most studies where scenarios are used for research, experimenters do not explicitly ascertain that scenarios do convey what they intend to (see for example Spiekermann et al. 2001; Ackerman et al., 1999; Günther & Spiekermann, 2005).

Participants' most frequently mentioned concerns with regard to the scenarios, match the potential drawbacks of Ambient Intelligence described in literature and discussed before in chapter 1. These concerns include privacy and security issues, and the disadvantage of being monitored versus wanting to be in control (see for example Abowd & Mynatt, 2000; ISTAG, 2001; Punie et al., 2005). Furthermore, participants addressed many specific requirements with regard to management of privacy preferences such as: context, recipient, purpose of use and type of information, and a combination of recipient and type of information.

Lederer, Beckman, et al. (2003) comment on the difficulty of evaluating ubiquitous computing applications. Applications need to be built, before they can be evaluated. And precisely this building of applications in the early stages of design or for iterative design is not ideal, because of the quantity of work that is needed. However, based on this study it is concluded that it remains important for participants to be able to experience at least parts of a system in order to evaluate it appropriately. Conveying the implications of using a system, such as for the management of privacy preferences, without participants being able to experience the system for themselves, does not allow participants to reflect on their own situations. Furthermore, different perceptions between participants may be less obvious with such an indirect approach for experiencing systems. A solution to this problem is that participants do not use a complete application, but that they use the interface of an application in combination with scenarios for contextualization, as was done in this study. Even though participants were not exposed to actual privacy risks, by applying privacy concerning scenarios in combination with the use of privacy interfaces participants were deemed capable of judging perceived risk for initial use of such interfaces.

This study obtained a large body of qualitative data. Participants were asked to state their two main concerns in an environment with Ambient Intelligence and comment on (the similarities or differences of) each of the three interface pairs. It would be very interesting to process the qualitative data in real-time and to use it as input in the same study, or to use a staged research approach. The qualitative comments regarding the interfaces could be used to investigate to what extent they cover characteristics of interfaces noticed by participants. Such an analysis provides insight into other important attributes that can be used to predict intention to use. A staged research approach could be that participants provide information about concerns in Ambient Intelligence situations (other than those already mentioned in the current study) and then interfaces are tested in their ability to decrease those particular concerns.

Evaluation Privacy Interfaces

After the first use of the interfaces participants expressed least concern with regard to the use of the Profiles UI and the Use UI, and mentioned slightly more concerns about the use of the Split UI. Perhaps the lack of overview provided by the Split UI contributed to this.

After the second use based on pre-determined tasks, the opinions about the 3 interfaces were more varied: the Profiles UI was considered easiest and the Use UI was considered most difficult. This could have been due to the set up of the tasks matching the Profiles UI better than the Use UI. However, in order to check for the occurrence of this kind of influence a pilot experiment was performed which showed that the difficulty of task descriptions for each of the interfaces was similar. Besides, the study controlled for order of using the interfaces, so neither of the interfaces could benefit from previous experience.

Based on these considerations, it must be concluded that the Profiles UI allowed participants to better fulfill predefined settings, whereas the Use UI did not. It may have been that the availability of default settings in the Use UI, which is an advantage when first exploring an interface, is a disadvantage when trying to achieve a predefined pattern of privacy settings. Further research should be conducted in order to establish what interface aspects are appreciated in case of clearly defined patterns of privacy settings or in case of undecided privacy preferences for instance when first exploring an interface.

After using the interfaces for the two tasks participants were asked to indicate to what extent each interface was regarded to be different from both other interfaces. Each of the interfaces was perceived to be different from the other interfaces. In addition, the results did not show that any two interfaces were more similar to each other than to the remaining interface. In that sense the creation of three different interfaces was successful.

The Profiles UI was expected to be perceived as providing low risk, and high trust, usefulness, ease of use and intention to use. It was indeed perceived to have low risk/concern, and with regard to the other four attributes it was positively perceived as such. The Use UI and Split UI were both expected to be perceived as providing a higher risk, and lower levels of trust, usefulness, ease of use and intention to use in comparison to the Profiles UI. This was indeed the case.

The Profiles UI was generally appreciated because it was considered to be a clear interface with the best overview, and it was regarded as most precise and specific. Furthermore, it allowed people to make combinations between recipient, purpose of use and type of information. A disadvantage of the Profiles UI was the amount of time needed to fully set privacy preferences. Most participants indicated to like a lot of possibilities in a privacy interface; however it should be able to set preferences quickly.

The Use UI was quicker to set in comparison to the Profiles UI, thanks to its default privacy levels. The Use UI and the Split UI were both considered to be confusing, difficult to understand or start using, not foolproof, and in general appreciation for these interfaces was neutral. Furthermore, the Use UI gathered most comments that it was not easy to use, and many comments about the unclear meaning of some UI elements. Its overview was considered to be mediocre and the amount of possibilities were perceived to be limited. The interface was however appreciated for the availability of default settings. Besides comments made with regard to both the Use UI and the Split UI, specific comments for the Split UI were its poor overview, and participants indicated to miss or dislike its ability to make combinations between recipient, purpose of use and type of information.

Overall, the Use UI and Split UI were perceived to be different, yet they were hardly distinguished on the basis of the measured five attributes (although the Split UI turned out to be slightly easier to use). Apparently participants perceive the Split UI and the Use UI to be different on some other dimension than the five attributes measured in this experiment. This is a possibility for future research. First of all the difference in ease of use between the two interfaces should be further examined. Perhaps the interfaces are different in terms of efficiency, ease of learning or satisfaction of use. The comments of participants provide even more directions for future investigation into the differences between the Use UI and Split UI. It seems that there is a difference in terms of availability of default settings, clarity of the interfaces, ability to make combinations, amount of possibilities, consequences of the settings, meaning of the elements, and perceived safety. It could be investigated whether using participants' qualitative comments helps to predict a difference in intention to use as well.

Even though specific interfaces were tested, they should be regarded as representations of the underlying conceptual models of Self-Representation, Information-Use and Split-Dimensions. Both the Profiles UI in this study and the faces metaphor by Lederer et al. (2004) are based on the conceptual model of self-representation. Based on an evaluation of their rendition of the conceptual model in isolation Lederer et al. (2004) dismissed the faces metaphor. Nevertheless, this study shows that the conceptual model of Self-Representation is valuable. In comparison to the conceptual models of Information-Use and Split-Dimension, supporting the idea of multiple identities is appreciated very much by users.

A combination of the Profiles UI and the Use UI could be a promising direction for the design of privacy interfaces; future privacy interfaces should aim to include the aspects of the Profiles UI such as clarity, overview and combinations, as well as the defaults settings of the Use UI. There is some tension between the interface being easy to use on the one hand and the amount of possibilities requested on the other hand. Similarly, in a focus group discussion Cranor et al. (2006) found that people want an interface to be extremely simple, but that there is reluctance to have choices reduced to just three default settings. Therefore, a lot of effort needs to be put in finding appropriate default settings. This is even more important since it turns out that users rarely change default settings (Cranor et al., 2006). A privacy interface should have logical combinations of disclosure to specific recipients, purposes of use and type of information. In this study many participants created different profiles for different groups of recipients such as themselves, their family, medical personnel, finance/insurance parties and store owners. Many participants gave themselves access to all data, for all purposes. Medical personnel for example got access to medical data, for related purposes. The most common combinations could be provided as default settings, to ensure that less time is needed for setting all required settings. However, it should be possible to make modifications to these defaults to keep users in control. Furthermore, it should be made very obvious to users what the consequences of the default settings are. Concerns about the specifics of the default settings are also addressed in Cranor et al. (2006) and Catlett (2000).

The acceptance model for Privacy Interfaces

The attributes trust, usefulness, ease of use and intention to use are closely related and participants' perceptions of interfaces do not differ much with regard to these attributes. If one of these attributes scores high, then all others do too. The opposite holds for risk. The acceptance model for privacy interfaces investigated (PI-Model see Figure 4.7, page 107) was a variation of existing models, in the sense that it focused on Ambient Intelligence environments instead of the internet. Besides, it was an extension of existing models since it included both privacy and trust factors in addition to the general elements for technology acceptance, namely usefulness and ease of use, in an attempt to predict intention to use.

The relative importance of perceived trust, risk, usefulness, and ease of use in trying to explain intention to use was investigated by means of Partial Least Squares using PLS Graph. Of the four tested PI-Model hypotheses (see Figure 4.7, page 107), three were confirmed. The relationships between perceived usefulness (.499; $H_{PM}4$), perceived ease of use (.271, $H_{PM}3$) and trust (.225; $H_{PM}1$) with intention to use were all positive and significant. Risk did not have a significant relationship with intention to use ($H_{PM}2$). This is surprising in itself, since one may expect that the ability of a privacy interface to reduce perceived risk is an important characteristic. However, this does not seem to be the case. The results of the present study indicate that the amount of risk perceived in various interfaces for setting privacy preferences is less important comparing to perceived trust, usefulness and ease of use. This confirmed the initial expectations that even in the context of privacy concerns other features are more important than the reduction of (privacy) risk.

The results of this study are dependent on the specific items used to measure each of the attributes and on the context. Since validated measures based on previous research were used one could expect these to represent similar concepts. Nevertheless, future research could investigate the role of the specific measures used. Furthermore, in this study context of use was conveyed by means of five different Ambient Intelligence scenarios in an attempt to provide participants with a good impression of the diversity of such an environment.

The four background models that do include both risk and intention to use, do find a negative relationship between the two constructs (Featherman & Pavlou, 2003; Lui & Jamieson, 2003; Dinev & Hart, 2006; Malhotra et al., 2004). This could be due to the product involved (privacy interface vs. websites), the context of use (Ambient Intelligence vs. e-commerce), or the specific risk measure used. The risk measure in this study was taken from Corritore et al. (2005). It assessed the extent of agreement with the perception of a kind of general risk, and was phrased like 'I feel' and 'I believe'. Except for the phrasing of the items, the content of the measure was quite similar to that of Malhotra et al. (2004). Two of the other studies used scales with varying anchors in order to assess different types of risk such as the size of the risk and the probability of risk (Lui & Jamieson, 2003; Featherman & Pavlou, 2003). Dinev and Hart (2006) only include measures concerning the size of the risk.

The items used to measure risk were originally intended to measure the extent of risk perceived when interacting with specific websites (Corritore et al., 2005). Perhaps risk involved in Privacy Interfaces should be measured by a different risk construct, i.e. the extent of perceived risk in a certain situation (for instance with Ambient Intelligence) in light of the specific Privacy Interface used to regulate information disclosure.

Two of the risk items turned out to be less useful compared to the other five risk items used. These two risk items could perhaps be improved by changing the wording of the sentences. “I am taking a chance” and the “risks outweigh the benefits” could be changed to “I am gambling” and “the risks are bigger than the benefits”. This might remove some of the ambiguity, and enhance interpretation of the items. Whether or not this will indeed improve the overall risk measure should be tested in future research.

The four items used in this study to measure ease of use, intended to cover both initial and more long-term ease of use. The concept of ease of use could perhaps be separated in different types of ease of use, such as efficiency, ease of learning or satisfaction of use.

As mentioned before, the perceived overall difference between the Use UI and the Split UI is not well explained by the five attributes of the PI-Model. This is an indication that other attributes are of importance in the evaluation of privacy interfaces. It can be investigated whether or not characteristics of the interfaces obtained by participants’ comments will also help to predict intention to use.

Especially after the analysis of the qualitative comments provided by participants it is felt that the concept of control should have been explicitly included in the Privacy Interface Acceptance Model. Control was addressed as a main concern about Ambient Intelligence scenarios. If a privacy interface provides more Control it is likely to increase intention to use. The element of Control is also included in the model by Dinev and Hart (2003).

In creating the PI-Model, constructs of concern and risk were considered to be similar concepts; however, it could be that including these as separate measures will improve the prediction of Intention Use. Hence, future research could aim to study whether or not the prediction of intention to use is improved by including two separate constructs, one for concern and one for risk in the acceptance model.

Classification of users

A hierarchical cluster analysis was performed by which four different groups of participants were distinguished on the basis of the perceived difference between interfaces and the five attributes measured. Only the first three groups were analyzed and described in this thesis, since the fourth group turned out to be a rest group. The first ‘Practical’ group is quite young and female and values privacy/security, as well as a privacy interface that is ease to use and provides many possibilities. These requirements are best provided by the Profiles UI and least by the Use UI. The ‘Pessimistic’ group is also young, highly educated, male and particularly cares about usefulness of an application. Then there is a relatively old and female group (‘Concern & Control). They are the most concerned. Within this group perceived privacy and trust influences intention to use.

5 Conclusions

This chapter first recapitulates the work presented in this thesis, followed by a critical reflection on the conducted research. Subsequently, directions for future research are presented and an account of the contributions of this research is provided. This chapter ends with concluding remarks.

5.1 RECAPITULATION

Chapter 1 introduced the topics of Ambient Intelligence and personalization. It motivated the need to study privacy in this field; in many discussions privacy is seen as a major concern limiting acceptance of Ambient Intelligence by the wider public. Chapter 1 provided a definition of privacy, and presented an overview of related work on user perceptions of privacy. It also presented two possible ways to address user privacy concerns: first by introducing legally based design guidelines for proper handling of personal information, and second by providing users with technical tools for privacy protection.

Chapter 2 presented a study that aimed to investigate how different types and usages of personal information would influence people's privacy decisions and attitudes. A comparison was made regarding practices and experiences of individuals using a Music Recommender system with two different user profiling approaches: one based on music preferences and one based on personality traits. The study showed that even though people considered personality traits to be more personal compared to music preferences, this did not lead to different disclosure behavior for these two types of information. Furthermore, it was more important to people whether or not the disclosure was anonymous than what information was disclosed or what situation the disclosure was occurring in. Finally, the study revealed that the existing instruments for measuring privacy such as the Privacy Attitude Questionnaire (Chignell et al., 2003) and Privacy Segmentation Index (Harris Interactive, 2002) appeared to be unable to predict actual disclosure behavior. Straightforward questions regarding the concerns people had about disclosure of specific types of information turned out to be better indicators of their behavior. More specifically, absence of worries about disclosure of information leads to significantly higher levels of disclosure.

Chapter 3 described a series of studies relating to the interpretation and importance of privacy guidelines from a user perspective. First, the interpretation of privacy guidelines was investigated in two pilot studies. These pilot studies aimed to establish whether a scenario-based approach could be used to study user attitudes relating to privacy and acceptance of personalized systems. Furthermore, the effect of complying or deviating from Fair Information Practices was investigated.
The results showed that people's understanding of these guidelines is limited. Participants confused various system features, or simply had a looser interpretation of system features which were not warranted directly by the privacy policy. Also, the study on the differences in interpretation between video- and text-based scenarios showed poor understanding of a system's compliance with privacy guidelines among participants. About one fifth to one quarter of the privacy guidelines were incorrectly interpreted. Better comprehension was achieved when a text scenario was preceded by a video scenario. This improvement in comprehension occurred for multiple guidelines, of which some were well and others poorly interpreted overall. The last study regarded the relative importance of privacy guidelines and showed that Insight (the possibility to inspect stored data) is considered to be more important in almost three quarters of the situations. The difference in relative importance between Insight and the other guidelines is statistically significant (expect for Openness and Security Safeguards). Least importance was attributed to the guideline of Modification (the possibility to modify or

erase collected data), though this was only significantly different from the importance of the guidelines Insight and Openness.

Chapter 4 presented a study comparing three different conceptual models for the specification of privacy preferences by users. Each conceptual model was realized into a graphical User Interface (UI).

- The interface based on the conceptual model of Self-Representation (called Profiles UI) allowed specific combinations of privacy settings. These privacy settings were determined by the following three dimensions: the recipient, the purpose of use and the type of information.
- The interface based on Information-Use (called Use UI*)* allowed participants to choose between 4 available levels of default privacy settings.
- The third interface based on the conceptual model of Split-Dimension, (called Split UI) was perhaps the most simple and restricted interface, since it did not have any defaults and it did not allow participants to make explicit combinations of privacy settings. Instead, the appropriate disclosure level of information can only be specified for each dimension separately.

Participants used all three interfaces for two different tasks. The first task involved free use of each interface based on people's own concerns and personal goals regarding disclosure of information in light of personalized environments. The second task involved the use of each interface according to some pre-defined goals. Finally, interfaces were evaluated in pairs with regard to the overall perceived difference, and the level of trust, risk, usefulness, ease of use and intention to use. The study investigated three main topics:

- The effect of different conceptual models for privacy interfaces on user's preferences in order to guide design of such interfaces. Overall, the interface that allowed people to make specific combination between the recipient, the purpose of use, and the type of information (Profiles UI) was preferred. This interface was considered to be clear, provided the best overview, and was regarded to be most precise and specific.
- The influence of perceived privacy and trust on intention to use i.e. measure which user interface aspects have the greatest impact on intention to use. Usefulness, ease of use and trust had positive and significant relations with intention to use. Risk did not have a significant relationship with intention to use (see Figure 4.36, pg 152).
- Whether there are any individual differences between participants. Four groups of people were distinguished with regard to their evaluation of the three interfaces: a 'Practical', a 'Pessimistic', a 'Concern & Control' and a rest group. The first three groups were analyzed and described in this thesis. The 'Practical' group was mainly formed by young females who valued privacy/security and preferred a privacy interface that was easy to use and had many possibilities. The 'Pessimistic' group included young, highly educated males. The third 'Concern & Control' group consisted of slightly older female users. They were the most concerned about their privacy.

5.2 EVALUATION OF RESEARCH

5.2.1 Providing an Ambient Intelligence context in research

Context is of major importance for the perception of privacy (Altman, 1975; Adams & Sasse, 2001; Consolvo et al., 2005; Lederer, Mankoff, et al., 2003; Sheehan, 2002), and consequently for research on this topic. However, at the time of the studies for this thesis, Ambient Intelligence had not yet permeated everyday life to a level that it can be used for proper field research to study any actual privacy related behavior. The main limitation of this thesis is that all studies somehow had to give participants the impression of Ambient Intelligence instead of allowing them to actually experience real Ambient Intelligence settings. In this thesis the experience of Ambient Intelligence was conveyed to study participants in two ways. First, by exposing them to prototypical systems that captured essential aspects of the Ambient Intelligence experience, particularly relating to the use of personal information, and second by means of scenarios describing situations that are relevant to Ambient Intelligence.

The study described in chapter 2 involved the use of a music recommender application. The music recommendation service allowed participants to balance their privacy needs with expected benefits of the service, while providing the experimenter control over the experimental conditions. The music recommender service captured the essence of applying user profiles for personalization. The service included user profiling according to 'personal' characteristics of people (their personality traits). As such, the study exposed some of the essential privacy risks that Ambient Intelligence could bring about. As participants had to disclose personal information, they could experience some actual privacy risks involved in the use of such a service.

This approach provided a higher level of realism than most related studies into privacy perception like, for example, those relying on surveys into privacy attitudes (IBM, 1999a; Cyber Dialogue, 2000; Harris Interactive, 2002). Furthermore, participants did indicate to perceive their experience as if they were using a music recommender system, rather than an experiment in privacy. Nevertheless, future research could benefit from studying use and disclosure of private information in the context of fully functional personalized services.

The studies described in chapter 3 did not involve actual risk for participants. However, the studies employed scenarios that aimed to provide participants with a context of health monitoring. The use of scenarios is a commonly followed approach in privacy research. In this thesis precautions were taken to ascertain that the scenario text was correctly interpreted by participants or did indeed convey privacy issues to participants.

In the study presented in chapter 4 the context of Ambient Intelligence was conveyed to participants by combining both scenarios and specific user interfaces. The scenarios successfully addressed privacy concerns and were perceived by participants to be realistic. Furthermore, the comments described by participants corresponded with general concerns that are raised whenever Ambient Intelligence is discussed (see also section 5.4.1). On the basis of the scenarios and specific tasks, participants were asked to use privacy interfaces for managing their personal information disclosure. These interfaces also helped participants to convey the context of Ambient Intelligence. The embodiment of the scenarios by means of the user interfaces provided the study participants with a better depiction of the setting comparing to more traditional methods used in privacy research as described earlier.

Both scenarios and prototypical systems help to set an Ambient Intelligence context for privacy research. Depending on the research phase or topic one can choose to use either one of the approaches, or use a combination of the two as was done in chapter 4.

5.2.2 Recruiting participants for privacy research

Another big concern in setting up representative privacy research is the natural tendency of privacy-concerned individuals to decline to participate. When consent is obtained or when the nature of the study is described, individuals who are more concerned about their privacy may refrain from participating. This is shown by the proportion of privacy concerned and unconcerned individuals taking place in the various studies. In the study of chapter 2 people were recruited for a study involving a music recommender service. In the study of chapter 4 people were recruited for the evaluation of interfaces for the management of privacy preferences. Even though it is likely that such a topic is attractive to privacy concerned individuals who want to control the disclosure of personal information, considerably less privacy concerned individuals took part in the latter study. Ordered from most to least concerned in the study of chapter 2 there were 38% fundamentalists, 50% pragmatists and 13% unconcerned individuals, whereas for chapter 4 these proportions were 14%, 74% and 12% respectively. Therefore, to recruit participants for any study regarding privacy, it seems to be a better practice to disguise the actual study subject of privacy. Instead the study could be described in terms of its tasks and scenarios. In such a way there is a higher chance to gather a representative user sample comparing to the situation when participants are aware of the privacy context of the study.

As one might expect, it was harder to recruit participants for the studies that lasted several hours or days rather than for studies that took less than an hour. This is problematic because, particularly with privacy research, studies may take longer. It takes time to let participants experience the privacy risks involved. For example, due to the fact that the music recommender experiment lasted for at least six days, there were not many participants interested to take part in the study, or they dropped out before completing the study. A possible way to address this problem is to contact people in the proximity of the researcher, since these people are generally more willing to take part. However, care should be taken that potential participants are unaware of the actual aim and scope of the research (see discussion in section 2.4).

5.3 SUGGESTIONS FOR FUTURE RESEARCH

5.3.1 Providing an Ambient Intelligence context in research

Since Ambient Intelligence has not yet entered our daily lives, it is difficult to use existing applications and to study the privacy concerns of their actual users. Using real applications helps to ensure that there is a real privacy risk involved. As Ambient Intelligence applications mature, it is interesting to engage them in field studies where user preferences and reactions to privacy interfaces are assessed in the context of realistic use. For example, existing music recommendation services such as Last.fm and MeeMix could be used. Both of these services use various types of data about the user to improve music recommendations.

Some difficulties arise with the use of existing applications for research. Data cannot be obtained without notifying users a priori, but asking permission to collect user data for research purposes may influence their behavior. Also, the analysis of the use of an existing application gives less control: it becomes more difficult to eliminate confounding variables, to ensure a balanced sample, and to survey opinions at appropriate points in time.

Therefore, participants' behavior and motivations could be investigated by means of the Experience Sampling Method or Day Reconstruction Method. The first method intends to obtain random samples from people's experiences in everyday-life. In an Experience Sampling study participants are instructed to report their experiences immediately whenever they receive a signal (Hormuth, 1986). In the Day Reconstruction Method participants systematically reconstruct their activities and experiences of the preceding day (Kahneman et al., 2004). Both methods help to avoid recall bias, which is an issue when interviewing people about their experiences some time after they occur.

5.3.2 Classifications of people's perspectives on information privacy

This thesis has provided further evidence that people do not have unanimous attitudes regarding privacy. It also identified multiple groups of users in the context of the various studies. Identifying groups of people with similar preferences is of major importance in order to offer each of them appropriate privacy controls. Moreover, if people are addressed as one homogenous group it is likely that privacy controls are less effective, since each group has different needs.

This research did not specifically aim to find one general clustering. However the studies presented resulted in separate classifications based on disclosure of information, and evaluation of privacy interfaces. Future research into classification of users should aim at supporting the identification of these different groups through other characteristics such as gender, education, country of residence, and other dimensions.

5.3.3 Using personality traits for user profiling

Contrary to the initial expectations, the study of chapter 2 showed that people are willing to use personality trait information for user profiling in a personalized music recommender application. However, this finding may be due to the fact that none of the participants in the study experienced an actual privacy breakdown. More longitudinal testing and realism is needed to be certain about the acceptability of personality traits for profiles. In anticipation of future research, considering the ease with which users disclose information that they consider personal, safeguards may be needed to prevent disclosure in unsafe situations. Further research is needed to investigate if the findings relating to personality can be extended to other applications.

5.3.4 Proper presentation of privacy guidelines

Multiple studies in this thesis showed that people have limited understanding of legal statements explaining privacy guidelines. People confuse one statement about a system with another, or have a broader and looser interpretation of some of the system features. People tend not to internalize what is actually stated in the text, but instead they make assumptions not completely supported by or even opposite to the privacy policy statements provided. This could be a general problem that occurs when interpreting text or it could be caused by the specific text used. The fact that also video scenarios were inadequately interpreted suggests that the problem is caused by the specific formulation of the privacy statements. Two possible explanations for these problems are discussed next.

The studies in chapter 3 concerning the understanding and importance of guidelines to protect people's privacy used textual scenarios consisting of loosely connected sentences. The scenarios lacked a fluent narrative structure to ensure a clear correspondence with the eight privacy attributes. It turned out that these scenarios were difficult for participants to read and interpret. In the two pilot studies, that used loosely connected sentences correct interpretation was 51.4% and 73.4%. In study 3, a stronger narrative structure was used, which improved understanding to 77.6% for the textual scenarios. Future research should investigate whether comprehension of privacy guidelines can be further improved by using scenarios with a fluent narrative structure.

In all studies of chapter 3 the scenarios referred to the Fair Information Practices (FIPs). Since FIPs include legal concepts, this may have complicated interpretation of the scenarios. It would, therefore, be interesting to investigate whether a different form for presenting the privacy guidelines would be easier to understand. An example could be guidelines that state not only potential threats, but also include benefits.

5.3.5 Use of text and video scenarios in research

Study 3 of chapter 3 compared the understanding of privacy guidelines for video- and text-based scenarios. It showed that text-based scenarios describing compliance with privacy guidelines were better understood than video-based scenarios. And that comprehension was improved when video-based scenarios were provided before the text. Future work could examine whether similar results are obtained outside the specific domain of privacy research. The basic problem of lack of comprehension has not been studied in the domain of Human-Computer Interaction where scenarios are used as the modus of communication during early design. If the results of this study can be generalized outside the scope of privacy it would imply that current research practices based on scenarios need to be critically reviewed.

Moreover, the third study of chapter 3 allowed participants to view both text- and video-based scenarios multiple times when answering questions regarding compliance with privacy guidelines. For text-based scenarios it was easier to read only part of the text that was most relevant for a particular question, whereas video was less suited for partial inspection. This may have resulted in a slightly better interpretation of the text-based scenarios. This thesis has pointed towards the potential problem of comparing text and video scenarios. Future research could investigate whether these differences in comprehension between text and video material are due to their varying qualities with regard to retrospection or whether they are caused by other factors.

5.3.6 Designing privacy tools

In the privacy interfaces study in chapter 4, only one interface enabled people to explicitly prevent particular instances of information disclosure, whereas the other two were set up to allow instances of information disclosure. This distinction between allowing and preventing disclosure of information was not noticed by all participants and caused improper settings of their privacy preferences. The study in this thesis was not set up to specifically investigate the effect of these two different approaches on privacy protective behavior, but this could be the focus of future research.

The study in chapter 4 also suggested that the availability of default settings could be an advantage when first exploring an interface, yet a disadvantage when following a clear pattern in defining privacy settings. Future research could aim to further investigate the role of default settings in privacy interfaces in relation to the extent to which people have a clear idea of their desired privacy settings.

The evaluation of privacy interfaces was conducted in a laboratory study using scenarios to convey an Ambient Intelligence context. Participants were using the privacy interfaces for only a few tasks, and the effects of their chosen privacy settings on the benefits of the Ambient Intelligence services was not further investigated. Longitudinal studies of actual use are needed to validate the claim that privacy interfaces supporting Self-Representation are valuable, and to investigate the effect of privacy settings on the services as well.

5.4 CONTRIBUTIONS

This thesis aimed to provide knowledge about people's perspectives on information privacy and about designing interaction solutions to reduce people's information privacy concerns related to Ambient Intelligence and personalization. Besides contributions to this main goal, the work in this thesis also provided insights into appropriate research methodology for both of these areas.

The two aims have been addressed through four different research questions focusing on: information privacy concerns, information disclosure behavior, communicating privacy consequences, and designing privacy interfaces. The contribution with regard to these four research areas as well as the methodological insights gained will be discussed in the following sections.

5.4.1 Information privacy concerns

This thesis has provided rich qualitative user data on people's main concerns about information privacy in the context of Ambient Intelligence. Various studies showed that people are indeed concerned about their information privacy in these contexts. Concerns were uttered in relation to the evaluation of system use (chapter 2), privacy guidelines for fair information practices (chapter 3), as well as scenarios describing Ambient Intelligence environments (chapter 4).

More specifically, it was shown that privacy concerns depend on the context involved, such as application, recipients or type of information. These concerns have been mentioned in earlier works (see for example Abowd & Mynatt, 2000; ISTAG, 2001; Punie et al., 2005), but were based on expert views regarding problems and concerns that would be triggered by Ambient Intelligence rather than on empirical findings. This thesis provides empirical support for these expert views.

The study in chapter 4, for example, showed that people are more concerned about their personal information in the context of health monitoring and location tracking than in the context of smart shopping or picture sharing. Furthermore, this thesis has pointed towards individual differences in privacy perception and concerns. In the study of chapter 2, about half of the interviewees indicated to regard personality traits as sensitive information, the others did not. Most of all this study showed that in networked applications about half of the users are primarily concerned about the protection of their identity.

This thesis also showed that not knowing which people may receive or get access to personal information, or making wrong assumptions about the potential recipients, heightens people's concerns about privacy. The influence of the Information Receiver (i.e. recipient) was identified before in the model by Adams and Sasse (2001) for the context of multimedia environments. The role of anticipated recipients on privacy concern was confirmed in all studies described in chapters 2, 3 and 4. Based on the music recommender study in chapter 2 it was found that people worried about other parties gaining access to their data. Based on study 4 in chapter 3 it has to be concluded that being informed about which other parties have access to one's data is the most important guideline (besides having insight into one's own data) compared to other guidelines for Fair Information Practices. Finally, in the study of chapter 4, potential recipients were frequently mentioned as a topic of concern regarding Ambient Intelligence environments.

This thesis has also demonstrated that people are concerned about their lack of insight into the purpose of information use in the context of Ambient Intelligence and personalization. The influence of the purpose was first identified in the model by Adams and Sasse (2001) for the context of multimedia environments. This thesis has shown that feedback, but also control, over purpose of use are important in many different Ambient Intelligence or personalization contexts, such as in the case of personal music or movie recommendations, health monitoring, automatic picture sharing and smart shopping.

The study in chapter 4 showed that people are also concerned about the possibilities to indicate their privacy preferences, such as specifying context, information type, purpose of use, recipient and a combination of recipient and information type. In other words, empirical evidence was provided for a theoretical argument often made in related literature (Cranor, 2004; Nguyen & Mynatt, 2002; Bellotti & Sellen, 1993): the importance of control over personal information in the context of privacy concerns. Perhaps even more significant is the fact that in this thesis the topic of control and its importance was raised by participants themselves. This can be contrasted to studies that explicitly solicit people's attitudes about control (as for example in the study by Günther & Spiekermann, 2005), it is possible that participants are unintentionally primed and that they do not bring up other issues that are important to them. As such the results may not provide a true reflection of the importance of the matter.

However, and in contrast to earlier published results, this thesis has shown that control is not the top concern for all. Statements regarding the importance of control can be refined by taking into account a more detailed segmentation of people regarding their privacy attitudes.

In conclusion, this thesis showed that people are indeed concerned about their information privacy in the context of Ambient Intelligence and personalization. It also demonstrated that people's concerns may be influenced by individual differences, the context involved (e.g. application, recipients or type of information), as well as the level of information and control provided to them (e.g. knowing or controlling who gets access to information). Having provided the conclusion with respect to people's concern about the level of control in an Ambient Intelligence environment; the next section will discuss whether people are actually exercising such control.

5.4.2 Information disclosure behavior

This thesis addressed the second research question about influences on information disclosure behavior of people in varying ways. The music recommender study in chapter 2 investigated actual information disclosure, and the study in chapter 4 provided some insights in people's willingness to disclose information through the settings they made using privacy interfaces. Based on these studies it was shown that willingness to disclose information depends on the balance between privacy concerns and perceived benefits of a system. In the study in chapter 2 it was found that people's hesitance to disclose information was due to privacy concerns, whereas full disclosure was not so much based on absence of concerns, but on perceived benefits one expects in return for the information provided.

In setting up the music recommender study in chapter 2 it was not assumed that the type of information involved in a certain situation would be the sole factor to determine disclosure behavior. Nevertheless, it was assumed that there would be a major difference in sensitivity between different types of information (e.g., personality traits vs. music preferences) and that this would result in different disclosure behaviors. The difference in sensitivity between the two types of information was confirmed, but did not result in different levels of disclosure. Thus, the information type involved (music preferences or personality traits) and the intended use of the information (collaborative filtering or access by other users) did not influence participants' willingness to disclose.

Instead, a large difference was found with regard to disclosing identity information in particular. One group of participants was particularly concerned about disclosure of identity data, whereas another group of participants was not. Earlier research in the form of surveys has often discussed how people's disclosure behaviors regarding internet use is directly influenced by whether people are identifiable or not (Ackerman et al., 1999). The empirical evidence in this thesis validated this claim and also showed that identity was a major obstacle for disclosure, rather than the type of information or the intended recipients (see chapter 2). This finding is relevant to system designers. They could try to offer one solution that will suit both groups of people by enabling people to select between multiple levels of identification for accessing personalized services (e.g. in identifiable, anonymous or pseudonymous form).

As indicated in the previous section this thesis demonstrated privacy concern regarding potential recipients of information. As a consequence of this concern people may refrain from disclosing any information at all out of fear that undesirable recipients may get access to their information. Some participants of the music recommender study chose lower levels of disclosure because of worries about the access to their data by other parties. If there is a possibility to distinguish between different groups of people with regard to the information they are allowed to receive, then people are likely to adapt the level of information disclosure to these different groups. Participants in chapter 4 expressed the desire to restrict disclosure of information to certain recipients, and this was also reflected in their behavior when setting the privacy interfaces. Such a result was possible to obtain as this thesis used an approach which is followed seldom in related research. It based the importance of recipients on actual disclosure behaviour and the extent to which participants exercise control over disclosure to other recipients.

The balancing between privacy concerns on the one hand and the expected benefits on the other hand has been discussed before in literature. However, prior works were based on mere surveys (Hann et al., 2002; O'Neil, 2001) or have not been empirically validated (Acquisti, 2004). Furthermore, these works mainly referred to the context of internet and e-commerce. This thesis provided empirical evidence for the balancing act between concerns and benefits, on the basis of actual disclosure behavior in the context of Ambient Intelligence and personalization. The fact that information disclosure depends on the trade-off between privacy concerns and perceived benefits is of particular importance to privacy researchers. They should take care of investigating (and manipulating) both actual behavior and underlying motivations by performing research that allows both observation and surveying or interviewing.

5.4.3 Communicating privacy consequences

The previous sections showed that there is a dependency between the extent to which people are informed about their environment on the one hand and their privacy concerns and disclosure behavior on the other hand. Lack of proper information about people's Ambient Intelligence environment or personalized applications is likely to raise privacy concerns (see section 5.4.1). These privacy concerns may influence people's disclosure behavior (see section 5.4.2). In other words, properly informing people about the setting they operate in is important to support positive perspectives on information privacy. This section will address more specifically the contributions regarding proper communication of the possible consequences of a system or environment for people's privacy.

This thesis showed that people want to be informed about the possible recipients of their information (chapter 2; chapter 3: study 4) as well as the purpose of use (chapter 2). Furthermore, people want to know what data about them is collected or stored (chapter 3: study 4). These findings are of importance to designers of systems that may affect people's privacy concerns due to the use of personal information. Providing people with information about use of their data is an issue particularly relevant in Ambient Intelligence environments. In less complex environments, such as a recommender system it is usually quite evident what information people give access to. Ambient Intelligence however, gives the opportunity to combine and re-use information easily, which makes it even more relevant to inform users properly about the ways their data will be used.

Participants' awareness of the consequences of information disclosure was addressed explicitly in the interviews of the study of chapter 2. Interviewees were asked about their expectations related to choosing a specific level of disclosure. The studies of chapters 3 and 4 did not address the people's awareness of consequences explicitly. However, from participants' behavior in these latter chapters it could be concluded that unawareness of consequences is an issue (e.g. by misinterpretations of privacy guidelines, or choosing incorrect settings with a privacy interface).

Multiple studies in this thesis showed that people have a limited understanding of the information regarding privacy consequences. In chapter 4 for example some participants did not notice the difference among interfaces with respect to allowing or preventing certain disclosure of information. The first three studies of chapter 3 showed limited understanding for legal statements explaining privacy guidelines. People confuse one statement about a system with another, or have a broader interpretation of some of the system features. Information about the relevance of the collected data for a particular purpose (data quality), was frequently confused with or interpreted as information based on other guidelines. Examples of such guidelines are: keeping the users informed about the type of data that is collected (collection limitation), the purpose for which it is used (purpose specification), or the fact that data is not used for other purposes than those specified (use limitation). People tend not to internalize what is actually stated in the text, but instead they make assumptions not completely supported by or even opposite to the privacy policy provided. This erroneous interpretation of privacy consequences of using a particular system may lead to severe privacy conflicts and remains a serious challenge for design of related systems and for research in this field. Based on the fact that participants' comprehension of privacy related text based on legal guidelines was limited, it is advised to find new ways of communicating the consequences of system use regarding people's privacy. This point was also put forward by Culnan (2003) who argues that current privacy policies are not effective, and therefore a different presentation of privacy policies is needed.

Furthermore, this thesis showed that there are differences in the understanding of privacy guidelines that are provided in a form of text and video scenarios. Study 3 of chapter 3 compared comprehension of privacy guidelines for video and text scenarios. It showed that a variation exists between the two forms. Text scenarios resulted in slightly better understanding of privacy guidelines. It was also shown that the order in which text and video are presented has a significant effect on the level of understanding of these guidelines. When a video-based scenario was shown first, the interpretation of a subsequently shown text-based scenario improved.
This finding is of importance to researchers since interpretation of scenarios should preferably be provided in textual form and be preceded by video. It can be expected that this finding also has implications for designers who want to convey consequences of system use. Again, a textual explanation preceded by video could be used best.

In summary, people like to be informed about several aspects that may influence the privacy consequences of being in an Ambient Intelligence environment (e.g. what data is involved, who gets the data, and what is it used for). However, properly informing people of these consequences is a challenge due to people's limited understanding of privacy related texts. While the principles of Fair Information Practices may be a possible starting point to inform people about their privacy, they definitely do not solve the hardest problems for privacy control. This is what the next section will discuss.

5.4.4 Designing privacy interfaces

The previous three sections already provided some directions for the design of privacy interfaces. First of all, such interfaces should allow people to fully experience the benefits of a service. Furthermore, privacy concerns should be minimized and may be addressed by properly informing people about the type of data involved, the potential recipient of information, and the purpose of use.

The usual approach to deal with the context sensitivity of privacy (mentioned before in section 5.4.1; see also Boyle & Greenberg, 2005) is to offer people a very fine level of control over the disclosure of their information. However, the study in chapter 2 showed that even when control is offered to people, it is not necessarily used. Therefore, designers of privacy tools should aim to provide users an appropriate control over the parameters influencing privacy perception. This section will provide guidance for the design of appropriate means to offer such control.

The study on the evaluation of privacy interfaces in chapter 4 provides empirical evaluation of a wide variety of privacy tools. This study suggested that interfaces for specifying privacy preferences should: be clear and provide a good overview, include a variety of options, and not cost a lot of time and effort to set. It also showed, in contrast to earlier research (Lederer et al., 2004) that the concept of Self-Representation is a credible metaphor for designing privacy interfaces. Nevertheless, longitudinal studies of actual use are needed to validate this claim. The evaluation in this thesis suggests that further improvements can be made by providing some default settings that allow users to save time and effort in defining their privacy and disclosure preferences.

Default settings are helpful to people who are required to specify privacy preferences without a clear idea of their desired settings, but not to people who know beforehand which settings they want to make. In other words, it may be that the availability of default settings, which are an advantage when first exploring an interface are a disadvantage in following a clear pattern of privacy settings.

There is a lot of interest by researchers in privacy interfaces that let users specify privacy policies in terms of information type. However, this thesis showed that context, recipient, and anonymity are of major importance for people's privacy perception. For that reason, designers of future privacy interfaces could aim to offer very coarse information categorizations (e.g. the Use UI provided only five categories) and finer control on the interfaces regarding context and recipient (as in the Profiles UI). Such an approach for privacy interfaces will enable people to exercise detailed control over those factors that are most important to them. Furthermore, it will probably require less time to configure the interface, which is a highly valued aspect. And finally, based on participants concerns regarding Ambient Intelligence scenarios it may be desirable to offer people the ability to switch off the system or to temporarily prevent information disclosure.

Due to the influence of recipients on willingness to disclose information, privacy interfaces that allow users to specify disclosure of information regarding specific recipients are desirable. Consequently, the Use UI (chapter 4) and Privacy Bird interface (Cranor et al., 2006), which do not allow recipients to be specified, are less favorable in that respect.

The relative importance of risk, trust, usefulness, and ease of use in trying to explain intention to use is investigated by means of PLS Graph in chapter 4. The relationships between usefulness, ease of use and trust with intention to use were all positive and significant. Risk did not have a significant relationship with intention to use, as it seems to be dominated by the other factors. Evidently, even in the context of privacy concerns, other features are considered to be more important than the reduction of risk.

The study in chapter 4 also showed that the overall perceived difference between privacy interfaces can be partially explained by the difference in trust, usefulness, ease of use, and intention to use. Qualitative data suggest that other factors can possibly explain the difference between privacy interfaces in terms of perceived efficiency, ease of learning or satisfaction of use.

These findings are of importance for system designers. Regardless the risk involved, people are willing to use a privacy interface if it is considered useful, easy to use and trustworthy.

Based on the study described in chapter 4, four groups of users were identified with regard to the evaluation of interfaces for privacy preference management. This means that different types of privacy interfaces or one flexible kind of privacy interface is needed to suit the desires of each different group. One of these groups of users did especially care about practical issues; they valued an interface that is easy to use and has many options available. Another group had a rather pessimistic view about Ambient Intelligence. They disliked most services depicted in the scenarios and wanted an interface that allowed them to set their privacy preferences quickly. The third group uttered a lot of concerns about Ambient Intelligence and cared most about control. The fourth group was less homogeneous to attribute one label to and can be considered a rest group.

In conclusion, the concept of self-representation, which may be extended with default settings, seems valuable to many people. Having the ability to specify disclosure to specific recipients is regarded important as well. Groups of users were distinguished with regard to their evaluation of privacy interfaces. These groups place different value to the amount of options or level of control provided by an interface, and the ease of use.

5.4.5 Methodology

The research described in this thesis has provided valuable insights into appropriate methodology for (privacy) research. Important implications for future empirical studies concerning privacy on the basis of this thesis are:

1. Apply triangulation of different data-collection methods;
2. Use representative samples of participants based on privacy segmentation;
3. Disguise the experimenter's interest in privacy;
4. Expose participants to realistic privacy risks;
5. Check the comprehension of stimulus material.

Few privacy studies follow such methodological precautions. However, without these precautions the value of privacy research is questionable. Therefore, the methodological guidelines proposed in this section and explained in more detail below should be applied when doing privacy research.

1. Apply triangulation of different data-collection methods

This thesis illustrated the difficulties of doing ethically acceptable and ecologically valid experimental work in the domain of Human-Computer Interaction and privacy. In privacy research a balance needs to be found between introducing actual risk (without seriously harming participants) and still keeping control over the experimental context. Field observations provide limited control over the experimental context, but they provide real risks. Laboratory studies provide great experimental control, yet providing realistic risks is more problematic. Using scenarios for contextualization seems a promising direction, since participants do perceive the concerns or risks involved in the depicted scenarios. The best way to deal with these issues is to apply a combination of different research methodologies in order to benefit from all approaches and to gather valid data.

2. Use representative sample of participants based on privacy segmentation

When investigating privacy attitudes of people, it is important to make sure that both privacy concerned and privacy unconcerned individuals are contacted for research purposes. Otherwise results may not reflect the general population.

In addition, ensuring a representative sample of participants and having appropriate measures for profiling attitudes of participants will allow comparison and meta analysis of results between different studies.

3. Disguise the experimenter's interest in privacy

Disguising the experimenter's interest in privacy serves two purposes. The first purpose is related to the previous point of ensuring a representative sample. By disguising the experimenter interest in privacy, it is likely that a more representative proportion of privacy concerned individuals takes part in research. Secondly, by sensitizing people into the direction of privacy, people may be unintentionally prompted towards the importance of privacy. Consequently, research results may be biased and may not provide a true reflection of the importance of the matter.

4. Expose participants to realistic privacy risks

It is important to expose participants to realistic privacy risks. Currently, however, this is seldom the case like for example in privacy surveys or interviews where participants are not confronted with the consequences of their self-reported behavior. In such cases participants may not seriously consider their privacy behavior and therefore, the reported behavior may not be a reflection of what they would do in reality. Furthermore, it is important that any risks provided in research situations are not mitigated by trust in the experimenter, since this again will reduce perceived risk in the research context.

The thesis has provided strong evidence regarding the discrepancy between stated attitudes and user behavior relating to privacy. This finding has implications for the validity of surveys and post-hoc interviews that do not explicitly investigate behavior. The study of chapter 2 was set up to investigate both disclosure behavior and underlying motives or attitudes. It turned out that stated motives underlying disclosure behavior do not unequivocally account for disclosure behavior. For example some people mentioned the same reason for disclosure in varying situations, while they changed their disclosure behavior across these situations. Others provided varying reasons for identical disclosure of information across situations. Furthermore, personality traits were claimed to be sensitive information yet they were disclosed to much the same extent as the less sensitive music preferences, despite people's claims that they balance costs against the benefits of disclosure. And even privacy-concerned individuals disclosed their profile information including their identity information.

Attitudes towards privacy turned out to be a poor predictor of disclosure behavior. Consequently, the ability to distinguish people's disclosure behavior on the basis of known privacy segmentations is limited. Instead, context-specific privacy concerns are a better approach for classifying people. Thus, whenever aiming to predict disclosure behavior or intention, general privacy attitudes are not sufficient, and more specific measures are needed. Such measures should stay as close as possible to the original context of use.

5. Check the comprehension of stimulus material

The studies in chapter 3 have provided insights into the possibility to conduct text-based empirical studies in the context of privacy. Privacy related statements expressed in text, involving the concepts of information collection versus use, require an extremely accurate reading and interpretation of text that cannot be assumed for the general public. Even relatively simple statements turned out to be ambiguous and were not correctly interpreted, perhaps because of the pre-conceptions and expectations of the participants. For the purposes of privacy research, where such statements are presented to users as a pre-experiment or post-experiment survey, it seems that it is necessary to be very thorough about testing the ability of subjects to comprehend accurately the questions presented to them or to grasp the fine differences in text scenarios that describe privacy issues.

In empirical research regarding privacy the exact interpretations of privacy related questions and descriptions must be tested rigorously. Based on the findings of study 3 in chapter 3 it is recommended that text-based scenarios are preceded by a video-based version for the purposes of privacy- and security-related user surveys.

5.5 CONCLUDING REMARKS

This thesis focused on Ambient Intelligence and personalization and people's perspective on information privacy in that context. It has provided substantial and triangulated empirical evidence based on a series of user studies that many of the privacy concerns of Ambient Intelligence raised by experts are also issues to prospective inhabitants of such environments. The studies illustrated the following concerns of people regarding Ambient Intelligence and personalization:

- Constantly being monitored;
- Being controlled by a system;
- Automatic disclosure of information;
- Potential access to information by other parties;
- Maintaining privacy;
- Being informed (correctly) about information practices;
- Security of collected and stored information.

The studies provided insight into priorities of users that are likely to be beneficial for researchers and designers working in this area.

The intrinsic features of Ambient Intelligence such as its invisibility and interconnectedness result in a limited understanding of the (potential) collection, storage and use of personal information by people, and hence cause concerns. As a consequence of this limited understanding people may fail to protect their privacy or may not know how to protect themselves against privacy violations. Studies in this thesis have shown that:

- People are not very careful in reading text in order to derive privacy consequences of systems.
- People may make inferences about the privacy consequences beyond what is warranted by the text.
- People tend to stick to their initial privacy settings even under varying privacy risks.

Based on the research carried out in this thesis, it must be concluded, that people can indeed become concerned when their privacy may be at stake. However, this does not mean that they actively protect their privacy when they have the means to do so. In other words, people may worry about their privacy, but they do not act to protect themselves against their concerns. Based on this thesis it is expected that three main perspectives with regard to information privacy can be distinguished:

1. Not caring about privacy or information disclosure (trust in society);
2. Caring about privacy and wanting to be properly informed about what information is collected and how it will be used (trust in legislation);
3. Caring about privacy and taking control of information disclosure (trust in technology).

There is a difference in the extent to which people value personalization or Ambient Intelligence, which could help to explain nuances in people's perspectives on information privacy within one group.

Consequently, this thesis states that there are two related prerequisites for people to properly manage their privacy in an Ambient Intelligence setting:

- People should be aware of the (digital) traces of personal information they leave behind.
- People should have control over their personal traces.

Awareness about traces left behind requires that people are informed about the (potential) collection, storage and use of personal information. This thesis has shown that doing this carefully is a challenge on its own due to people's loose interpretation of statements about information use.

A running theme throughout this thesis has been the context sensitive nature of privacy risks, privacy preferences and disclosure behaviors. Current solutions for managing personal information do not match this level of contextualization. This thesis suggests that solutions of the future should recognize people and their situational context, and adapt and anticipate towards their privacy related needs and choices. Perhaps the ultimate aim of designers is to design a privacy interface that embodies Ambient Intelligence. Such an interface should be – as Ambient Intelligence is meant to be – integrated in the environment and enable people to manage their privacy without conscious effort. Managing one's privacy should be flexible, relaxing and enjoyable, unobtrusive, and nowhere unless one needs it. As such a privacy interface should provide seamless, intuitive support allowing people to concentrate on their real tasks. Perhaps this could be in the form of a Digital Privacy Assistant, which knows a lot about the user (gradually learned over time), and who knows exactly when it is important to take independent decisions and when the user's approval is needed.

Bibliography

Aarts, E. (2003). Technological issues in Ambient Intelligence. In E. Aarts, & S. Mazano (Eds.), *The new everyday: views on Ambient Intelligence* (pp. 12-17). Rotterdam, The Netherlands: 010 Publishers.

Aarts, E. (2005). Ambient Intelligence drives open innovation. *Interactions*, 12(4), 66-68.

Aarts, E., Harwig, H., & Schuurmans, M. (2002). Ambient Intelligence. In J. Denning (Ed.), *The invisible future: The seamless integration of technology into everyday life* (pp. 235-250). New York, NY: McGraw Hill.

Abowd, G.D., & Mynatt, E.D. (2000). Charting past, present, and future research in Ubiquitous Computing. *ACM Transactions on Computer-Human Interaction*, 7(1), 29-58.

Ackerman, M.S. (2000). The intellectual challenge of CSCW: The gap between social requirements and technical feasibility. *Human-Computer Interaction*, 15(2), 179-203.

Ackerman, M.S., & Cranor, L. (1999). Privacy critics: UI components to safeguard users' privacy. *Extended abstracts on Human Factors in Computing Systems: CHI '99*, 258-259.

Ackerman, M.S., Cranor, L.F., & Reagle, J. (1999). Privacy in e-commerce: Examining user scenarios and privacy preferences. *Proceedings of the 1st ACM conference on Electronic Commerce: EC '99*, 1-8.

Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification. *Proceedings of the 5th ACM conference on Electronic Commerce: EC '04*, 21-29.

Acquisti, A., & Grossklags, J. (2003). Losses, gains and hyperbolic discounting: An experimental approach to information security attitudes and behaviors. *2nd Annual Workshop on Economics and Information Security: WEIS 2003*.

Adams, A. 2001. *Users' perceptions of privacy in multimedia communications*. Doctoral dissertation, University College London, England.

Adams, A., & Sasse, M.A. (2001). Privacy in multimedia communications: Protecting users, not just data. In A. Blandford, J. Vanderdonckt, & P. Gray (Eds.), *People and computers XV: Interaction without frontiers. Joint Proceedings of HCI2001 and IHM2001* (pp. 49-64). London: Springer.

Ajzen, I., & Fishbein, M. (2005). The influence of attitudes on behavior. In D. Albarracín, B.T. Johnson, & M.P. Zanna (Eds.), *The handbook of attitudes* (pp. 173-221). London: Erlbaum.

Aldenderfer, M.S., & Blashfield, R.K. (1985). *Cluster analysis* (2nd ed., Quantitative applications in the social sciences, 44). London: Sage.

Altman, I. (1975). *The environment and social behavior: Privacy, personal space, territory, crowding*. S.L.: Brooks/Cole.

Barton, J. (2006). TiVo-lution. *ACM Queue*, 4(3), 28-35.

Bellotti, V. (1997). Design for privacy in multimedia computing and communications environments. In P. Agre, & M. Rotenberg (Eds.), *Technology and privacy: The new landscape* (pp. 63-98). Cambridge, MA: MIT Press.

Bellotti, V., & Sellen, A. (1993). Design for privacy in Ubiquitous Computing environments. *Proceedings of the third European conference on Computer Supported Cooperative Work: ECSCW'93*, 77-86.

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

Black, J.A., & Champion, D.J. (1976). *Methods and issues in social research*. Chichester, England: Wiley.

Boyd, D. (2002). *Faceted id/entity: Managing representation in a digital world*. Master's thesis, Massachusetts Institute of Technology, Cambridge, MA.

Boyle, M., & Greenberg, S. (2005). The language of privacy: Learning from video media space analysis and design. *ACM Transactions*, 12 (2), 328-370.

Buzznet (n.d.). *About Buzznet* [On-line]. Retrieved, June 5, 2008 from http://www.buzznet.com/

Byers, S., Cranor, L.F., & Kormann, D. (2003). Automated analysis of P3P-abled Web sites. *Proceedings of the 5th International Conference on Electronic Commerce: ICEC '03*, 326-338.

Campbell & Stanley. (1966). *Experimental and quasi-experimental designs for research*. Boston: Houghton Mifflin.

Carroll, J.M. (1995). *Scenario-based design: Envisioning work and technology in system development*. New York: John-Wiley & Sons.

Catlett, J. (2000). Open letter to P3P developers & replies. Proceedings of the 10th Conference on Computers, Freedom and Privacy: Challenging the Assumptions, CFP '00, 157-164.

CBS (2006, August 3). *StatLine. Kerncijfers 'Onderwijsniveau beroepsbevolking'* [On-line, Key figures on 'Education level labourforce']. Retrieved July 1, 2008 from http://statline.cbs.nl/StatWeb/publication/?DM=SLNL&PA=70896ned&D1=0-1&D2=0&D3=0-2,7,20,24,l&D4=0&D5=0&D6=l&HDR=G5,T,G1,G3,G4&STB =G2&VW=T

CBS (2008, February 27). *StatLine. Kerncijfers 'Bevolking'* [On-line, Key figures on 'Population']. Retrieved July 1, 2008 from http://statline.cbs.nl/StatWeb/ publication/?DM=SLNL&PA=37296ned&D1=0-2,8-13,22-24,56&D2=l&HDR= G1&STB=T&VW=T

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

Chignell, M.H., Quan-Haase, A., & Gwizdka, J. (2003). The Privacy Attitude Questionnaire (PAQ): Initial development and validation. *Proceedings of the Human Factors and Ergonomics Society 47th Annual Meeting*, 1326-1330.

Child, I.L. (1968). Personality in culture. In E.F. Borgatta, & W.W. Lambert (Eds.), *Handbook of personality theory and research* (pp. 82-145). Chicago: Rand McNally.

Chin, W.W. (1998). Issues and opinion on structural equation modeling [Commentary]. *MIS Quarterly*, 22(1), VII-XVI.

Chung, E., Hong, J., Lin, J., Prabaker, M., Landay, J.A., & Liu, A. (2004). Development and evaluation of emerging design patterns for Ubiquitous Computing. *Proceedings of the 5th conference on Designing Interactive Systems: DIS 2004*, 233-242.

Clarke, R. (1999). Internet privacy concerns confirm the case for intervention. *Communications of the ACM*, 42(2), 60-67.

Consolvo, S., Smith, I.E., Matthews, T., LaMarca, A. Tabert, J., & Powledge, P. (2005). Location disclosure to social relations: Why, when & what people want to share. *Proceedings of the SIGCHI conference on Human Factors in Computing Systems: CHI '05*, 81-90.

Consolvo, S., & Walker, M. (2003). Using the Experience Sampling Method to evaluate Ubicomp applications. *IEEE Pervasive Computing*, 2(2), 24-31.

Corritore, C.L., Marble, R.P., Wiedenbeck, S., Kracher, B., & Chandran, A. (2005). Measuring online trust of websites: Credibility, perceived ease of use, and risk. *Proceedings of the Eleventh Americas Conference on Information Systems*, 2419-2427.

Cranor, L.F. (2004). 'I didn't buy it for myself': Privacy and ecommerce personalization. In C.-M. Karat, J.O. Blom, & J. Karat (Eds.), *Designing personalized user experiences in ecommerce* (pp. 57-73). Norwell, MA: Kluwer Academic.

Cranor, L.F., Guduru, P., & Arjula, M. (2006). User interfaces for privacy agents. *ACM Transactions on Computer-Human Interaction*, 13(2), 135-178.

Csikszentmihalyi, M., & Larson, R. (1987). Validity and reliability of the Experience-Sampling Method. *Journal of Nervous and Mental Disease*, 175, 526–536.

Culnan, M.J. (2000). Protecting privacy online: Is self-regulation working? *Journal of Public Policy & Marketing*. 19(1), 20-27.

Culnan, M. (2003, March). How privacy notices promote informed choice. In Center for Democracy and Technology, *Considering consumer privacy: A resource for policy makers and practitioners* (pp. 12-16). Retrieved June 5, 2008, from http://www.cdt.org/privacy/ccp/ccp.pdf

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

Cyber Dialogue Inc. (2000). *Privacy vs. personalization* (Part III). [On-line]. Retrieved 20 August, 2003, from http://www.egov.vic.gov.au/pdfs/wp-2000-privacy3.pdf

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.

Denzin, N.K. (Ed.). (1970). *Sociological methods: A sourcebook*. S.L.: Aldine Publishing.

Dickinson, I., Reynolds, D., Banks, D., Cayzer, S., & Vora, P. (2003). User profiling with privacy: A framework for adaptive information agents. In M. Klusch et al. (Eds.), *Intelligent information agents* (LNAI 2586, pp. 123-151). Berlin Heidelberg: Springer.

Dinev, T., & P. Hart, P. (2003). Privacy concerns and internet use: A model of trade-off factors. In *Best Paper Proceedings of Annual Academy of Management Meeting* (pp. 131-137). Briarcliff Manor, NY: Academy of Management.

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

Donthu, N. & Cherian, J. (1993). Differences in consumer perceptions of similarity and dissimilarity. *Marketing Letters*, 4(1), 31-38.

Emans, B. (1990). *Interviewen: Theorie, techniek en training*. [Interviewing: Theory, technique and training] Groningen, The Netherlands: Wolters-Noordhoff.

Erickson, M.L. (2008, May). Dissimilarity and the classification of male singing voices. *Journal of Voice*, 22 (3), 290-299.

European Parliament. (1995, November 23). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal of the European Communities*, No L. 281, 31-50.

Everitt, B.S. (1993). *Cluster analysis* (3rd ed.). London: Edward Arnold.

Featherman, M.S., & Pavlou, P.A. (2003). Predicting e-services adoption: A perceived risk facets perspective. *International Journal of Human-Computer Studies*, 59, 451-474.

Fischer, G. (2001). User modeling in Human-Computer Interaction. *User Modeling and User-Adapted Interaction*, 11, 65-86.

Fornell, C., & Larcker, D.F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*; 18, 39-50.

Gabrielsen, G. (2000). Paired comparisons and designed experiments. *Food Quality and Preference*, 11, 55-61.

Garbarino, E., & Strahilevitz, M. (2004). Gender differences in the perceived risk of buying online and the effects of receiving a site recommendation. *Journal of Business Research*, 57, 768-775.

Garde-Perik, E. van de, Markopoulos, P., & Ruyter, B. de (2006a). On the relative importance of privacy guidelines for ambient health care. *The fourth Nordic Conference on Human-Computer Interaction: NordiCHI 2006*, 377-380.

Garde-Perik, E. van de, Markopoulos, P., & Ruyter, B. de. (2006b). Privacy policies and text-based empirical research: Methodological issues. *CHI 2006 Workshop on Privacy and HCI: Methodologies for Studying Privacy Issues*.

Garde-Perik, E. van de, Markopoulos, P., Ruyter, B. de, Eggen, J.H., & IJsselsteijn, W. (2008). Investigating privacy attitudes and behavior in relation to personalization. *Social Science Computer Review*, 26(1), 20-43.

Garfinkel, S. (2000). *Database nation: The death of privacy in the 21st century*. Paris: O'Reilly.

Gefen, D. & Straub, D. (2005). A practical guide to factorial validity using PLS-Graph: Tutorial and annotated example. *Communications of the Association for Information Systems*, 16, 91-109.

Get Safe Online (2007) Press release #8: Social networkers and wireless networks users provide “rich pickings” for criminals [On-line]. *Get Safe Online Week 2007*. 12th November, 2007. Retrieved 11 November, 2008, from http://www.getsafeonline.org/nqcontent.cfm?a_id=1469

Goffman, E. (1959). *The presentation of self in everyday life*. Garden City, New York: Doubleday.

Good, N.S., & Krekelberg, A. (2003). Usability and privacy: A study of KaZaA P2P file sharing. *Proceedings of the SIGCHI conference on Human factors in Computing Systems: CHI ‘03*, 137-144.

Gosling, S.D., Rentfrow, P.J., & Swann, W.B.Jr. (2003). A very brief measure of the Big Five personality domains. *Journal of Research in Personality*, 37, 504-528.

Günther, O., & Spiekermann, S. (2005). RFID and the perception of control: The consumer’s view. *Communications of the ACM*, 48(9), 73-76.

GVU Center, Georgia Tech Research Corporation. (1998). GVU’s 10th WWW user survey. [On-line]. Retrieved 16 October, 2007, from http://www.cc.gatech.edu/user_surveys/

Hann, I., Hui, K.L., Lee, T.S., & Png, I.P.L. (2002). Online information privacy: Measuring the cost-benefit trade-offs. *Proceedings of the Twenty-Third International Conference on Information Systems*, 1-10.

Harris Interactive. (2002, February). Privacy on and off the internet: What consumers want (Study No. 15229). [On-line]. New York, NY: Harris Interactive. Retrieved January 10, 2007, from http://www.aicpa.org/download/webtrust/priv_rpt_21mar02.pdf

Hong, J.I., Ng, J.D., Lederer, S., & Landay, J.A. (2004). Privacy risk models for designing privacy-sensitive ubiquitous computing systems. *Proceedings DIS 2004*, 91-100.

Hormuth, S.E. (1986). The sampling of experiences in situ, *Journal of Personality*, 54(1), 262-293.

Iachello, G., & Abowd, G.D. (2005). Privacy and proportionality: Adapting legal evaluation techniques to inform design in ubiquitous computing. *Proceedings of the SIGCHI conference on Human factors in computing systems: CHI ‘05*, 91-100.

Iachello, G., & Hong, J. (2007). End-user privacy in Human-Computer Interaction. *Foundations and Trends in Human - Computer Interaction*, 1(1), 1-137.

IBM. (1999a, October). IBM multi-national consumer privacy survey. [On-line]. Retrieved 20 August 2003, from http://www.ibm.com/services/e-business/priwkshop.html

IBM. (1999b). Pervasive computing [Theme issue]. *IBM Systems Journal*, 38(4).

IBM. (n.d.). *IBM Personal Care Connect* [On-line]. Retrieved June 5, 2008, from http://www-03.ibm.com/industries/healthcare/doc/content/resource/business/1537659105.html

ISTAG. (2001, February). *Scenarios for Ambient Intelligence in 2010* [On-line]. Retrieved 15-04-04, from ftp://ftp.cordis.europa.eu/pub/ist/docs/istagscenarios2010.pdf

Jensen, C., Potts, C. (2004). Privacy policies as decision-making tools: An evaluation of online privacy notices. *CHI Letters*, 6, 471-478.

Jiang, X., Hong, J.I., & Landay, J.A. (2002). Approximate information flows: Socially-based modeling of privacy in ubiquitous computing. *Proceedings Ubicomp 2002* (LNCS 2398), 176-193

Kahneman, D., Krueger, A.B., Schkade, D.A., Schwarz, N., & Stone, A.A. (2004). A survey method for characterizing daily life experience: The Day Reconstruction Method. *Science*, 306, 1776-1780.

Karat, J. (1995). Scenario use in the design of a speech recognition system. In J.M. Carroll (Ed.), *Scenario-Based design: Envisioning work and technology in system development* (pp. 109-133). New York: John-Wiley & Sons.

Kobsa, A. (2001). Generic user modeling systems. *User Modeling and User-Adapted Interaction*, 11(1-2), 49-63.

Kobsa, A. (2002). Personalized hypermedia and international privacy. *Communications of the ACM*, 45(5), 64-67.

Kobsa, A. (2003). A component architecture for dynamically managing privacy constraints in personalized web-based systems. *Privacy Enhancing Technologies* (LNCS 2760, pp 177-188). Berlin Heidelberg: Springer.

Kobsa, A., Koenemann, J., & Pohl, W. (2001). Personalized hypermedia presentation techniques for improving online customer relationships. *The Knowledge Engineering Review*, 16(2), 111-155.

Kobsa, A., & Schreck, J. (2003). Privacy through pseudonymity in user-adaptive systems. *ACM Transactions on Internet Technology*, 3(2), 149-183.

Kobsa, A., & Teltzrow, M. (2005). Contextualized communication of privacy practices and personalization benefits: Impacts on users' data sharing and purchase behavior. *4th International Workshop, PET 2004* (LNCS 3424), 329-343.

Langheinrich, M. (2001). Privacy by design: Principles of privacy-aware Ubiquitous systems. *Proceedings of the Third International Conference on Ubiquitous Computing: UbiComp 2001* (LNCS 2201), 273-291.

Langheinrich, M. (2002). A privacy awareness system for Ubiquitous Computing environments. *Proceedings International Conference on Ubiquitous Computing: UbiComp 2002,* 237-245.

Langheinrich, M. (2005). *Personal privacy in Ubiquitous Computing tools and system support*. Doctoral dissertation, Swiss Federal Institute of Technology Zurich, Switzerland.

Lau, T., Etzioni, O., & Weld, D.S. (1999). Privacy interfaces for information management. *Communications of the ACM*, 42(10), 88-94.

Lederer, S., Beckmann, C., Dey, A.K., & Mankoff, J. (2003, June). Managing personal information disclosure in Ubiquitous Computing environments (IRB-TR-03-015). Berkeley, CA: Intel Research Berkeley.

Lederer, S., Dey, A.K., & Mankoff, J. (2002). A conceptual model and a metaphor of everyday privacy in ubiquitous computing environments (Technical Report: CSD-02-1188). Berkeley: University of California at Berkeley.

Lederer, S., Hong, J.I., Dey, A.K., & Landay, J.A. (2004). Personal privacy through understanding and action: Five pitfalls for designers. *Personal and Ubiquitous Computing*, 8(6), 440-454.

Lederer, S., Hong, J.I., Jiang, X., Dey, A.K., Landay, J.A., & Mankoff, J. (2003, October). Towards everyday privacy for ubiquitous computing (Technical Report UCBCSD-03-1283), Berkeley: University of California at Berkeley.

Lederer, S., Mankoff, J., & Dey, A.K. (2003). Who wants to know what when? Privacy preference determinants in Ubiquitous Computing. *Extended abstracts on Human Factors in Computing Systems: CHI '03*, 724-725.

Lui, H.K., & Jamieson, R. (2003). Integrating trust and risk perceptions in business-to-consumer electronic commerce with the technology acceptance model. *Proceedings of the Eleventh European Conference on Information Systems: ECIS*, 1154-1170.

Mahmud, Al A., Kaptein, M., Moran, O., Garde-Perik, E. van de, & Markopoulos, P. (2007). Understanding compliance to privacy guidelines using text-and video-based scenarios. *Human-Computer Interaction: Interact 2007* (LNCS 4663, Part II), 156-168.

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

Margulis, S. (2003). On the status and contribution of Westin's and Altman's theories of privacy. *Journal of Social Issues*, 59(2), 411-429.

Martens, J.B.O.S. (2003). Image technology design: a perceptual approach. Dordrecht: Kluwer Academic.

Milgram, S. (1974). *Obedience to authority: An experimental view*. New York, NY: Harper and Row.

Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing*, 18, 15-29.

Nardi BA. (1992). The use of scenarios in design. *SIGCHI Bulletin*, 24(4), 13-14.

Neustaedter, C., & Greenberg, S. (2003). The design of a context-aware home media space for balancing privacy and awareness. *Proceedings of the 5th International Conference on Ubiquitous Computing: Ubicomp 2003*, 297-314.

Nguyen, D.H., & Mynatt, E.D. (2002, June). Privacy mirrors: Understanding and shaping socio-technical Ubiquitous Computing systems (Technical Report GIT-GVU-02-16). Atlanta: Georgia Institute of Technology. Retrieved 3 December, 2007, from http://www.erstwhile.org/writings/PrivacyMirrors.pdf

Nielsen, J. (1993). *Usability engineering*. San Diego: Academic Press.

Nokia Mobilize and Share, MOSH. [On-line]. Retrieved June 5, 2008, from http://mosh.nokia.com/.

Ofcom. (2008). Social Networking: A quantitative and qualitative research report into attitudes, behaviours and use [On-line]. 2 April 2008. Retrieved 11 November, 2008, from http://www.ofcom.org.uk/advice/media_literacy/medlitpub/medlitpubrss/socialnetworking/report.pdf

O'Neil, D. (2001). Analysis of Internet users' level of online privacy concerns. *Social Science Computer Review*, 19 (1), pp. 17-31.

Olivero, N., & Lunt, P. (2004). Privacy versus willingness to disclose in e-commerce exchanges: The effect of risk awareness on the relative role of trust and control. *Journal of Economic Psychology*, 25(2), 243-262.

Organisation for Economic Co-operation and Development, OECD. (1980, September 23). Guidelines on the protection of privacy and transborder flows of personal data [On-line]. Retrieved, October 13, 2005, from http://www.oecd.org/document/20/ 0,3343,en_2649_34255_15589524_1_1_1_1,00.html

Organisation for Economic Co-operation and Development, OECD. (2007). Participative web and user-created content: Web 2.0, wikis and social networking [On-line]. Retrieved 11 November, 2008, from http://www.oecd.org/document/ 40/0,3343,en_2649_34223_39428648_1_1_1_1,00.html

Patil, S., Romero, N.A., & Karat, J. (2006). Privacy and HCI: Methodologies for studying privacy issues. *CHI '06 extended abstracts on Human factors in computing systems*, 1719-1722.

Pedersen, D. M. (1979). Dimensions of privacy. *Perceptual and Motor Skills*, 48, 1291-1297.

Pedersen, D.M. (1999). Model for types of privacy by privacy functions. *Journal of Environmental Psychology*, 19, 397-405.

Perik, E., Ruyter, B. de, Markopoulos, P., & Eggen, J.H. (2004). The sensitivities of user profile information in music recommender systems. *Second Annual Conference on Privacy, Security and Trust: PST 2004*, 137-141.

Pettersson, J.S. Fischer-Hübner, S., Danielsson, N., Nilsson, J., Bergmann, M., Clauss, S., Kriegelstein, T., & Krasemann, H. (2005). Making PRIME usable. *Proceedings of the 2005 symposium on Usable privacy and security: SOUPS '05*, 53-64.

Philips Motiva, [On-line]. Retrieved June 5, 2008 from http://www.medical.philips.com/main/products/telemonitoring/products/motiva/

Privacy Protection Study Commission (1977) *Personal privacy in an information society: The report of the Privacy Protection Study Commission transmitted to President Jimmy Carter on July 12, 1977* [On-line]. Retrieved 27-11-2007, from http://www.epic.org/privacy/ppsc1977report/

Punie, Y., Delaitre, S., Maghiros, I., & Wright, D. (Eds.). (2005, November). *Dark scenarios on Ambient Intelligence: Highlighting risks and vulnerabilities*. (SWAMI Deliverable D2. A report of the SWAMI consortium to the European Commission under contract 006507).

Raykov, T., & Marcoulides, G.A. (2000). *A first course in structural equation modeling*. London: Lawrence Erlbaum.

Rentfrow, P. J., & Gosling, S. D. (2003). The do re mi's of everyday life: The structure and personality correlates of music preferences. *Journal of Personality and Social Psychology*, 84, 1236-1256.

Ridder, H. de (1996). Current issues and new techniques in visual quality assessment, *Proceedings International Conference on Image Processing 1996*, 1, 869-872.

Ridder, H. de (2001, January). Cognitive issues in image quality measurement. Journal of Electronic Imaging 10(1), 47-55.

Riegelsberger, J. (2005). *Trust in mediated interactions*. Doctoral dissertation, University College London, England.

Robertson, S.P. (1995). Generating object-oriented design representations via scenario queries. Pg. 279-308. In J.M. Carroll (Ed.), *Scenario-based design: Envisioning work and technology in system development*. New York: John-Wiley & Sons.

Rode, J., Johansson, C., DiGioia, P., Filho, R.S., Nies, K., Nguyen, D.H., Ren, J., Dourish, P., & Redmiles, D. (2006). Seeing further: Extending visualization as a basis for usable security. *Proceedings of the second symposium on Usable privacy and security: SOUPS '06*, 145-155.

Romero, N.A., Perik, E.M., & Patil, S. (2005). Appropriate methodology for empirical studies of privacy. *Proceedings Human-Computer Interaction: Interact 2005*, 87-89.

Satyanarayanan, M. (2002). A catalyst for mobile and ubiquitous computing. *IEEE Pervasive Computing*, 1(1), 2-5.

Scheffé, H. (1952). An analysis of variance for paired comparisons. *Journal of the American Statistical Association*, 47(259), 381-400.

Sheehan, K. (1999). An investigation of gender differences in on-line privacy concerns and resultant behaviors. *Journal of Interactive Marketing* 13(4), 24-38.

Sheehan, K. (2002). Toward a typology of internet users and online privacy concerns. *The Information Society*, 18(1), 21-32.

Sophos. (2007). Sophos Facebook ID probe shows 41% of users happy to reveal all to potential identity thieves [On-line]. 14 August 2007. Retrieved 11 November, 2008, from http://www.sophos.com/pressoffice/news/articles/2007/08/facebook.html

Spiekermann, S., Grossklags, J. & Berendt, B. (2001) E-privacy in 2nd generation e-commerce: Privacy preferences versus actual behavior. *Proceedings of the 3rd ACM conference on electronic commerce (EC '01)*, 38-47.

SPSS (2005). *Help Topics of SPSS 14.0 for Windows*. Release 14.0.0 (5 Sep 2005).

Stanford, V. (2002). Using pervasive computing to deliver elder care. *IEEE Pervasive Computing Magazine*, 1(1), 10-13.

Straub, D., Boudreau, M.C., & Gefen, D. (2004). Validation guidelines for IS positivist research. *Communications of the Association for Information Systems*, 13, 380-427.

Strauss, A., & Corbin, J. (1990). *Basics of qualitative research: Grounded theory procedures and techniques*. Newbury Park, CA: Sage.

Suh, B., & Han, I. (2002). Effect of trust on customer acceptance of internet banking. *Electronic Commerce Research and Applications*, 1, 247-263.

Teltzrow, M., & Kobsa, A. (2004). Impacts of user privacy preferences on personalized systems. In C.-M. Karat, J.O. Blom, & J. Karat (Eds.), *Designing personalized user experiences in ecommerce* (pp. 315-332). Norwell, MA: Kluwer Academic Publishers.

Temme, D., Kreis, H., & Hildebrandt, L. (2006). PLS path modeling: A software review. SFB 649 Discussion Paper 2006-084. Humboldt University Berlin. Retrieved, 3 June 2008 from http://edoc.hu-berlin.de/series/sfb-649-papers/2006-84/PDF/84.pdf

Thompson, R.L., Higgins, C.A., & Howell, J.M. (1994). Influence of experience on personal computer utilization: Testing a conceptual model. *Journal of Management Information Systems*, 11(1), 167-187.

Trewin, S. (2000). Configuration agents, control and privacy. *Proceedings on the 2000 conference on Universal Usability* (pp.9-16). New York: ACM.

United States Department of Health, Education and Welfare. (1973, July). Records, computers and the rights of citizens: Report of the secretary's Advisory Committee on Automated Personal Data Systems. Retrieved 27-11-2007, from http://aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm

W3C. (1998, July). *P3P Guiding Principles: W3C NOTE 21 July 1998*. [On-line] Retrieved January 10, 2007, from http://www.w3.org/TR/NOTE-P3P10-principles

Warren, S.D., & Brandeis, L.D. (1890). The right to privacy. Harvard Law Review, 4(5) Retrieved 27-11-2007, from http://www-swiss.ai.mit.edu/6805/articles/privacy/Privacy_brand_warr2.html

Weiser, M. (1991). The computer for the twenty-first century. *Scientific American*, 265, 94-104.

Westin, A.F. (1967). *Privacy and freedom*. New York, NY: Atheneum.

Whiddett, R., Hunter, I., Engelbrecht, J., & Handy, J. (2006). Patients' attitudes towards sharing their health information. *International Journal of Medical Informatics*, 75, 530-541.

Summary

Current developments towards Ambient Intelligence and related technological visions of the future are founded on continuous collection of information about individuals and their activities. This collection of information, its potentially persistent storage, dissemination and use raise privacy concerns. In the debate surrounding privacy and Ambient Intelligence, this thesis takes a user centered perspective examining the attitudes, preferences and behaviors of people regarding disclosure of information. Furthermore, it uses these insights to guide the design of interfaces for managing one's related privacy needs.

The work presented in this thesis comprises three study domains. First, privacy concerns and disclosure behavior in relation to a music recommender system were investigated. It was anticipated that people would weigh the costs and benefits of their disclosure decisions and act accordingly. Also, it was expected that personality traits would be considered more personal or private than music preferences, resulting in lower willingness to disclose such information. However, it turned out that despite the fact that personality traits indeed were considered more personal than music preferences, disclosure levels were similar. This study also demonstrated the methodological difficulties of studying privacy. Despite the efforts to provide a true music recommendations service, participants felt protected somehow by the context of the research. This study showed that it is not sufficient to just consider privacy disclosure as a trade-off pertaining to the personal value of information but that other factors regarding the context of disclosure play an important role, e.g., recipient, assumed use of information, level of anonymity, or study context.

The second domain investigated legal principles or guidelines as a basis to inform users regarding privacy consequences in four related studies. Two pilot studies showed that comprehension of privacy guidelines is poor. Another study on the differences in interpretation between video- and text-based scenarios showed poor understanding of the compliance with privacy guidelines as well. Text-based scenarios describing privacy guidelines were better understood than video-based scenarios. Furthermore, it turned out that comprehension can be improved when video-based scenarios are provided before the text. Also, the relative importance of each guideline was evaluated. Participants were offered pairs of privacy guidelines in a health care context, and were asked to indicate their most preferred guideline. Participants particularly valued to have access to their own personal data (Insight), followed by having information about the other parties that have access to their information (Openness).

The last domain concerned interface solutions for managing privacy preferences of users. In this study participants compared three interfaces based on three different conceptual models regarding the way personal information is managed. The first conceptual model of Self-Representation takes a social psychology perspective focusing on how individuals manage the presentation of their 'self' through selective disclosure of information. The second conceptual model of Information-Use enables users to specify which types of information may not be disclosed for specific purposes of use. The third conceptual model of Split-Dimension enables users to specify approved levels of information disclosure split across three separate dimensions: recipient, purpose of use, and type of information. Overall, the interface based on Self-Representation was judged

best with regard to the five attributes: trust, risk, usefulness, ease of use and intention to use. The interface based on Split-Dimension seemed slightly easier to use than the interface based on Information-Use, but apart from that these two interfaces were perceived to be similar. There were large differences regarding the perception of the three interfaces across participants. Based on these differences four clusters of participants were distinguished. Three clusters appreciated the conceptual model based on Self-Representation, but they differed in the extent to which the other two conceptual models were appreciated. There was one rest cluster which did not have a clear preference for any of the interfaces. Also, in this study a model was evaluated in order to determine the relative importance of trust, risk, usefulness, and ease of use on intention to use. Risk did not have a significant relation with intention to use, whereas usefulness had the highest impact on intention to use. Trust and ease of use both had small influences on intention to use. Apparently even in the context of privacy interfaces trust, usefulness, and ease of use are more important than perceived privacy risks.

Based on the work presented in this thesis it can be concluded that any system that is meant to provide users control over their personal information in a personalized context should give users insight into their own personal data. Furthermore, it should inform users about which persons and parties have access to their information. Users should be protected not to disclose information that is anyway regarded as personal, since they may not realize this at the moment of initial use of the system. Systems for setting personal preferences for disclosure of information should allow people a great deal of control. However, it should be easy to achieve this level of control, by the existence of default settings that are preferably protective of the users' personal information.

Curriculum Vitae

August 26, 1975	Born in Oldenzaal
1987 – 1993	Voorbereidend Wetenschappelijk Onderwijs (VWO, Highschool) Thijcollege Oldenzaal
1993 – 1998	Household and Consumer Sciences (MSc) Agricultural University of Wageningen
1998 – 2000	User-System Interaction (MTD) Postgraduate Programme in Technological Design Eindhoven University of Technology
2001 – 2001	Junior Product Manager Set Top Boxes Philips Digital Networks, Eindhoven
2001 – 2003	Project Manager Qualitative Research OP&P Product Research, Utrecht
2003 – 2008	PhD Candidate Industrial Design, Eindhoven University of Technology, and Philips Research Laboratories Eindhoven
2008 –	Post Doctoral Researcher Industrial Design, Eindhoven University of Technology

Appendix A: Inquiries Chapter 2

A1. MEASURES THROUGHOUT THE USE OF THE RECOMMENDER

Music Preferences

For the following items, please indicate your basic preference level for the genres listed using the scale provided:

MP1	○	Classical	1: Strongly dislike
MP2	○	Blues	2
MP3	○	Country	3
MP4	○	Dance/Electronica	4: Neither agree nor disagree
MP5	○	Folk	5
MP6	○	Rap/hip-hop	6
MP7	○	Soul/funk	7: Strongly like
MP8	○	Religious	
MP9	○	Alternative	
MP10	○	Jazz	
MP11	○	Rock	
MP12	○	Pop	
MP13	○	Heavy Metal	
MP14	○	Soundtracks/theme songs	

Scoring for the four music preference dimensions: Reflective & Complex: 1, 2, 5, 10; Intense & Rebellious: 9, 11, 13; Upbeat & Conventional: 3, 8, 12, 14; Energetic & Rhythmic: 4, 6, 7. [10]

Personality traits

Here are a number of personality traits that may or may not apply to you. Please indicate for each statement the extent to which you agree or disagree with that statement. You should rate the extent to which the pair of traits applies to you, even if one characteristic applies more strongly than the other.

	I see myself as:		
Tip1	○	Extraverted, enthusiastic	1 = Disagree strongly
Tip2	○	Critical, quarrelsome	2 = Disagree moderately
Tip3	○	Dependable, self-disciplined	3 = Disagree a little
Tip4	○	Anxious, easily upset	4 = Neither agree nor disagree
Tip5	○	Open to new experiences, complex	5 = Agree a little
Tip6	○	Reserved, quiet	6 = Agree moderately
Tip7	○	Sympathetic, warm	7 = Agree strongly
Tip8	○	Disorganized, careless	
Tip9	○	Calm, emotionally stable	
Tip10	○	Conventional, uncreative	

TIPI scoring ("R" = reverse-scored): Take the AVERAGE of the two items (the standard item and the recoded reverse-scored item) that make up each scale. Extraversion: 1, 6R; Agreeableness: 2R, 7; Conscientiousness; 3, 8R; Emotional Stability: 4R, 9; Openness to Experiences: 5, 10R.

[10] Italic sections were not provided to participants, but are added to this appendix for clarification.

Quality rating playlist

Before getting a new playlist, please indicate to what extent you feel that the quality of the current playlist is good:

○ Very bad
○
○
○
○ Very good

Music Recommender Setting - Comparison of preferences/characteristics

The quality of your recommendations may improve when your preferences/characteristics are compared to those of other users.

Please indicate below what level of permission you provide the Music Recommender for the comparison of your preferences/characteristics to those of other users.

○ **No permission** (your preferences/characteristics will not be used for the comparison, the Recommender will operate the same way as before)
○ **Restricted permission** (the Recommender will use your preferences/characteristics for comparison in anonymous form)
○ **Full permission** (the Recommender will use your preferences/characteristics including your e-mail address for comparison)

Depending on the type of recommender system in use, the text above addressed either preferences or characteristics (for the music preference based recommender and the personality-based recommender respectively).

Music Recommender Setting - Showing preferences/characteristics to others

The quality of your recommendations may improve if you allow the system to show your preferences/characteristics to other users. This will also enable you to exchange recommendations or ideas with them.

Please indicate below what level of permission you provide the Music Recommender for showing your preferences/characteristics to other users.

○ **No permission** (your preferences/characteristics will not be shown to others, the Recommender will operate the same way as before)
○ **Restricted permission** (the Recommender will show your preferences/characteristics to other users in anonymous form)
○ **Full permission** (the Recommender will show your preferences/characteristics including your e-mail address to other users)

Depending on the type of recommender system in use, the text above addressed either preferences or characteristics (for the music preference based recommender and the personality-based recommender respectively).

A2. QUESTIONNAIRE AFTER THE USE OF THE RECOMMENDER

Background questions	**Possible answer**
What is your gender?	○ Male ○ Female
What is your age?	*(Open question)*
What is your function type? (eg. research, teaching, administration)	*(Open question)*
What is your area of expertise? (eg. computer science, psychology)	*(Open question)*
How many CD's do you (approximately) have?	○ Less then 25 ○ Between 25-50 ○ Between 51-100 ○ Between 101-200 ○ More then 200
How often do you listen to music from your PC?	○ Always ○ Frequently ○ Sometimes ○ Rarely ○ Never
How many MP3 songs do you (approximately) have?	○ Less then 25 ○ Between 25-50 ○ Between 51-100 ○ Between 101-200 ○ More then 200

General questions Music Recommender	**Possible answer**
What is your opinion of the Music Recommender application in general?	○ Like it a lot ○ Like it somewhat ○ Neither like, nor dislike ○ Dislike it somewhat ○ Dislike it a lot
What elements of the application did you particularly like?	(*Open Question*)
What elements of the application did you particularly dislike?	(*Open Question*)

Sensitivity of information	**Possible answer**
How did you feel about the fact that you were asked to indicate your preference level for music genres?	(*Open Question*)
How did you feel about the fact that you were asked to indicate your personality traits?	(*Open Question*)
During your use of the Music Recommender it may or may not have been possible for other people to observe your personal information. Please indicate, for each of the following situations, whether you find such a situation worrying or not.	
Do you find it worrying… ○ when other people can observe your preferences for music genres? ○ when other people can observe your personality traits? ○ when a music content provider may observe your preferences for music genres? ○ when a music content provider may observe your personality traits?	 ○ No ○ Yes

User effort	**Possible answer**
○ How much effort was it for you to indicate your music preferences? ○ How much effort was it for you to indicate your personality traits?	○ Much effort ○ Little effort ○ No effort

Quality of recommendations

Did you notice any difference in the overall quality of the recommended songs between A and B (see below)?
A) the songs recommended to you based on your preferences for music genres
B) the songs recommended to you based on your characteristics

Possible answer

○ The preference based recommendations where much better
○ The preference based recommendations where a little better
○ There was no difference between the two types of recommendations
○ The characteristic based recommendations where a little better
○ The characteristic based recommendations where much better

Disclosure choices	**Possible answer**
You have been asked four times to choose the level of permission (no, restricted, full) with regard to the use of your personal information. You are asked to comment on your choices below.	
For the comparison of your music preferences to those of other users you gave the system …. (no / restricted / full) permission.	
○ Why did you choose this particular level of permission?	*(Open question)*
○ What level of permission would you provide the system if you could choose again?	No / Restricted / Full permission
○ Why would you choose this level of permission now?	*(Open question)*
For showing your music preferences to other users (in return for possible recommendations by them) you gave the system …. (no / restricted / full) permission. *(Same 3 questions as above)*	
For the comparison of your characteristics to those of other users you gave the system …. (no / restricted / full) permission. *(Same 3 questions as above)*	
For showing your music preferences to other users (in return for possible recommendations by them) you gave the system …. (no / restricted / full) permission. *(Same 3 questions as above)*	

Evaluation privacy statements	**Possible answer**
Please indicate, for each of the following statements, the extent to which you agree or disagree with that statement.	
General privacy statements ○ I am afraid my personal information will be accessible to unintended parties. ○ Information in automated systems is secure. ○ I am willing to provide personal information in return for low-cost products or convenience. ○ I have concerns about companies mutually exchanging personal information about me. ○ I am concerned about threats to my personal privacy nowadays. ○ I use encryption of e-mail messages to protect my privacy. ○ I am afraid that companies will share my personal information to others. ○ I rarely read privacy policies on websites. ○ I would provide personal information in order to use a service, if the purpose of the information request is clear. ○ Sometimes when personal information is required, I provide fictitious data. ○ Whenever there is personal information collected about me, I want to be able to check and correct the information held about me. ○ There are adequate safeguards for the personal information kept in databases by businesses. ○ I like to get advance notice when information is collected about me. ○ I don't mind that companies use my personal details, as long as I know about it, and can stop it. ○ I am aware of my rights based on privacy laws.	○ Strongly disagree ○ Somewhat disagree ○ Neither agree, nor disagree ○ Somewhat agree ○ Strongly agree
PSI (Privacy Segmentation Index) statements ○ Consumers have lost all control over how personal information is collected and used by companies. ○ Most businesses handle the personal information they collect about consumers in a proper and confidential way ○ Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today	○ Strongly disagree ○ Somewhat disagree ○ Neither agree, nor disagree ○ Somewhat agree ○ Strongly agree

Closure	**Possible answer**
Before you finish this questionnaire, please indicate whether you are interested in participating in future research.	○ No, I am not interested in participating in future research ○ Yes, I am interested in participating in future research
You have reached the end of the questionnaire about your experiences with the Music Recommender. Thanks for your time. Please click the “finish!” button below before you close your browser.	
To provide you with a small token of appreciation for participating in this research, please enter your name and your home or office address here.	
○ Full name ○ Street ○ Zip code ○ City	*(Open question)*
Is there anything else you would like to add or comment on?	*(Open question)*

A3. INTERVIEW TOPICS

Before we start to discuss your experiences, first of all I would like to thank you for you participation in this research.

Permission audio recording.

General

First I will ask you some general questions, afterwards I will go more into detail and discuss the way you used the Music Recommender.

- What is you first reaction to the use of the Music Recommender?
- What do you think was the purpose or focus of this research?

  2 goals:
  - Difference in quality between recommended music based on genre preferences and music based on personality traits
  - The way people share personal information or keep it to themselves with regard to personalized services (focus interview)
- You have been using two main versions of the Music Recommender. In one the recommendations were based on your preferences for music genres. The other version recommended music to you based on your characterization of yourself. If you compare these two applications with each other, what do you notice?

Specific

(Topics are to be used as guidance only. The order is not fixed, but will depend on the course of the conversation.)

Now, we will discuss all phases of the experiment in more detail.

Music based on genre preferences – no use of information

- Advantages
- Disadvantages

Music based on genre preferences – compare info to others

- Choice permission in return for improved recommendations: why yes/no
- What was the basis of your decision, what were the considerations?
- Why restricted (anonymous) or full permission
- Expectations upfront
- Experiences afterwards, apply changes?
- Advantages
- Disadvantages

Music based on genre preferences – show info to others

- Choice permission in return for improved recommendations: why yes/no
- What was the basis of your decision, what were the considerations?
- Why restricted (anonymous) or full permission
- Expectations upfront
- Experiences afterwards, apply changes?
- Advantages
- Disadvantages

Music based on characterization - no use of information

- Advantages
- Disadvantages

Music based on characterization - compare info to others

- Choice permission in return for improved recommendations: why yes/no
- What was the basis of your decision, what were the considerations?
- Why restricted (anonymous) or full permission
- Expectations upfront
- Experiences afterwards, apply changes?
- Advantages
- Disadvantages

Music based on characterization - show info to others

- Choice permission in return for improved recommendations: why yes/no
- What was the basis of your decision, what were the considerations?
- Why restricted (anonymous) or full permission
- Expectations upfront
- Experiences afterwards, apply changes?
- Advantages
- Disadvantages

Remaining comments or questions

Appendix B: Questionnaires Chapter 3

B1. QUESTIONNAIRE OF STUDY 1

Page 1A

Evaluation of a Health Support System

This is a small questionnaire about your opinion of a Health Support System.
Thanks in advance for your participation.

Context

Imagine the following context:

- John is suffering from diabetes and lives alone with his dog. As long as he controls his sugar intake, he can do whatever he likes. In the past he had some problems to stick to his diet, since he is not that interested in preparing food or cooking.
- Recently, a health support system, that monitors various health parameters, like blood pressure, weight, pulse and glucose levels, is installed in his house. This system allows John to guard his health and makes it easier to live healthy, since it can also give meal suggestions.
- The system checks John's glucose levels constantly. This helps him to better regulate his diet and also gives him a warning in case of deterioration. This gives John piece of mind, but also supports his doctor.

Aim of the questionnaire

- In this study you're exposed to some variations of the health support system like the one installed in John's house. Some system features may be more desirable than others. This is what we want to find out in order to improve the system.
- First of all we would like to know whether the descriptions of the system features are clear or not. You are exposed to two different systems.
- For each system, you will first read a system description. After reading this description, you will be asked to indicate whether or not you feel that the system described lives up to some system features. In some cases you may be asked to formulate a new description that better expresses the system features.

Page 1B

Health Support System 1

Please read the description of System 1 presented below:

The health support system does not inform John about the various types of information that are collected and stored. The system informs John that the collected information will be used to monitor his health parameters. The system collects information that is relevant for monitoring John’s health. The collected information may be disclosed and used for purposes other than those John is informed about, such as marketing or advertising. John knows what services, organizations or individuals have access to his personal information. The stored information is not protected by any means against security risks. John can not inspect all the information that is stored about him. John can not modify or erase the information that is stored about him.

Evaluation System 1

Please indicate for each of the following system features whether you think System 1 provides this feature or not: (by circling the appropriate answer)

- John is informed in advance about the type of data that will be collected Yes / No
- John is informed about the use/purpose of data collection Yes / No
- All the data that is collected is relevant to the main purpose Yes / No
- The data will be used only to serve the main purpose Yes / No
- John is informed about the other parties that have access to his data Yes / No
- The data is securely stored Yes / No
- John can get insight into the data that is stored about him Yes / No
- John has the possibility to make changes in the stored data Yes / No

Please hand over this page to the experimenter.

Page 2A

Health Support System 2

Now you will be provided with another system description. Please read the description of System 2 presented below:

The health support system informs John that it collects and stores information about weight, blood pressure, pulse and glucose levels. The system does not inform John what the collected information will be used for. The system may also collect information that is not related to health monitoring, for example the amount of time John spend watching TV, or registering what websites he visited. The collected information will not be disclosed or used for purposes other than those John is informed about, such as marketing or advertising. John does not know what services, organizations or individuals have access to his personal information. The stored information is protected against risks by security safeguards. John can inspect all the information that is stored about him. John can modify or erase the information that is stored about him.

Evaluation System 2

Please indicate for each of the following system features whether you think System 2 provides this feature or not: (by circling the appropriate answer)

o	John is informed in advance about the type of data that will be collected	Yes / No
o	John is informed about the use/purpose of data collection	Yes / No
o	All the data that is collected is relevant to the main purpose	Yes / No
o	The data will be used only to serve the main purpose	Yes / No
o	John is informed about the other parties that have access to his data	Yes / No
o	The data is securely stored	Yes / No
o	John can get insight into the data that is stored about him	Yes / No
o	John has the possibility to make changes in the stored data	Yes / No

Page 2B

Additional questions

Could you please indicate for each of the following conditions, whether you are suffering from them or not? (by circling the appropriate answer)

○	Heart failure	Yes / No
○	Diabetes	Yes / No
○	COPD (Chronic Obstructive Pulmonary Disease)	Yes / No
○	Asthma	Yes / No
○	Depression	Yes / No

Could you please indicate your age by checking the appropriate box below?

○ 25 years or younger

○ Between 26 and 45

○ Between 46 and 65

○ 66 years or older

Please hand over this page to the experimenter.

Page 3A

Description of System 1

Below you will be asked a few additional questions about the description of Health Support System 1. To help you answer the following questions, the original description of the system is presented at the next page.

You’ve indicated that system 1 provides a feature such that ‘John is informed in advance about the type of data that will be collected’. Please reformulate the concerning paragraph in such a way that the system DOES NOT provide this feature:

You’ve indicated that system 1 does not provide a feature such that ‘John is informed about the use/purpose of data collection’. Please reformulate the concerning paragraph in such a way that the system DOES provide this feature:

You’ve indicated that system 1 does not provide a feature such that ‘All the data that is collected is relevant to the main purpose’. Please reformulate the concerning paragraph in such a way that the system DOES provide this feature:

You’ve indicated that system 1 provides a feature such that ‘The data will be used only to serve the main purpose’. Please reformulate the concerning paragraph in such a way that the system DOES NOT provide this feature:

You’ve indicated that system 1 does not provide a feature such that ‘John is informed about the other parties that have access to his data’. Please reformulate the concerning paragraph in such a way that the system DOES provide this feature:

Page 3B

You've indicated that system 1 provides a feature such that 'The data is securely stored'. Please reformulate the concerning paragraph in such a way that the system DOES NOT provide this feature:

You've indicated that system 1 provides a feature such that 'John can get insight into the data that is stored about him'. Please reformulate the concerning paragraph in such a way that the system DOES NOT provide this feature:

You've indicated that system 1 provides a feature such that 'John has the possibility to make changes in the stored data'. Please reformulate the concerning paragraph in such a way that the system DOES NOT provide this feature:

<u>Original description Health Support System 1:</u>

The health support system does not inform John about the various types of information that are collected and stored. The system informs John that the collected information will be used to monitor his health parameters. The system collects information that is relevant for monitoring John's health. The collected information may be disclosed and used for purposes other than those John is informed about, such as marketing or advertising. John knows what services, organizations or individuals have access to his personal information. The stored information is not protected by any means against security risks. John can not inspect all the information that is stored about him. John can not modify or erase the information that is stored about him.

Please hand over this page to the experimenter.

Page 4A

Description of System 2

Below you will be asked a few additional questions about the description of Health Support System 1. To help you answer the following questions, the original description of the system is presented at the next page.

You've indicated that system 2 does not provide a feature such that 'John is informed in advance about the type of data that will be collected'. Please reformulate the concerning paragraph in such a way that the system DOES provide this feature:

You've indicated that system 2 provides a feature such that 'John is informed about the use/purpose of data collection'. Please reformulate the concerning paragraph in such a way that the system DOES NOT provide this feature:

You've indicated that system 2 provides a feature such that 'All the data that is collected is relevant to the main purpose'. Please reformulate the concerning paragraph in such a way that the system DOES NOT provide this feature:

You've indicated that system 2 does not provide a feature such that 'The data will be used only to serve the main purpose'. Please reformulate the concerning paragraph in such a way that the system DOES provide this feature:

You've indicated that system 2 provides a feature such that 'John is informed about the other parties that have access to his data'. Please reformulate the concerning paragraph in such a way that the system DOES NOT provide this feature:

Page 4B

You've indicated that system 2 does not provide a feature such that 'The data is securely stored'. Please reformulate the concerning paragraph in such a way that the system DOES provide this feature:

You've indicated that system 2 does not provide a feature such that 'John can get insight into the data that is stored about him'. Please reformulate the concerning paragraph in such a way that the system DOES provide this feature:

You've indicated that system 2 does not provide a feature such that 'John has the possibility to make changes in the stored data'. Please reformulate the concerning paragraph in such a way that the system DOES provide this feature:

<u>Original description Health Support System 2:</u>

The health support system informs John that it collects and stores information about weight, blood pressure, pulse and glucose levels. The system does not inform John what the collected information will be used for. The system may also collect information that is not related to health monitoring, for example the amount of time John spend watching TV, or registering what websites he visited. The collected information will not be disclosed or used for purposes other than those John is informed about, such as marketing or advertising. John does not know what services, organizations or individuals have access to his personal information. The stored information is protected against risks by security safeguards. John can inspect all the information that is stored about him. John can modify or erase the information that is stored about him.

This was the last page.

Thanks for your participation!

B2. QUESTIONNAIRE OF STUDY 2

Page 1A

(identical to pilot 1)

Page 1B

Health Support System 1

Please read the description of System 1 presented below:

The system does not inform John that it will collect data regarding his health, blood pressure, pulse and glucose level. The system informs John that data is collected in order to monitor his diabetes condition. The system informs John that it will only collect data that is useful for tracking his diabetes condition. The system informs John that it uses his data for other reasons than the main purpose of the system as well. The system informs John regarding all the organizations or individuals who can access his data. The system informs John that his data is not protected by any security safeguards. The system does not provide facilities for John to inspect all data collected about him. The system does not provide facilities to allow John to modify or erase any data about him.

Evaluation System 1

Please indicate for each of the following system features whether you think System 1 provides this feature or not: (by circling the appropriate answer)

- The user is informed about the type of data that will be collected. Yes / No
- The user is informed about the main purpose for which the data will be used. Yes / No
- The system only collects data that is relevant to the main purpose of the system. Yes / No
- The data will be used solely to serve the main purpose of the system. Yes / No
- The user is informed about which other parties have access to the collected data. Yes / No
- The data is securely stored. Yes / No
- The user can inspect the stored personal data. Yes / No
- The user has the possibility to make changes in the stored data Yes / No

Please hand over this page to the experimenter.

Page 2A

Health Support System 2

Now you will be provided with another system description. Please read the description of System 2 presented below:

The system informs John that it will collect data regarding his health, blood pressure, pulse and glucose level. The system does not inform John that data is collected in order to monitor his diabetes condition. The system informs John that it collects also data that is useful for things other than tracking his diabetes condition. The system informs John that it will not use his data for any other reason than the main purpose of the system. The system does not inform John regarding all the organizations or individuals who can access his data. The system informs John that all his data is securely stored. The system provides facilities for John to inspect all data collected about him. The system provides facilities to allow John to modify or erase any data about him.

Evaluation System 2

Please indicate for each of the following system features whether you think System 2 provides this feature or not: (by circling the appropriate answer)

o	The user is informed about the type of data that will be collected.	Yes / No
o	The user is informed about the main purpose for which the data will be used.	Yes / No
o	The system only collects data that is relevant to the main purpose of the system.	Yes / No
o	The data will be used solely to serve the main purpose of the system.	Yes / No
o	The user is informed about which other parties have access to the collected data.	Yes / No
o	The data is securely stored.	Yes / No
o	The user can inspect the stored personal data.	Yes / No
o	The user has the possibility to make changes in the stored data	Yes / No

Page 2B

(identical to pilot 1)

Page 3A

Description of System 1

Below you will be asked a few additional questions about the description of Health Support System 1. To help you answer the following questions, the original description of the system is presented at the next page.

You've indicated that system 1 provides a feature such that 'The user is informed about the type of data that will be collected'. Please reformulate the concerning paragraph in such a way that the system DOES NOT provide this feature:

You've indicated that system 1 does not provide a feature such that 'The user is informed about the main purpose for which the data will be used'. Please reformulate the concerning paragraph in such a way that the system DOES provide this feature:

You've indicated that system 1 does not provide a feature such that 'The system only collects data that is relevant to the main purpose of the system'. Please reformulate the concerning paragraph in such a way that the system DOES provide this feature:

You've indicated that system 1 provides a feature such that 'The data will be used solely to serve the main purpose of the system'. Please reformulate the concerning paragraph in such a way that the system DOES NOT provide this feature:

You've indicated that system 1 does not provide a feature such that 'The user is informed about which other parties have access to the collected data'. Please reformulate the concerning paragraph in such a way that the system DOES provide this feature:

Page 3B

You've indicated that system 1 provides a feature such that 'The data is securely stored'. Please reformulate the concerning paragraph in such a way that the system DOES NOT provide this feature:

You've indicated that system 1 provides a feature such that 'The user can inspect the stored personal data'. Please reformulate the concerning paragraph in such a way that the system DOES NOT provide this feature:

You've indicated that system 1 provides a feature such that 'The user has the possibility to make changes in the stored data'. Please reformulate the concerning paragraph in such a way that the system DOES NOT provide this feature:

Original description Health Support System 1:

The system does not inform John that it will collect data regarding his health, blood pressure, pulse and glucose level. The system informs John that data is collected in order to monitor his diabetes condition. The system informs John that it will only collect data that is useful for tracking his diabetes condition. The system informs John that it uses his data for other reasons than the main purpose of the system as well. The system informs John regarding all the organizations or individuals who can access his data. The system informs John that his data is not protected by any security safeguards. The system does not provide facilities for John to inspect all data collected about him. The system does not provide facilities to allow John to modify or erase any data about him.

Please hand over this page to the experimenter.

Page 4A

Description of System 2

Below you will be asked a few additional questions about the description of Health Support System 1. To help you answer the following questions, the original description of the system is presented at the next page.

You've indicated that system 2 does not provide a feature such that 'The user is informed about the type of data that will be collected'. Please reformulate the concerning paragraph in such a way that the system DOES provide this feature:

You've indicated that system 2 provides a feature such that 'The user is informed about the main purpose for which the data will be used'. Please reformulate the concerning paragraph in such a way that the system DOES NOT provide this feature:

You've indicated that system 2 provides a feature such that 'The system only collects data that is relevant to the main purpose of the system'. Please reformulate the concerning paragraph in such a way that the system DOES NOT provide this feature:

You've indicated that system 2 does not provide a feature such that 'The data will be used solely to serve the main purpose of the system'. Please reformulate the concerning paragraph in such a way that the system DOES provide this feature:

You've indicated that system 2 provides a feature such that 'The user is informed about which other parties have access to the collected data'. Please reformulate the concerning paragraph in such a way that the system DOES NOT provide this feature:

Page 4B

You've indicated that system 2 does not provide a feature such that 'The data is securely stored'. Please reformulate the concerning paragraph in such a way that the system DOES provide this feature:

You've indicated that system 2 does not provide a feature such that 'The user can inspect the stored personal data'. Please reformulate the concerning paragraph in such a way that the system DOES provide this feature:

You've indicated that system 2 does not provide a feature such that 'The user has the possibility to make changes in the stored data'. Please reformulate the concerning paragraph in such a way that the system DOES provide this feature:

Original description Health Support System 2:

The system informs John that it will collect data regarding his health, blood pressure, pulse and glucose level. The system does not inform John that data is collected in order to monitor his diabetes condition. The system informs John that it collects also data that is useful for things other than tracking his diabetes condition. The system informs John that it will not use his data for any other reason than the main purpose of the system. The system does not inform John regarding all the organizations or individuals who can access his data. The system informs John that all his data is securely stored. The system provides facilities for John to inspect all data collected about him. The system provides facilities to allow John to modify or erase any data about him.

This was the last page.

Thanks for your participation!

B3. QUESTIONNAIRE OF STUDY 3

Page 1

Evaluation of a Health Support System

This is a small questionnaire about your opinion of a Health Support System.

Imagine the following context:

- John is suffering from diabetes and lives alone with his dog. As long as he controls his sugar intake, he can do whatever he likes. In the past he had some problems to stick to his diet, since he is not that interested in preparing food or cooking.
- Recently, a health-support system, that monitors various health parameters, like blood pressure, weight, pulse and glucose levels, is installed in his house. This system allows John to guard his health and makes it easier to live healthy, since it can also give meal suggestions.
- The system checks John's glucose levels constantly. This helps him to better regulate his diet and also gives him a warning in case of deterioration. This gives John peace of mind, but also supports his doctor.

Aim of the questionnaire

- In this study you will be exposed to two different descriptions of a home-based health-support system. Some system features may be more desirable than others. This is what we want to find out in order to improve the system.
- After each system description you will be asked to indicate whether or not you feel that the system described lives up to some assumptions about it. Each system should be evaluated separately.
- In all, the survey should take no longer than 3-5 minutes.

Page 2

System One

John is checking his diabetes condition using his newly installed health support system that helps him easily and comfortably measure his glucose, blood pressure and pulse. The system does not give a complete breakdown of all of the data that is collected, but informs John that it collects data to monitor his diabetes. He is also assured about the fact that all data collected is necessary for this purpose. In the menu of his health support system, John can see that his data can be used for other purposes as well and shows him a list of people and organizations that may access his data. John is not one of these people. He may not inspect, modify or erase data collected about him. In the same menu, John also finds out that the system does not protect his data with any security safeguards.

Evaluation of the System

Below are some questions about the system you've just read, please circle whether you think the system provides this feature or not:

- The user is informed about the type of data that will be collected Yes / No
- The user is informed about the main purpose for which the data will be used Yes / No
- The system only collects data that is relevant to the main purpose of the system Yes / No
- The data will be used solely to serve the main purpose of the system Yes / No
- The user is informed about which other parties have access to the collected data Yes / No
- The data is securely stored Yes / No
- The user can inspect the stored personal data Yes / No
- The user has the possibility to make changes in the stored data Yes / No

Page 3

System Two

Please watch the video of System Two.

Evaluation of the System

Below are some questions about the system you've just seen, please circle whether you think the system provides this feature or not:

- The user is informed about the type of data that will be collected Yes / No
- The user is informed about the main purpose for which the data will be used Yes / No
- The system only collects data that is relevant to the main purpose of the system Yes / No
- The data will be used solely to serve the main purpose of the system Yes / No
- The user is informed about which other parties have access to the collected data Yes / No
- The data is securely stored Yes / No
- The user can inspect the stored personal data Yes / No
- The user has the possibility to make changes in the stored data Yes / No

B4. QUESTIONNAIRE OF STUDY 4

Screen 1

Evaluation of a Health Support System

This is a small questionnaire about the evaluation of a Health Support System. *The questionnaire is addressed in particular to people with chronic diseases like Heart failure, Diabetes, Chronic Bronchitis and Emphysema (COPD), Asthma or Depression, who may benefit from such a health support system.* [11]

It will take about 15 minutes time to complete this questionnaire.
This questionnaire is only available in English.

If you feel *that you may benefit from a Health Support system, and are* [11] comfortable answering questions in English, we invite you to start the questionnaire by clicking on the button below.

Thanks in advance for your participation.

[Start questionnaire]

Screen 2

Context

A Health Support System may be beneficial to several people with a chronic disease like Heart failure, Diabetes, Chronic Bronchitis and Emphysema (COPD), Asthma or Depression. For the purpose of this questionnaire we will provide you with a context based on a person with diabetes, see the text below.

Imagine the following context:

- John is suffering from diabetes and lives alone with his dog. As long as he controls his sugar intake, he can do whatever he likes. In the past he had some problems to stick to his diet, since he is not that interested in preparing food or cooking.
- Recently, a health support system, that monitors various health parameters, like blood pressure, weight, pulse and glucose levels, is installed in his house. This system allows John to guard his health and makes it easier to live healthy, since it can also give meal suggestions.
- The system checks John's glucose levels constantly. This helps him to better regulate his diet and also gives him a warning in case of deterioration. This gives John peace of mind, but also supports his doctor.

[Next]

[11] These italic parts were removed in later stages of the study in order to allow people without a chronic condition to participate in the study

Screen 3

Aim of the questionnaire

- In this questionnaire you’re exposed to some variations of a health support system like the one installed in John’s house. Some features may be more desirable than others, and this is what we want to find out in order to improve the system.
- You will first read a description of a base scenario. After reading this scenario, you will be provided with two possibilities to adapt the system. Your opinion about the possible adaptation is what we are interested in.

[Next]

Screen 4 - 31

Base Scenario - Health Support System

The system does not inform John that it will collect data regarding his health, blood pressure, pulse and glucose level. The system does not inform John that data is collected in order to monitor his diabetes condition. The system informs John that it also collects data that is useful for things other than tracking his diabetes condition. The system informs John that it uses his data for other reasons than the main purpose of the system as well. The system does not inform John regarding all the organizations or individuals who can access his data. The system informs John that his data is not protected by any security safeguards. The system does not provide facilities for John to inspect all data collected about him. The system does not provide facilities to allow John to modify or erase any data about him.

Possible Adaptation

It would be possible to adapt the system described above. You will be offered 28 pairs of possible adaptations. Could you please indicate for each presented pair which of the two adaptations you would prefer?

Each possible adaptation will replace the corresponding system feature of the base scenario described above. We are interested in knowing what type of adaptation you would prefer as a user of such a Health Support System.

Pair xx of 28
Please indicate which of the two adaptations you would prefer by checking the appropriate box below.

	Preferred adaptation
Description of first possible adaptation	0
OR	
Description of second possible adaptation	0

[Next]

Additional information regarding Screen 4 - 31 [12]

For each screen the participant is offered a pair of adaptations. The counter in the middle of the screen (Pair xx of 28) indicates the number of the pair, so that it is clear to the participant how many questions remain.

Every participant is offered all 28 pairs in random order. The order of adaptations within a pair is alternated, by using Order A and B for every other participant. This takes care of offering each guideline a similar amount of times on the first and on the second place within a pair of adaptations (see table below).

	Order A		**Order B**			**Order A**		**Order B**	
Pair	**1st**	**2nd**	**1st**	**2nd**	**Pair**	**1st**	**2nd**	**1st**	**2nd**
1	MO	IN	IN	MO	**15**	CL	PS	PS	CL
2	PS	OP	OP	PS	**16**	MO	SS	SS	MO
3	CL	UL	UL	CL	**17**	UL	PS	PS	UL
4	SS	DQ	DQ	SS	**18**	IN	SS	SS	IN
5	OP	CL	CL	OP	**19**	CL	MO	MO	CL
6	UL	SS	SS	UL	**20**	DQ	OP	OP	DQ
7	PS	IN	IN	PS	**21**	IN	UL	UL	IN
8	MO	DQ	DQ	MO	**22**	OP	MO	MO	OP
9	SS	OP	OP	SS	**23**	SS	PS	PS	SS
10	DQ	UL	UL	DQ	**24**	DQ	CL	CL	DQ
11	PS	MO	MO	PS	**25**	UL	MO	MO	UL
12	IN	CL	CL	IN	**26**	PS	DQ	DQ	PS
13	OP	UL	UL	OP	**27**	SS	CL	CL	SS
14	DQ	IN	IN	DQ	**28**	OP	IN	IN	OP

Full description of guidelines/adaptations

CL The system informs John that it will collect data regarding his health, blood pressure, pulse and glucose level.

PS The system informs John that data is collected in order to monitor his diabetes condition.

DQ The system informs John about the fact that it will only collect data that is useful for tracking his diabetes condition.

UL The system informs John about the fact that it will not use his data for any other reason than the main purpose of the system.

OP The system informs John regarding all the organizations or individuals who can access his data.

SS The system informs John about the fact that all his data is securely stored.

IN The system provides facilities for John to inspect all data collected about him.

MO The system provides facilities to allow John to modify or erase any data about him.

[12] This information was not provided to participants, but is added to this appendix for clarification.

Screen 32

Additional questions

Could you please indicate for each of the following conditions, whether you are suffering from them or not?

o	Heart failure	Yes / No
o	Diabetes	Yes / No
o	Chronic Bronchitis and Emphysema (COPD)	Yes / No
o	Asthma	Yes / No
o	Depression	Yes / No

Could you please indicate your age by checking the appropriate box below?

o 25 years or younger

o Between 26 and 45

o Between 46 and 65

o 66 years or older

[Next]

Screen 33

THANK YOU!

You have completed the questionnaire.

Thanks for your participation!

Appendix C: Background Models Chapter 4

The table below shows an overview of the background models used in Chapter 4, and the shortened code that will be used to identify each of them in this appendix. The table indicates which elements of the P-Model are included in each background model.

Background model	Code	Trust	Risk / Concern	Usefulness	Ease	Intention to use
Chellappa & Sin (2005)	Chel05	●	●	●		●
Corritore et al. (2005)	Cor05	●	●		●	
Dinev & Hart (2003)	Din03					
Dinev & Hart (2006)	Din06	●	●			●
Featherman & Pavlou (2003)	Fea03		●	●	●	●
Lui & Jamieson (2003)	Lui03	●	●	●	●	●
Malhotra et al. (2004)	Mal04	●	●			●
Suh & Han (2002)	Suh02	●		●	●	●

Code	Trust	Scale	Scale anchors
Che05	I am familiar with the Web site(s) of (names of firms).		
Che05	I have previously used or purchased services or products from (names of firms).		
Cor05	I expect this website will not take advantage of me.	Likert	
Cor05	I believe this website is trustworthy.	Likert	
Cor05	I believe this website will not act in a way that harms me.	Likert	
Cor05	I trust this website.	Likert	
Din03	Internet websites are secure environments in which to conduct financial and business transactions.	5 point Likert	
Din03	Internet websites are reliable environments in which to conduct business transactions.	5 point Likert	
Din03	Internet websites are reliable places to exchange information with others.	5 point Likert	
Din06	Rate the extent to which you agree with the following statement: Internet websites are safe environments in which to exchange information with others.	5 point Likert	Strongly disagree–Strongly agree
Din06	Rate the extent to which you agree with the following statement: Internet websites are reliable environments in which to conduct business transactions.	5 point Likert	Strongly disagree–Strongly agree
Din06	Rate the extent to which you agree with the following statement: Internet websites handle personal information submitted by users in a competent fashion.	5 point Likert	Strongly disagree–Strongly agree
Lui03	*(Various construct for facets of Trust)*		
Mal04	I trust that online companies would keep my best interests in mind when dealing with (the information).	7 point	Strongly disagree–Strongly agree
Mal04	Online companies are in general predictable and consistent regarding the usage of (the information).	7 point	Strongly disagree–Strongly agree
Mal04	Online companies are always honest with customers when it comes to using (the information) that I would provide.	7 point	Strongly disagree–Strongly agree
Suh02	This Internet banking site is trustworthy	Likert	Strongly disagree–Strongly agree
Suh02	I trust in the benefits of the decisions of this Internet banking site	Likert	Strongly disagree–Strongly agree
Suh02	This Internet banking site keeps its promises and commitments	Likert	Strongly disagree–Strongly agree
Suh02	This Internet banking site keeps customers' best interests in mind	Likert	Strongly disagree–Strongly agree
Suh02	This Internet banking site would do the job right even if not monitored	Likert	Strongly disagree–Strongly agree
Suh02	I trust this Internet banking site	Likert	Strongly disagree–Strongly agree

Code	Risk / Concern	Scale	Scale anchors
Che05	I am sensitive about giving out information regarding my preferences	7 point Likert	Strongly disagree–Strongly agree
Che05	I am concerned about anonymous information (information collected automatically but cannot be used to identify me, such as my computer, network information, operating system, etc.) that is collected about me.	7 point Likert	Strongly disagree–Strongly agree
Che05	I am concerned about how my personally un-identifiable information (information that I have voluntarily given out but cannot be used to identify me, e.g., Zip Code, age-range, sex, etc.) will be used by the firm.	7 point Likert	Strongly disagree–Strongly agree
Che05	I am concerned about how my personally identifiable information (infor-mation that I have voluntarily given out AND can be used to identify me as an individual, e.g., name, shipping address, credit card or bank ac-count information, social security number, etc.) will be used by the firm.	7 point Likert	Strongly disagree–Strongly agree
Cor05	I feel vulnerable when I interact with this website.	Likert	
Cor05	I believe that there could be negative consequences from using this website.	Likert	
Cor05	I am taking a chance interacting with this website.	Likert	
Cor05	I feel it is unsafe to interact with this website.	Likert	
Cor05	I feel that the risks outweigh the benefits of using this website.	Likert	
Cor05	I feel I must be cautious when using this website.	Likert	
Cor05	It is risky to interact with this website.	Likert	
Din03	I am concerned that a person can find private information about me on the Internet	5 point Likert	
Din03	I am concerned about submitting information on the Internet, because of what others might do with it.	5 point Likert	
Din03	I am concerned about submitting information on the Internet, because it could be used in a way I did not foresee.	5 point Likert	
Din06	What do you believe is the risk for regular Internet users due to the possibility that: Records of transactions could be sold to third parties?	5 point Likert	Very low risk–Very high risk
Din06	What do you believe is the risk for regular Internet users due to the possibility that: Personal information submitted could be misused?	5 point Likert	Very low risk–Very high risk
Din06	What do you believe is the risk for regular Internet users due to the possibility that: Personal information could be made available to unknown individuals or companies without your knowledge?	5 point Likert	Very low risk–Very high risk
Din06	What do you believe is the risk for regular Internet users due to the possibility that: Personal information could be made available to government agencies?	5 point Likert	Very low risk–Very high risk

Code	Risk / Concern	Scale	Scale anchors
Din06	Indicate the extent to which you are concerned about the following: I am concerned that the information I submit on the Internet could be misused.	5 point Likert	Not at all concerned–Very concerned
Din06	Indicate the extent to which you are concerned about the following: I am concerned that a person can find private information about me on the Internet.	5 point Likert	Not at all concerned–Very concerned
Din06	Indicate the extent to which you are concerned about the following: I am concerned about submitting information on the Internet, because of what others might do with it.	5 point Likert	Not at all concerned–Very concerned
Din06	Indicate the extent to which you are concerned about the following: I am concerned about submitting information on the Internet, because it could be used in a way I did not foresee.	5 point Likert	Not at all concerned–Very concerned
Fea03	On the whole, considering all sorts of factors combined, about how risky would you say it would be to sign up for and use XXXX?	7 point semantic differential	Not risky at all / Very risky
Fea03	Using XXXX to pay my bills would be risky.	7 point Likert	Strongly disagree–Strongly agree
Fea03	XXXX are dangerous to use.	7 point Likert	Strongly disagree–Strongly agree
Fea03	Using XXXX would add great uncertainty to my bill paying.	7 point Likert	Strongly disagree–Strongly agree
Fea03	Using XXXX exposes you to an overall risk.	7 point semantic differential	Improbable - Probable
Lui03	Overall, I am concerned about experiencing some kind of loss if I transact with this system.	7 point	
Lui03	All things considered, I think I would be making a mistake if I use this system to make a transaction.	7 point	
Lui03	Transacting with the online system would pose problems for me that I just don't need.	7 point	
Lui03	How would you characterise the decision of whether to transact with this system?	7 point	Very insignificant risk - Very significant risk
Lui03	How would you characterise the decision of whether to transact with this system?	7 point	Very positive situation - Very negative situation
Lui03	How would you characterise the decision of whether to transact with this system?	7 point	Very high potential for gain - Very high potential for loss
Mal04	Compared to others, I am more sensitive about the way online companies handle my personal information.	7 point	Strongly disagree–Strongly agree
Mal04	To me, it is the most important thing to keep my privacy intact from online companies.	7 point	Strongly disagree–Strongly agree
Mal04	I am concerned about threats to my personal privacy today.	7 point	Strongly disagree–Strongly agree

Code	Risk / Concern	Scale	Scale anchors
Mal04	In general, it would be risky to give (the information) to online companies.	7 point	Strongly disagree–Strongly agree
Mal04	There would be high potential for loss associated with giving (the information) to online firms.	7 point	Strongly disagree–Strongly agree
Mal04	There would be too much uncertainty associated with giving (the information) to online firms.	7 point	Strongly disagree–Strongly agree
Mal04	Providing online firms with (the information) would involve many unexpected problems.	7 point	Strongly disagree–Strongly agree

Code	Usefulness / Value	Scale	Scale anchors
Che05	I value Web pages that are personalized for the device (e.g. computer, palm, mobile phone etc.), browser (e.g. Netscape, Internet explorer) and operating system (e.g. Windows, Unix) that I use.	7 point Likert	Strongly disagree–Strongly agree
Che05	I value Web sites that are personalized for my usage experience preferences	7 point Likert	Strongly disagree–Strongly agree
Che05	I value Web sites that acquire my personal preferences and personalize the services and products themselves	7 point Likert	Strongly disagree–Strongly agree
Che05	I value goods and services that are personalized based on information that is collected automatically (such as IP address, pages viewed, access time) but cannot identify me as an individual.	7 point Likert	Strongly disagree–Strongly agree
Che05	I value goods and services that are personalized on information that I have voluntarily given out (such as age range, salary range, Zip Code) but cannot identify me as an individual.	7 point Likert	Strongly disagree–Strongly agree
Che05	I value goods and services that are personalized on information I have voluntarily given out and can identify me as an individual (such as name, shipping address, credit card information).	7 point Likert	Strongly disagree–Strongly agree
Fea03	*(Pre-validated TAM measures)*		
Lui03	Using the system improves my performance in my purchasing.	7 point	
Lui03	Using the system increases my productivity in purchasing.	7 point	
Lui03	Using the system enhances my effectiveness in purchasing.	7 point	
Lui03	I find the system to be useful in my purchasing.	7 point	

Code	Usefulness / Value	Scale	Scale anchors
Suh02	Using this Internet banking site enhances the productivity of my banking activities	Likert	Strongly disagree–Strongly agree
Suh02	Using this Internet banking site has a critical role in supporting my banking activities	Likert	Strongly disagree–Strongly agree
Suh02	Using this Internet banking site makes it easier to do my banking activities	Likert	Strongly disagree–Strongly agree
Suh02	Using this Internet banking site enables me to accomplish banking activities more quickly	Likert	Strongly disagree–Strongly agree
Suh02	Using this Internet banking site improves my performance of banking activities	Likert	Strongly disagree–Strongly agree
Suh02	I find this Internet banking site useful for my banking activities	Likert	Strongly disagree–Strongly agree

Code	Ease of use	Scale	Scale anchors
Che05	I value Web pages that are personalized for the device (e.g. computer, palm, mobile phone etc.), browser (e.g. Netscape, Internet explorer) and operating system (e.g. Windows, Unix) that I use.	7 point Likert	Strongly disagree–Strongly agree
Che05	I value goods and services that are personalized based on information that is collected automatically (such as IP address, pages viewed, access time) but cannot identify me as an individual.	7 point Likert	Strongly disagree–Strongly agree
Che05	I value goods and services that are personalized on information that I have voluntarily given out (such as age range, salary range, Zip Code) but cannot identify me as an individual.	7 point Likert	Strongly disagree–Strongly agree
Che05	I value goods and services that are personalized on information I have voluntarily given out and can identify me as an individual (such as name, shipping address, credit card information).	7 point Likert	Strongly disagree–Strongly agree
Fea03	*(Pre-validated TAM measures)*		
Lui03	Learning to operate the system will be easy for me.	7 point	
Lui03	I find it easy to get the system to do what I want it to do.	7 point	
Lui03	It is easy for me to become skilful at using the system.	7 point	
Lui03	I find the system easy to use.	7 point	
Suh02	It is easy for me to learn how to utilize this Internet banking site	Likert	Strongly disagree–Strongly agree
Suh02	I find it easy to get this Internet banking site to do what I want it to do	Likert	
Suh02	It is easy to remember how to use this Internet banking site	Likert	
Suh02	My interaction with this Internet banking site is clear and understandable	Likert	

Code	Intention to use	Scale	Scale anchors
Din03	Internet usage for: Purchase goods (e.g., books or CDs) or services (e.g., airline tickets or hotel reservations) from websites that require me to submit accurate and identifiable information (i.e., credit card information).	5 point Likert	
Din03	Internet usage for: Retrieve information from websites that require me to submit accurate and identifiable registration information, possibly including credit card information (e.g., using sites that provide personalized stock quotes, insurance rates, or loan rates; or using sexual or gambling websites).	5 point Likert	
Din03	Internet usage for: Conduct sales transactions at e-commerce sites that require me to provide credit card information (e.g., using sites for purchasing goods or software).	5 point Likert	
Din03	Internet usage for: Retrieve highly personal and password protected financial information (e.g., using websites that allow me to access my bank account or my credit card account).	5 point Likert	
Din06	To what extent are you willing to use the Internet to: Purchase goods (e.g., books or CDs) or services (e.g., airline tickets or hotel reservations) from websites that require me to submit accurate and identifiable information (i.e., credit card information)	5 point Likert	Not at all–Very much
Din06	To what extent are you willing to use the Internet to: Retrieve information from websites that require me to submit accurate and identifiable registration information, possibly including credit card information (e.g., using sites that provide personalized stock quotes, insurance rates, or loan rates; or using sexual or gambling websites)	5 point Likert	Not at all–Very much
Din06	To what extent are you willing to use the Internet to: Conduct sales transactions at e-commerce sites that require me to provide credit card information (e.g., using sites for purchasing goods or software)	5 point Likert	Not at all–Very much
Din06	To what extent are you willing to use the Internet to: Retrieve highly personal and password-protected financial information (e.g., using websites that allow me to access my bank account or my credit card account)	5 point Likert	Not at all–Very much
Fea03	*(Pre-validated TAM measures)*		

Code	Intention to use	Scale	Scale anchors
Lui03	Assuming I have access to the system, I intend to use it.	7 point	
Lui03	Given that I have access to the system, I predict that I would use it.	7 point	
Lui03	It is likely that I will transact with this system in the near future.	7 point	
Mal04	Given this hypothetical scenario, specify the extent to which you would reveal (the information) through the Internet.	7 point semantic	Unlikely - likely
Mal04	Given this hypothetical scenario, specify the extent to which you would reveal (the information) through the Internet.	7 point semantic	Not probable - Probable
Mal04	Given this hypothetical scenario, specify the extent to which you would reveal (the information) through the Internet. [r]	7 point semantic	Willing - Unwilling
Suh02	Using this Internet banking site is a good idea	Likert	Strongly disagree–Strongly agree
Suh02	Using this Internet banking site is a wise idea	Likert	Strongly disagree–Strongly agree
Suh02	Using this Internet banking site is a pleasant idea	Likert	Strongly disagree–Strongly agree
Suh02	Using this Internet banking site is a positive idea	Likert	Strongly disagree–Strongly agree
Suh02	Using this Internet banking site is an appealing idea	Likert	Strongly disagree–Strongly agree
Suh02	I intend to continue using this Internet banking site in the future	Likert	Strongly disagree–Strongly agree
Suh02	I expect my use of this Internet banking site to continue in the future	Likert	Strongly disagree–Strongly agree
Suh02	I will frequently use this Internet banking site in the future	Likert	Strongly disagree–Strongly agree
Suh02	I will strongly recommend others to use this Internet banking site	Likert	Strongly disagree–Strongly agree

Appendix D: Questionnaire Chapter 4

D1. INTRODUCTION & MEASURE 1: GENERAL BACKGROUND DATA

Introduction

Introduction to the study: The evaluation of Interfaces for managing privacy preferences

Thank you for your interest to participate in this study on the evaluation of interfaces for managing privacy preferences. In this study you will be using three different interfaces that allow you to set preferences with regard to the disclosure of information. The study consists of four different sections. In some sections you will only be answering questions; in others you will also be using some interfaces. We would like to know your opinion about each of these interfaces.

We are interested in your opinion, so there are no wrong or right answers. Anything you will do or say will be valuable to us, as this will give us input on how to improve interfaces like the ones in this study in the future.

There will be breaks scheduled in between the sections, however, if at any point in time you need a break or you want to quit your participation then please inform the experimenter.

As you see, the screen is made up out of two different parts. The main part, where this text is positioned is the most important part. In this part you will be given explanations, asked questions to answer or shown interfaces to use. The top part of the screen displays on the left side exactly in which section of the study and on which page you are.

Throughout the study whenever you press the 'Next' button, please allow some time for the next page to be loaded in your browser.

Please press the 'Next' button below, to start the study.

Section 1 - Page 1/3

Before you will actually be using the various interfaces, we would like to ask a few questions about your background, such as demographics and your experience with technology. Please complete each of the following questions:

General demographics *(GVU's tenth WWW User Survey)* [13]

Sex	What is your gender?	○ Female *(F)* ○ Male *(M)*
Age	What is your age?	*(open field for 2 numbers - required)*
Edu	Please indicate the highest level of education you have completed	○ Grammar School *(1)* ○ High School or equivalent *(2)* ○ Vocational/Technical School (2 year) *(3)* ○ Some College *(4)* ○ College Graduate (4 year) *(5)* ○ Master's Degree (MS) *(6)* ○ Doctoral Degree (PhD) *(7)* ○ Professional Degree (MD, JD, etc.) *(8)*

[13] Italic sections were not provided to participants, but are added to this appendix for clarification.

Experience with technology *(GVU's tenth WWW User Survey)*

WebUse	How long have you been using the Internet?	○ Less than 6 months *(1)* ○ 6 to 12 months *(2)* ○ 1 to 3 years *(3)* ○ 4 to 6 years *(4)* ○ 7 years or more *(5)*
ComTech	Which of the following technologies do you use to communicate with others on a routine basis? (please check all that apply)	○ Fax *(1)* ○ Email *(2)* ○ Wired phone (including cordless) *(3)* ○ Cellular phone *(4)* ○ Pagers *(5)* ○ Voice mail *(6)* ○ Postal mail *(7)* ○ Other *(8)*
WebTech	Which of the following Internet specific technologies have you used in the past year? (please check all that apply)	○ Chat/Online discussion *(1)* ○ Internet phone *(2)* ○ Internet fax *(3)* ○ "Push" technologies (Pointcast, Castanet, Channels, etc.) *(4)* ○ Streaming audio over the Internet (Real Audio, etc.) *(5)* ○ Video conferencing over the Internet (Netmeeting, etc.) *(6)* ○ Digital signature/id cards (Verisign, RSA. etc.) *(7)* ○ 3-D environments (VRML, Active 3D, etc.) *(8)* ○ Viewed a web page containing Java/JavaScript *(9)* ○ Other technologies *(10)* ○ None of the above *(11)*

Section 1 - Page 2/3

Personality traits *(S. Gosling)*

Here are a number of personality traits that may or may not apply to you. Please indicate for each statement the extent to which you agree or disagree with that statement. You should rate the extent to which the pair of traits applies to you, even if one characteristic applies more strongly than the other.

	I see myself as:	1 = Disagree strongly
Tip1	○ Extraverted, enthusiastic	2 = Disagree moderately
Tip2	○ Critical, quarrelsome	3 = Disagree a little
Tip3	○ Dependable, self-disciplined	4 = Neither agree nor disagree
Tip4	○ Anxious, easily upset	5 = Agree a little
Tip5	○ Open to new experiences,	6 = Agree moderately
Tip6	complex	7 = Agree strongly
Tip7	○ Reserved, quiet	
Tip8	○ Sympathetic, warm	
Tip9	○ Disorganized, careless	
Tip10	○ Calm, emotionally stable	
	○ Conventional, uncreative	

TIPI scoring ("R" = reverse-scored): Take the AVERAGE of the two items (the standard item and the recoded reverse-scored item) that make up each scale. Extraversion: 1, 6R; Agreeableness: 2R, 7; Conscientiousness; 3, 8R; Emotional Stability: 4R, 9; Openness to Experiences: 5, 10R.

Section 1 - Page 3/3

Privacy concern *(Harris Interactive)*

Please indicate for each of the following statements, the extent to which you agree or disagree with that statement.

PSI1 Consumers have lost all control over how personal information is collected and used by companies.

PSI2 Most businesses handle the personal information they collect about consumers in a proper and confidential way

PSI3 Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today

○ Strongly disagree *(1)*
○ Somewhat disagree *(2)*
○ Somewhat agree *(3)*
○ Strongly agree *(4)*

Fundamentalists agree (strongly or somewhat) with PSI1 and disagree (strongly or somewhat) with PSI2 & 3. Unconcerned disagree with PSI1 and agree with PSI2 & 3. Pragmatists give any other response combination.

D2. MEASURE 2: EVALUATION SCENARIOS

Section 2 - Introduction

Situations for managing privacy preferences

In this section of the study we will provide you with some situations in which you may feel the need to manage the disclosure of your personal information. Six different situations will be provided to you.

First, please read the introductory text below.

Linda Brown, 41, is married to John. They have two children, Juliet of 16 and Sam of 13 year-old. They recently moved to a new so-called smart house which is equipped with all kinds of technology to make life easy. Linda is in the process of letting her house know her preferences with regard to allowing and prohibiting disclosure of information.

Bob Conner is a 25-year old law-student. He lives with four other students in a house on campus. Bob got a new cell phone for his birthday last week, and he wants to set it up and connect it to his smart living environment.

You will now be provided with a description of six situations concerning Linda or Bob and how they try to adapt what the system does. Imagine yourself confronted with such a system and execute the tasks with your own situation in mind.

Section 2 - Page 1/11 - Scenario 1

Situations for managing privacy preferences

Please read the text of the first situation, shown below.

Bob's cell phone has a camera, which he uses to take pictures where-ever he goes. The camera makes use of a new service that helps him automatically share his pictures with friends or family, and his own photo-collection stored at his PC back home. More than this, pictures are automatically annotated with information regarding the time and location where they were taken.
Bob really appreciates this automatically sharing of pictures since it saves him a lot of trouble searching for the right pictures, adding context information and then sending them to some of his relatives. Also, he enjoys using the location and time information to find pictures in his collection. On the other hand, he feels it maybe somewhat risky if his parents get to see all the pictures from his last holiday with his mates.

Task:
You may want to share your pictures with some people who are close to you to share your experiences. However, there may be some people whom you don't want to have access to your pictures. You may want to have your pictures available on other devices, to be able to view them from other places or in other modes as well, or maybe you prefer to keep them on your cell phone. Maybe you want your pictures only to be used for certain purposes. Possibly you want the additional time and location information only to be accessible by some people or for some purposes.
Please take some time to think about this situation.

[*Button:* NEXT]
At the bottom of each scenario a 'Next" button is displayed, only when this button is pressed, the scenario questions will be shown (see paragraph after scenario 5).

Section 2 - Page 2/11 - Scenario 2

Situations for managing privacy preferences

Now, please read the text of the second situation, shown below.

Linda Brown goes shopping at the local mall. These days, shopping is very efficient: products are labeled with special tags that are detected as she put them in her shopping trolley. She no more has to queue at the check out: her credit card is charged automatically as she pushes the trolley out of the mall. One of the facilities of the shop that you can opt to use, is to receive suggestions for items to purchase as you walk along: this is usually items she has bought on other occasions and if not, promotions that seem to fit her shopping pattern. Linda is aware that the shop keeps records of what she buys every week and some computer makes suggestions to match these records. As her trolley attempts to attract her attention to a specific item she notices another woman whose trolley suggests real junk food, she would never buy for her family. As she walks out of the store, she receives suggestions for other services offered by her supermarket chain: these are of all kinds, financial, holidays and medical services.

Task:
You may want to allow the use of smart tags by some shops or devices, but not by others. Maybe you want the smart tags only to be used for particular purposes.
Please take some time to think about this situation.

[*Button:* NEXT]

Section 2 - Page 3/11 - Scenario 3

Situations for managing privacy preferences

Now, please read the text of the third situation, shown below.

On the campus where Bob lives there is a location tracking network. This is meant for students to help find their friends or teachers. Also, in some parts of town the system is working. In some occasions Bob thinks it is desirable that other people can trace him, sometimes, however, he prefers to be ‘hidden’. Bob uses this feature when he does not know which classroom he should be going to or to check different locations before he goes, to avoid bumping into some colleagues of his that he does not get on with. During the various appointments he makes during the day, the tracking facility helps Bob and his friends coordinate: they wait for him when he is slightly delayed, he can catch up with them if they move on to the next place without him.

Task:
You may want to allow the use of location information by some persons, but not by others. Maybe you want your location information only to be used for particular purposes.
Please take some time to think about this situation.

[*Button:* NEXT]

Section 2 - Page 4/11 - Scenario 4

Situations for managing privacy preferences

Now, please read the text of the fourth situation, shown below.

Juliet and Sam want to surprise their mother with a nice movie. Lately, their mother has been very busy and they feel she needs a break. They want to use their mother’s personal movie record to buy and download a movie over the internet. The question is whether they have full access to her movie record, or whether Linda has blocked some of her personal favorites for her children. The personal favorites list consists of all movies and TV programs watched, as well as all websites visited. This information can be used by the smart house to recommend new programs or websites that maybe interesting to Linda.

Task:
You may want to allow the use of your movie record by some persons, but not by others. And perhaps you like all possible devices in your house to be able to access your record or not. Maybe you want your movie record only to be available for particular purposes.
Please take some time to think about this situation.

[*Button:* NEXT]

Section 2 - Page 5/11 - Scenario 5

Situations for managing privacy preferences

Now, please read the text of the fifth situation, shown below.

Linda's house also monitors some medical parameters for her, such as heart rate, blood pressure, weight, and mood information. This information may be used by several parties, and for several purposes. E.g. her family doctor can decide to prescribe alternative medication if some parameters indicate change is needed.

Task:
You may want to allow the use of your medical data by some persons, but not by others. And perhaps you like everyone in your house to be able to access your medical record or not. Maybe you want your medical data only to be available for particular purposes.
Please take some time to think about this situation.

[*Button:* NEXT]

Section 2 - Appears at bottom of Pages 1-5/11 - Scenario Questions

At the bottom of each scenario a 'Next" button is displayed, only when this button is pressed, the following scenario questions will be shown.

Evaluation Situation

Now, you will be asked 3 questions about the situation you have just read. Please complete the questions below:

Famil1…n	To what extent do you feel that the described situation could be realistic for you?	○ Not at all realistic *(1)* ○ *(2)* ○ *(3)* ○ *(4)* ○ *(5)* ○ *(6)* ○ Extremely realistic *(7)*
ConcS1…n	Now imagine that you are in such a situation yourself. Please indicate to what extent you would be concerned about your privacy.	○ Not at all concerned *(1)* ○ *(2)* ○ *(3)* ○ *(4)* ○ *(5)* ○ *(6)* ○ Extremely concerned *(7)*

Please describe concisely what would be your two main concerns when being in such a situation as described before:

TopConcS1…n (open field for text)

Section 2 - Page 6/11

General Evaluation

Before you were asked to evaluate each of the situations separately, but now please imagine that you are living in an environment where the same technologies that are available to Linda and Bob, are available to you.

Please indicate for each statement below to what extent you agree or disagree with that statement for such an environment:

Ris1	I would feel vulnerable being in such an environment.
Ris2	I would believe that there could be negative consequences from being in such an environment.
Ris3	I would be taking a chance being in such an environment.
Ris4	I would feel it is unsafe to be in such an environment.
Ris5	I would feel that the risks outweigh the benefits of being in such an environment.
Ris6	I would feel I must be cautious when being in such an environment.
Ris7	It would be risky to be in such an environment.

○ Strongly disagree *(1)*
○ *(2)*
○ *(3)*
○ *(4)*
○ *(5)*
○ *(6)*
○ Strongly agree *(7)*

D3. MEASURE 3: SEPARATE EVALUATION INTERFACES

Section 2 - Page 7/11

First use of interfaces – *Personal Aims*

Now you will use three different interfaces that allow you to set your preferences with regard to the disclosure of information. These interfaces differ from each other in the way that preferences can be specified. Your task is to explore each interface and to adjust its settings in an attempt to minimize any concerns you may have about the disclosure of information in light of the six situations that were presented to you before.

Please note that it may take some time before the interface is fully loaded.

Section 2 - Page 8-10/11

Please explore this first/second/last interface and adjust its settings in an attempt to minimize any concerns you may have about the disclosure of information in light of the six situations that were presented to you before and briefly described below.

- Automatically sharing annotated pictures
- Easy shopping due to product tags, automatic payment & product suggestions
- Location tracking
- Personal movie/TV record
- Health monitoring

At the bottom of the page the appropriate interface is displayed including its title.

Section 2 - Page 11/11

Evaluation first use of interfaces - *Personal Aims*

You have used three different interfaces for setting your privacy preferences in an attempt to minimize your concerns.

Please indicate for each interface below to what extent you felt more or less concerned after the actual use of that interface compared to before.

[PICTURE & NAME OF INTERFACE ARE SHOWN]

After using Interface [UI1…n] I felt:

ConcUI1…n
○ Very much less concerned than before *(1)*
○ *(2)*
○ *(3)*
○ *(4)*
○ *(5)*
○ *(6)*
○ Very much more concerned than before *(7)*

Break

This would be a good moment for you to have a little break. Please feel free to take a cup of coffee or tea.

Please remember to keep your browser open.

Section 3 - Introduction

Second use of interfaces – *Pre-specified Aims*

Now you will use each of the three different interfaces again. This time your task is somewhat different than before. You will be asked to make three different kinds of settings with each interface. After making all three settings with one interface, you will move to the next interface.

Please carefully read the information provided next to each interface, since it will contain detailed instructions about specific settings you're asked to make with that interface.

Please note that some parts of a task may not require you to fill out all elements of an interface or may not require any action at all.

Section 3 - Page 1-3/4

Second use of interfaces

Please carefully read the instructions provided below and set the interface in order to match the instructions as good as possible.

[Interfaces will be used in randomized order between participants. Each participant will perform all three tasks with one interface, and then move to the next interface. To make comparison of tasks easier, below each task is presented for all three interfaces, before the next task is presented. Since, the focus is on the evaluation of the interface and not the tasks themselves, it is decided not randomize the order in which the tasks are presented.]

Task 1 - Profiles
You are participating in a health-monitoring program that allows various people, like your doctor or insurance company, to have remote access to your personal information while you are able to stay at home.
In the light of this program you decide to make all of the following settings:

- You want your home doctor to have access to precise information regarding your cholesterol and bank account number for insurance coverage.
- You want your home doctor to have access to vague information regarding your heart rate and blood pressure.
- You do not want your employer to get access to your cholesterol and blood pressure.
- You do not want your insurance company to get access to any of the data mentioned above for identifying high-risk people.

Task 1 - Split
You are participating in a health-monitoring program that allows various people, like your doctor or insurance company, to have remote access to your personal information while you are able to stay at home.
In the light of this program you decide to make all of the following settings:

- You want your home doctor to receive precise data.
- You do not want your weight cholesterol, or heart rate information to be available.
- You want to allow precise data to be available for insurance coverage.
- You do not want your information to be available for marketing purposes.

Task 1 - Custom4
You are participating in a health-monitoring program that allows various people, like your doctor or insurance company, to have remote access to your personal information while you are able to stay at home.
In the light of this program you decide to make all of the following settings:

- You want your medical information to be available for insurance coverage.
- You do not want your medical information to be used for identifying people at high-risk for specific health problems, or for marketing purposes.
- You do not want your entertainment information to be used to decide about future health care services.
- You want your financial information to be used for insurance coverage.

Task 2 - Profiles
You are using a cell phone that allows others to track your location.
In the light of this feature you decide to make all of the following settings:

- You do not want your location data to be available to your employer.
- You do not want your location data to be available to anyone for personal contents/ads, or to identify high-risk people for specific health problems.
- You want your precise location data to be available to emergency personnel for any circumstance.
- You want your precise location data to be available to receive immediate health care.

Task 2 - Split
You are using a cell phone that allows others to track your location.
In the light of this feature you decide to make all of the following settings:

- You do not want your employer to get any data.
- You want your precise location data to be available to emergency personnel.
- You do not want your data to be used for personal contents/ads.
- You want your precise location data to be available to receive immediate health care.

Task 2 - Custom4
You are using a cell phone that allows others to track your location.
In the light of this feature you decide to make all of the following settings:

- You do not want your location data to be available to anyone to determine your habits, interests, or other characteristics.
- You do want your location data to be available to interest you in other products or services.
- You do not want your location data to be available for sharing with other companies.
- You want your location data to be available for personal communication.

Task 3 - Profiles
You are using a mobile device that allows you to automatically share pictures, messages and location information.
In the light of this device you decide to make all of the following settings:

- You want your personally created pictures to be accessible in the most precise level to all family related persons.
- You do not want your employer to get access to your pictures and text messages.
- You want your approximate location information to be available to your spouse.
- You do not want your pictures and text messages to be used for determining the suitability for a job, or to make future health care decisions.

Task 3 - Split

You are using a mobile device that allows you to automatically share pictures, messages and location information.

In the light of this device you want to make all of the following settings:

- You want your personally created pictures to be accessible in the rough level to others.
- You do not want your employer to get access to any of your information.
- You want your rough location information to be available.
- You do not want the information to be used for determining the suitability for a job, or to make future health care decisions.

Task 3 - Custom4

You are using a mobile device that allows you to automatically share pictures, messages and location information.

In the light of this device you want to make all of the following settings:

- You want your personally created pictures and text messages to be available for personal communication.
- You do not want your location information to available to anyone to determine your habits, interests, or other characteristics.
- You do not want the personally created information to be used for determining the suitability for a job, or to make future health care decisions.
- You want to share your text messages with other parties in order to get better services.

Section 3 - Page 4/4

Evaluation second use of interfaces

Please indicate for each of the interfaces below to what extent you felt that it was easy or difficult to make the required settings with that interface.

[PICTURE & NAME OF INTERFACE ARE SHOWN]

Making the required settings with Interface [UI1…n] was:

SubExprUI1…n

○ Extremely easy *(1)*
○ *(2)*
○ *(3)*
○ *(4)*
○ *(5)*
○ *(6)*
○ Extremely difficult *(7)*

Break

This would be a good moment for you to have a little break. Please feel free to take a cup of coffee or tea.

Please remember to keep your browser open.

D4. MEASURE 4: PAIRED EVALUATION INTERFACES

Section 4A - Introduction

Overall difference

You have just used 3 different interfaces for setting your own privacy preferences and for some additional tasks. We would like to know your opinion about each interface on several aspects.

First, you will be asked to compare two interfaces at a time and to evaluate the extent to which these interfaces are different from each or other or equal to each other taken all possible factors into account.

For each comparison, please note which interfaces are involved. The names and screenshots of the interfaces you're supposed to compare are provided.

Section 4A - Page 1-3/3

Overall difference

[PICTURES & NAMES OF EACH PAIR OF INTERFACES ARE SHOWN]

Overall, taken all things into account, to what extent do you feel that the two interfaces shown below are different from each other?

Dif UIy UIx…n 5. Extremely different
4.
3.
2.
1.
0. Not at all different

[This question is repeated for all three pairs of interfaces in random order]

Section 4B - Introduction Page 1/3

Evaluation of Interfaces

You have just evaluated the extent to which the 3 interfaces are different from each other or equal to each other taking all possible factors into account. Now, we will like to know your opinion about each interface on several particular aspects.

You will be asked to compare two interfaces at a time with regard to a particular statement. Please compare the two interfaces on the basis of the statement provided and decide to what extent the interfaces differ.

For each comparison, please note what statement and which interfaces are involved. The names and screenshots of the interfaces you're supposed to compare are provided.

Even though the current question seems quite similar to the previous question, the answering scale is quite different. Therefore, we will give you some information about how to use the answering scale for the current set of questions and provide two examples as well.

How to use the answering scale:

- If you feel that there is no difference between the two interfaces with regard to the statement provided, then select the middle option of the answering scale "Equally applicable".
- If you feel that there is a difference between the two interfaces with regard to the statement provided, then decide to what extent you feel that the statement is more applicable to one interface in comparison to the other. Select one of the three options of the answering scale beneath the most applicable interface to indicate the extent to which you feel that the statement is more applicable to that particular interface in comparison to the other.

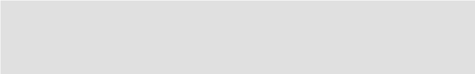
Section 4B - Introduction Page 2/3

Example 1

Please compare the two interfaces shown below on the basis of the following statement:

This interface is yellow

Please indicate to what extent you feel that the statement is more applicable to one interface in comparison to the other or whether you feel that the statement is equally applicable to both interfaces.

	Interface X				Interface Y	
						
(-3)	*(-2)*	*(-1)*	*(0)*	*(-1)*	*(-2)*	*(-3)*
Strongly	Moderately	Slightly	Equally	Slightly	Moderately	Strongly
… more applicable to interface on left			applicable	… more applicable to interface on right		

Answer
Since there is not much difference in the extent to which these interfaces are (not) yellow, they could be considered equally yellow, and so the answer "Equally applicable" (middle option) will reflect the comparison best.

Section 4B - Introduction Page 3/3

Example 2

Please compare the two interfaces shown below on the basis of the following statement:

<u>This interface is black</u>

Please indicate to what extent you feel that the statement is more applicable to one interface in comparison to the other or whether you feel that the statement is equally applicable to both interfaces.

Interface Z Interface X

(-3)	(-2)	(-1)	(0)	(1)	(2)	(3)
Strongly	Moderately	Slightly	Equally	Slightly	Moderately	Strongly
… more applicable to interface on left			applicable	… more applicable to interface on right		

Answer

Both interfaces are black to some extent; however there is a difference in blackness between the two interfaces. Z is probably regarded more black than interface X. Thus, one of the options on the left side of the answering scale beneath interface Z will reflect the comparison best. The actual option you choose (“Strongly”, “Moderately”, or “Slightly”) will depend on the extent to which you feel that Interface Z is more black than interface X. Please note that if the statement to compare the interfaces on was “This interface is white”, then one of the three options on the right side of the scale would best reflect the comparison indicating that Interface X is considered to be whiter than interface Z.

Next task

Now, you will be asked to compare three pairs of interfaces on the basis of 22 different statements.

Popup – After examples

You are about to start the evaluation of the first pair of interfaces.

Section 4B - Page 1-22/22 - For each pair

[PICTURES & NAMES OF EACH PAIR OF INTERFACES ARE SHOWN]

Please compare the two interfaces on the basis of the statement shown below:

[First, one pair of interfaces is compared on the basis of all 22 statements in randomized order. Then the same order of statements is used for the comparison of the second and third pair of interfaces.]

1 *Tru4* I trust this profile manager.

2 *Ris1* I feel vulnerable when I interact with this profile manager.

3 *Val1* Using this profile manager improves my performance to use personalized services while protecting my privacy.

4 *Eas1* Learning to operate this profile manager was easy for me.

5 *Ris2* I believe that there could be negative consequences from using this profile manager.

6 *Use1* Assuming I have access to this profile manager, I intend to use it.

7 *Tru1* I expect this profile manager will not take advantage of me.

8 *Ris3* I am taking a chance interacting with this profile manager.

9 *Val2* Using this profile manager increases my productivity to use personalized services while protecting my privacy.

10 *Eas2* I found it easy to get this profile manager to do what I wanted it to do.

11 *Ris4* I feel it is unsafe to interact with this profile manager.

12 *Use2* Given that I have access to this profile manager, I predict that I would use it.

13 *Tru2* I believe this profile manager is trustworthy.

14 *Ris5* I feel that the risks outweigh the benefits of using this profile manager.

15 *Val3* Using this profile manager enhances my effectiveness to use personalized services while protecting my privacy.

16 *Eas3* I found it easy for me to become skillful at using this profile manager.

17 *Ris6* I feel I must be cautious when using this profile manager.

18 *Use3* It is likely that I will use this profile manager in the near future.

19 *Tru3* I believe this profile manager will not act in a way that harms me.

20 *Ris7* It is risky to interact with this profile manager.

21 *Val4* I find this profile manager to be useful to use personalized services while protecting my privacy.

22 *Eas4* I found this profile manager easy to use.

(-3)	*(-2)*	*(-1)*	*(0)*	*(1)*	*(2)*	*(3)*
Strongly	Moderately	Slightly	Equally	Slightly	Moderately	Strongly
… more applicable to interface on left			applicable	… more applicable to interface on right		

Popup - After evaluation first & second pair

You are finished with the evaluation of this pair of interfaces. Next you will be asked to compare a different pair of interfaces. Please take some time to notice which interfaces you are supposed to compare.

Popup - After evaluation last pair

You are finished with the evaluation of the three pairs of interfaces.

Section 4C - Introduction

Additional Comments

Now you will be given the opportunity to provide additional comments with regard to the three different interfaces.

Section 4C - Page 1-3/3 - For each pair

Additional Comments

Please list any additional comments you may have with regard to the differences between the two interfaces shown below as far as they are not covered by any of the previous questions.

[PICTURES & NAMES OF EACH PAIR OF INTERFACES ARE SHOWN]

Pair1…n (open field for text)

Completed!

You have reached the end of the questionnaire

Thank you!

Appendix E: Additions to Chapter 4

E1. RATIONALE BEHIND GENERAL BACKGROUND MEASURES

The GVU's 10th WWW User Survey (GVU Center, 1998) was taken as a basis for the demographics and experience with technology measures (1.1 & 1.2), since it is a well-known web based survey intended to characterize Internet users, their reasons for using the WWW, and their opinions of WWW tools and technologies.

Personality traits were obtained by using the Ten Item Personality Inventory, TIPI by Gosling et al., 2003. The TIPI encompasses a personal judgment of the extent to which 10 pairs of personality traits apply on a scale from 1 (disagree strongly) to 7 (agree strongly). It gives people the following task description: *"Here are a number of personality traits that may or may not apply to you. Indicate (…) the extent to which you agree or disagree with that statement. You should rate the extent to which the pair of traits applies to you, even if one characteristic applies more strongly than the other."* Examples of pairs of personality traits used in TIPI are 'reserved/quiet' or 'sympathetic/warm'. The TIPI scores can be converted to the Big Five personality dimensions (i.e. Extraversion, Agreeableness, Conscientiousness, Neuroticism, and Openness to Experiences).
The Big Five personality dimensions are frequently used in personality assessments, although they are usually based on long questionnaires of sometimes more than 200 items that have to be rated. For the purpose of this study (similar to the Music Recommender study by Van de Garde-Perik et al., 2008), it was felt that such a long questionnaire would take too much time and effort for the participants. The TIPI test was created by Gosling et al. (2003) for situations where very short measures are needed or where personality is not the primary focus of interest. Both these conditions hold for this study also, so the TIPI was chosen as a personality inventory.

Concern for privacy was measured by using the Privacy Segmentation Index, PSI (Harris Interactive, 2002). The PSI consists of three statements about the use of personal information by organizations. Participants have to judge the extent to which they agree with each of these three statements. It is important to include a measure of privacy attitudes in order to ascertain that participants have varying privacy attitudes (Van de Garde-Perik et al., 2008). Most measures for privacy concern contain many items and are used only scarcely, for example the Privacy Attitude Questionnaire which is based on 36 items (Chignell et al. (2003). The specific PSI index was included in this study because of its brevity, and because this type of clustering is widely used in HCI research (Ackerman et al., 1999; Berendt et al., 2005, Consolvo et al., 2005).

E2. RESULTS GENERAL BACKGROUND MEASURES

Demographics

In total 78 participants started and completed the study, of which 29 were female (37%), and 49 were male (63%). Participant ages ranged from 18 to 60 with an average age of 32. For 95% of the participants education level was between high school and a doctoral degree.
Most participants had long time experience using the Internet. Only 4% of the participants had 3 years or less experience. 21% of the participants had 4 to 6 years of experience. And 77% had over 7 years of experience. Since the intention was to recruit participants who feel confident using a PC it is not surprising that most participants have long experience on the Internet.

This means that the sample is more male and more educated than the general population (For the Dutch population in 2008, 49.4% is male and 50.6% is female; CBS, 2008. In this study 22% of the participants had high school education or less, compared to 69% for the labor force in Holland aged between 15 and 64; CBS, 2006). The fact that the sample is more male may lead to lower privacy concerns overall (Garbarino & Strahilevitz, 2004; Sheehan, 1999; GVU Center, 1998; Harris Interactive, 2002). The effect of education level on privacy concern is not univocal, some find that higher education levels increases privacy concern (Sheehan, 2002), while others find the opposite (Harris Interactive, 2002). However, in the sample of the current study it turned out that out of the 12 questions regarding concern (measure 2.1) and risk (measure 2.2) there were only a few cases where the male and more educated participants rated the concern or risk higher compared to the other participants.

Experience with technology

Participants were asked about the types of communication technologies they use on a routine basis. Most used communication technologies were e-mail (100%) and phone (wired 82% and cell 81%). The high use of e-mail is another indication of the intended computer experience among the participants of this study.

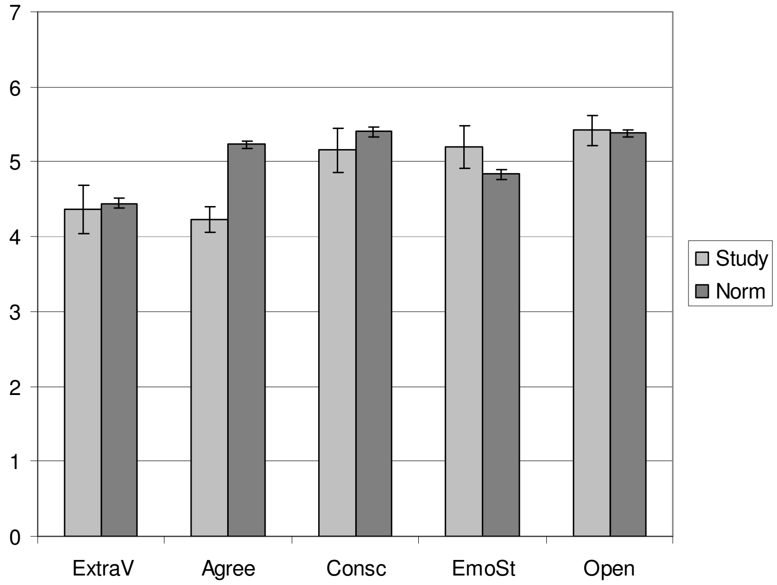
Participants were also asked about their experience with various web technologies in the past year. Most participants indicated to have viewed a web page containing Java or Java script (77%), used chat/online discussion (74%), and used streaming audio via the Internet (67%). Internet fax was used by least people (5%) in the last year.

This means that the participants are experienced with and aware of the current technological landscape. Therefore, they will be able to appreciate the privacy concerns and information disclosure choices presented to them in this study.

Typology of participants

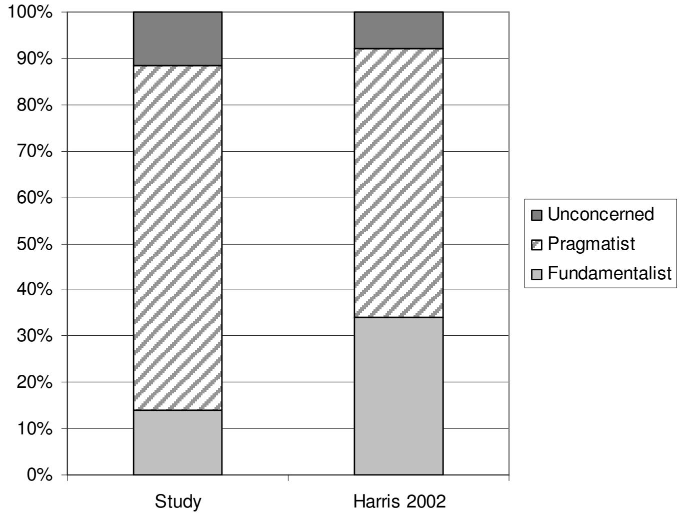
Participant scores on the TIPI Inventory were on average fairly neutral for the traits Extraversion (mean score 4.4) and Agreeableness (means score 4.2). Participants rated themselves as somewhat Conscientious (5.2), Emotional Stable (5.2) and Open to Experiences (5.4). For the traits Agreeableness, Emotional Stability, and Openness to Experiences participants tended to use the upper part of the scale (see Figure E.1). The normative data as published by Gosling et al. (2003) is 4.4, 5.2, 5.4, 4.8, and 5.4 respectively. This study's participants score lower on Agreeableness. However, overall the sample of this study is not particularly skewed towards any specific personality trait.

Figure E.1. Personality traits of participants in comparison to norm provided by Gosling et al. (2003)



Note: Mean score on each personality trait including 95%confidence interval. ExtraV = Extraversion, Agree = Agreeableness, Consc = Conscientiousness, EmoSt = Emotional Stability, Open = Openness to new experiences.

Figure E.2. Privacy Segmentation by PSI Index



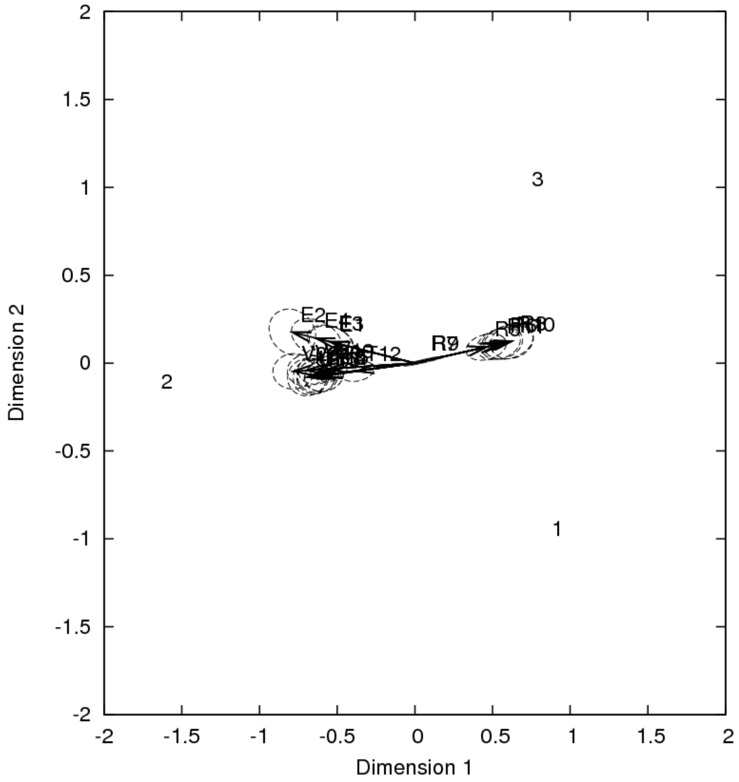
In order to obtain the PSI Index, participants rated three statements about the use of personal information by companies and organizations. It turns out that most participants (74%) can be considered pragmatists on the basis of their answers (being pragmatic about their privacy), and 14% fundamentalists (having strong opinions about their privacy), 12% can be considered unconcerned (see Figure E.2). Compared to the Harris Interactive sample (2002: 58%, 34% and 8% respectively) this study contains more pragmatists and less fundamentalists. This could have led to fewer privacy concerns in the sample of this study, however, it turned out that the level of privacy concern based on the scenarios is not significantly different for fundamentalists and pragmatists.

E3. ALTERNATIVE ANALYSIS AND PRESENTATION OF PAIRED EVALUATION

There is a possible alternative approach to represent the results regarding the paired evaluation of the interfaces. This approach is based on a combination of Multi Dimensional Scaling (MDS) and multiple regression. Within MDS the data points are regarded as approximations of the actual distances between the three interfaces in terms of dissimilarity. In this case the aim of the MDS analysis is to turn the overall difference ratings provided by participants into a set of proper Euclidean distances. The final configuration consists of an arrangement of points in a small number of dimensions. The points are located in such a way that the distance between them matches the dissimilarities between the objects as closely as possible (Coxon, 1982). Since in this study the number of objects (interfaces) is three, no more than two dimensions are needed to represent the dissimilarities between the interfaces. Multiple regression is used to learn more about the relationship between several independent or predictor variables and a dependent or criterion variable. In this study the distance in X and Y coordinates of two interfaces is given by the MDS analysis and is used to predict the distance in attribute perception between the two interfaces. This is repeated for all 3 interface pairs and all 22 attribute items.

The result of MDS and multiple regression for the whole sample is shown in Figure E.3. The figure depicts the relative distance between the three interfaces as based on the overall difference rating. When the overall difference between two interfaces was rated small by participants, then these interfaces are shown closer together in the figure.

Figure E.3. Example of multidimensional model for the three interfaces for the total sample



Note: The numbers indicate the 3 interfaces (1: Use UI; 2: Profiles UI and 3: Split UI), while the arrows indicate the directions in which perceived trust (T), risk (R), usefulness (V), ease of use (E) and intention to use (U) increase.

The horizontal and vertical axes of the figure are arbitrary in the sense that the graph can be translated, rotated, and scaled without influencing its interpretation. The interpretation of the space comes from the vectors shown for each of the five attributes measured. Furthermore, qualitative comments about the differences between the interfaces in the pairs could be used to further explain the dimensions 1 and 2 as currently depicted. If projections of the interfaces are made perpendicular to the arrows indicating each attribute, it becomes clear how an interface was evaluated.

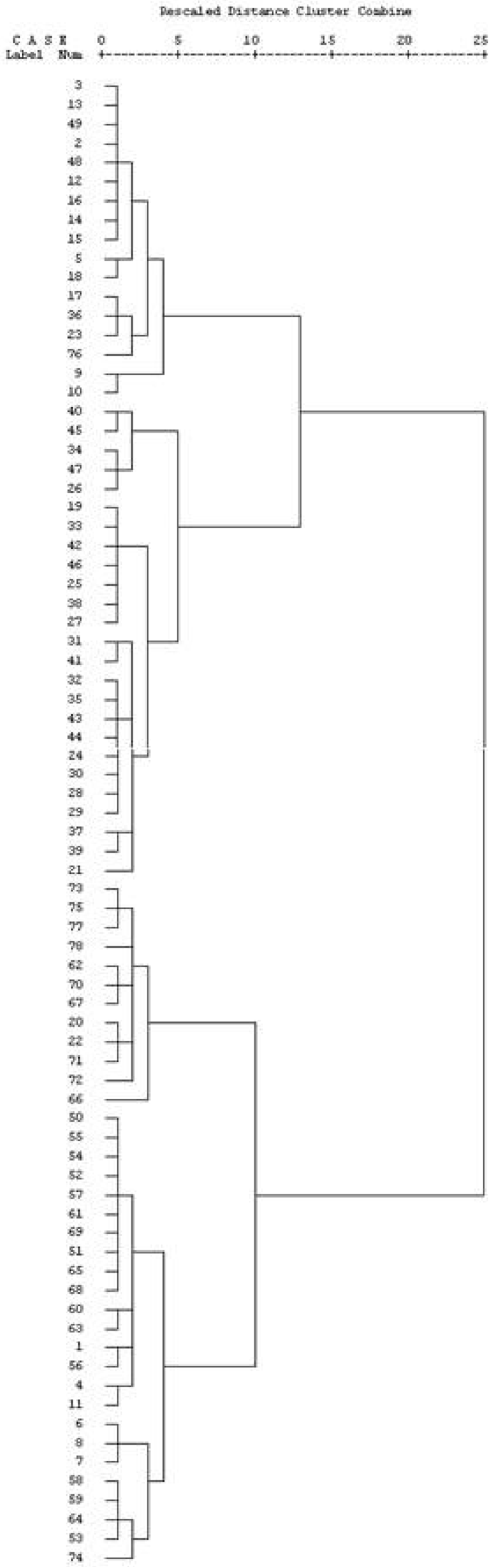
Figure E.3 shows that the privacy interfaces 1 and 3 (Use and Split) represent high levels of risk for the total sample, whereas the Profiles interface (2) represents low levels of risk. For all other attributes the opposite is true. The Profiles interface represents high levels of trust, usefulness, ease of use and intention to use, whereas Split and Use interfaces represent low levels on these attributes. The Split and Use UI are most different in terms of ease of use, since the angle of this attribute vector is least perpendicular to Split-Use line. The Split UI shows higher levels of ease of use than the Use UI.

The risk attribute is opposite to the intention to use and trust dimensions (same angle, thus they could be regarded as extremes of the same dimension). Ease of use is measuring a concept that is most distinct from risk (different angle), followed by usefulness. The perceived overall difference between the Split and Use UI is not explained very well by the five attributes measured.

E4. DENDROGRAM USED FOR CLUSTER ANALYSIS

Figure E.4 shows the dendrogram which is used (among others) to determine the number of clusters in chapter 4. According to SPSS a dendrogram is a visual representation of the steps in a hierarchical clustering solution that shows the clusters being combined and the values of the distance coefficients at each step. Connected vertical lines designate joined cases. The dendrogram rescales the actual distances to numbers between 0 and 25, preserving the ratio of the distances between steps (SPSS 14.0). The dendrogram on the next page shows that the distance between a 4- or 5-cluster solution is relatively large, therefore a 4-cluster solution is chosen.

Figure E.4. Dendrogram used for cluster analysis



E5. DESCRIPTION OF CLUSTERS

In chapter 4 cluster analysis based on Ward's method and the Squared Euclidean distance between cases was used in order to describe differences among participants with respect to their evaluation of the three interfaces. The final solution chosen was based on four clusters. However, since the fourth cluster was a heterogeneous cluster no clear pattern of evaluation for the three interfaces emerged. The results for the fourth cluster were not presented in the main text of chapter 4, but instead are presented in this appendix. This appendix provides more detailed descriptions of all four clusters.

Overall difference

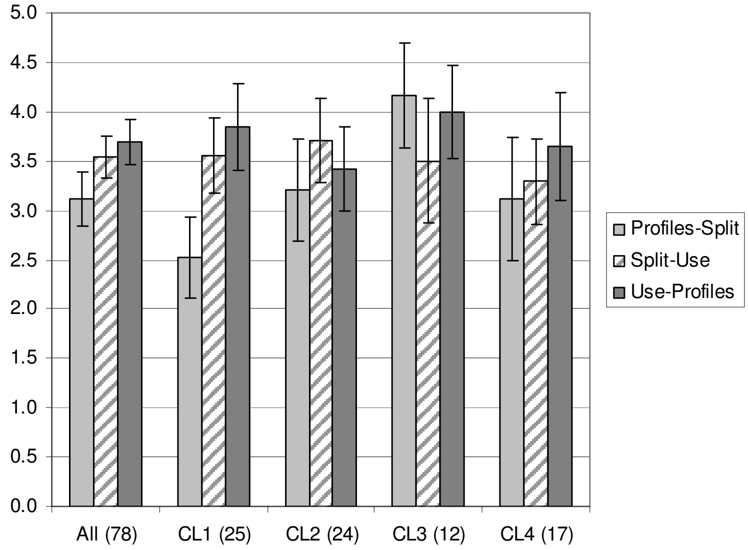
In Figure E.5 the difference scores for the three interface pairs are shown for whole sample and for the four distinguished clusters. The answering patterns for the overall perceived differences between the three interface pairs are similar for cluster 1, cluster 4 and the total sample of participants. For these groups the overall difference is perceived to be smallest between the Profiles UI and the Split UI and largest between the Use UI and the Profiles UI. Cluster 4 scores all three interface pairs fairly similar in overall difference, yet the overall difference between the Use UI and the Profiles UI is perceived to be somewhat larger (3.65 compared to 3.29 and 3.12).

Basic description of cluster 4 based on UI attributes

The last and fourth cluster (see Figure E.6) consists of 17 participants. This group of participants barely notices a difference between the interfaces with regard to the five attributes measured. The Split UI is slightly more preferred in comparison with the other two interfaces.

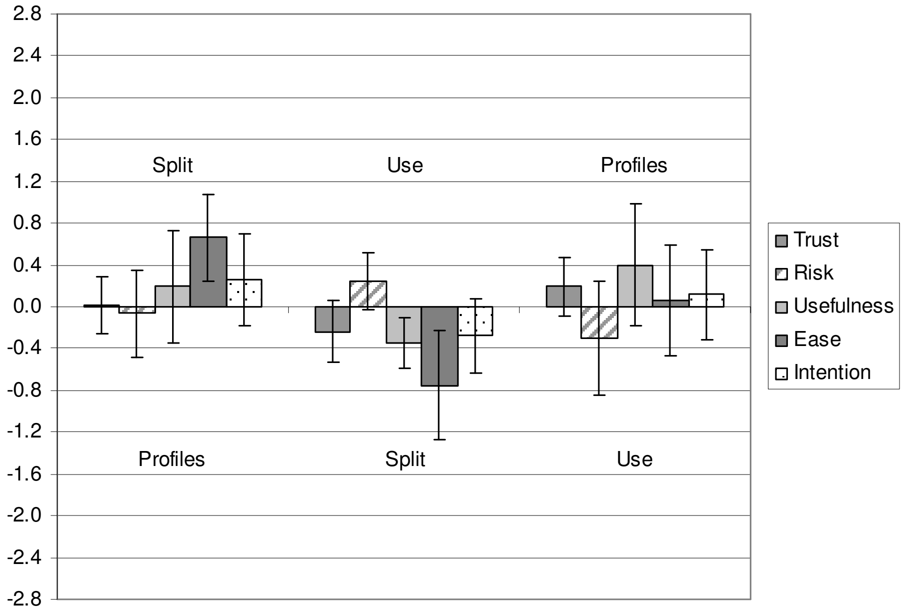
For the fourth cluster, as expected, hardly any paired comparison scores are significantly different from zero. Only the difference in ease of use between the Profiles UI and Split UI is significantly different from zero. And for the comparison between the Split UI and the Use UI both usefulness and ease of use are significantly different from zero. This indicates that the participants of this fourth cluster perceived the interfaces to be similar with regard to the measures of the five attributes.

Figure E.5. Overall difference between interface pairs for total sample and separate clusters



Note: Including 95% confidence interval. All: Total sample. CL: Cluster. The number in parentheses shows the number of participants in each group.

Figure E.6. Relative attribute rating of each interface pair for Cluster 4



Note: n=17. Figure shows rating for the following pairs: Profiles-Split; Split-Use; Use-Profiles. Negative or positive scores indicate that the first or respectively the second interface of a pair is scoring higher on a particular attribute, in accordance with the interface labels in the graph (score max: +3; min: -3). Including 95% confidence interval. No real preference, Split UI slightly more preferred.

General background data

Now a further examination of the difference between the four distinguished clusters is presented. First the clusters are analyzed on the basis of differences in gender and age. Clusters 2 and 4 have a relatively low percentage of female participants (both 29%) compared to the other two clusters (48% and 42%). The average age of participants in cluster 3 is fairly high (37.3 yrs) and the age of participants in clusters 1 and 2 is fairly low (30.9 and 29.2) in comparison to the overall average 32.1). The average age of participants in cluster 4 (34.2) is in between that of the other clusters.

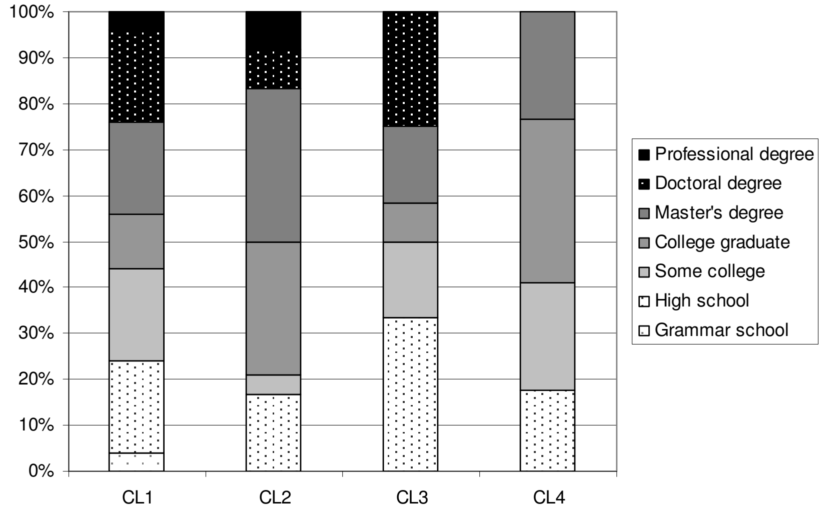
Figure E.7 shows that there are some differences in education level between the participants of the four clusters.

Experience with technology

With regard to the amount of years participants have used the Internet, cluster 2 and cluster 4 are slightly less experienced (29% of the participants have less than 7 years experience) than cluster 1 and cluster 3 (16% and 17%).

The use of communication technologies and Internet technologies by participants of the different clusters is compared. Cluster 1 is a heavy user of somewhat outdated technologies (such as wired phone 88% vs. 79% on average for other clusters; and postal mail 60% vs. 43% on average for other clusters). Cluster 2 makes little use of most communication technologies in comparison to the other clusters except to some extent cell phone use. Cluster 3 is in comparison to the other clusters a heavy user of the fax (17% vs. 8%), cell phone (92% vs. 79%) and to some extent voice mail. Cluster 4 is perhaps least advanced in their use of communication technologies, more heavily depending on the wired phone (82%) instead of the cell phone (65%) and on postal mail (47%) instead of voice mail (35%).

Figure E.7. Spread in education level among the clusters



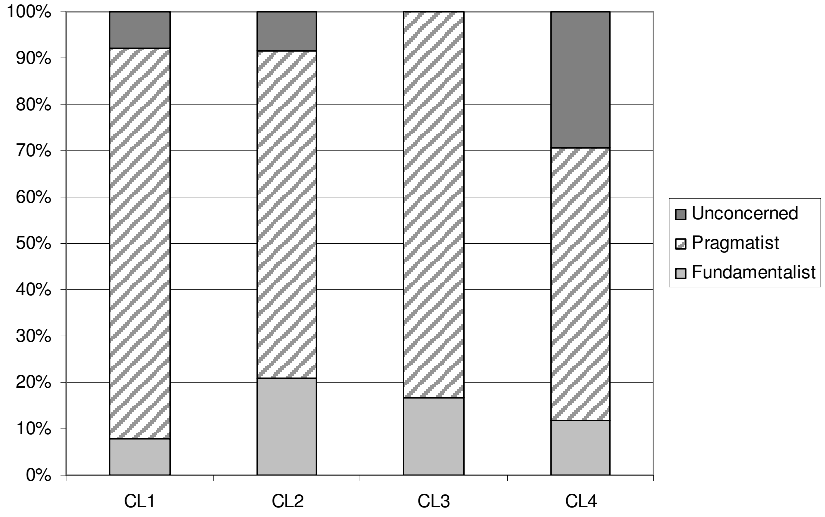
It seems that none of the clusters has a high use of all Internet technologies, but instead that the clusters are slightly different in the kind of technologies used. Cluster 1 and cluster 4 are relatively heavy users of digital signature or ID cards in comparison to the other clusters. Cluster 2 has more experience with streaming audio and video conferencing in comparison to the other clusters. And more participants of cluster 3 in comparison to those of the other clusters have experience with web technologies such as chat/online discussion, Internet phone, and visiting websites with Java (script).

Typology of participants

With regard to the Big Five personality traits based on the TIPI inventory there is little spread among the different clusters. Only for extraversion and conscientiousness there are slight differences between the clusters. Participants of cluster 2 rate themselves as least extravert (4.0 vs. 4.5). Participants of cluster 1 rate themselves as least conscientious (4.9) and participants of cluster 3 and 4 find themselves most conscientious (5.4).

Figure E.8 shows the spread in privacy segmentation according to the PSI index among the participants of the four clusters. In comparison to the other clusters, cluster 1 has a fairly large proportion of privacy pragmatists (84%) and small proportion of privacy fundamentalists (8%). For cluster 2 this picture is reversed; since it consists of a fairly small proportion of privacy pragmatists in comparison to the other clusters (71%) and a large proportion of privacy fundamentalists (21%). Cluster 3 does not have any privacy unconcerned participants, but a fairly large proportion of privacy pragmatists (83%). Taken together this means that participants of cluster 3 are quite concerned about their privacy with no unconcerned individuals and fairly many fundamentalists. Cluster 1 and cluster 2 are more neutral in their privacy attitude. Cluster 4 tends to be least concerned about their privacy with most unconcerned individuals.

Figure E.8. Spread in Privacy Segmentation Index among the clusters



Evaluation scenarios

Figure E.9 shows the difference in average perceived realism and perceived privacy concern across the five scenarios for the four different clusters. It shows that cluster 3 perceives the scenarios somewhat differently from the other clusters. Participants of cluster 3 find the scenarios on average more realistic (5.7 vs. 4.5, 4.5 and 4.7), and express slightly more concern about their privacy (5.8 vs. 5.1, 5.0, and 4.5).

Figure E.9. Spread in perceived realism & privacy concern of the scenarios among the clusters

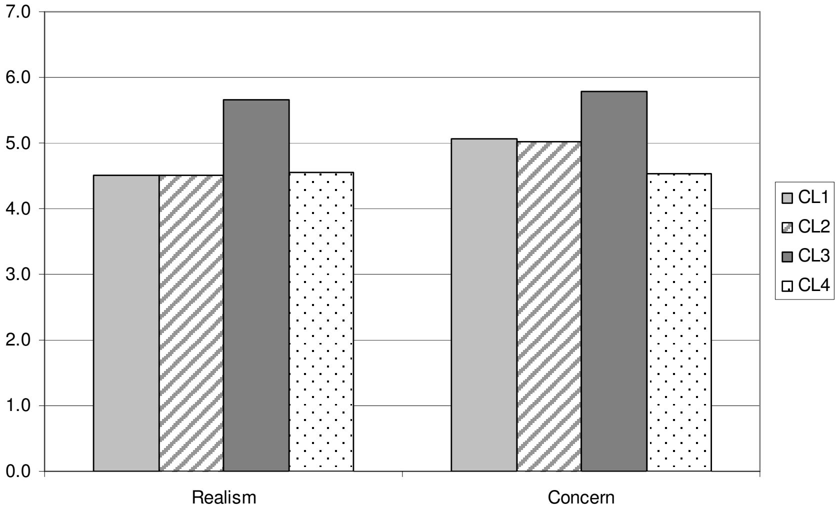
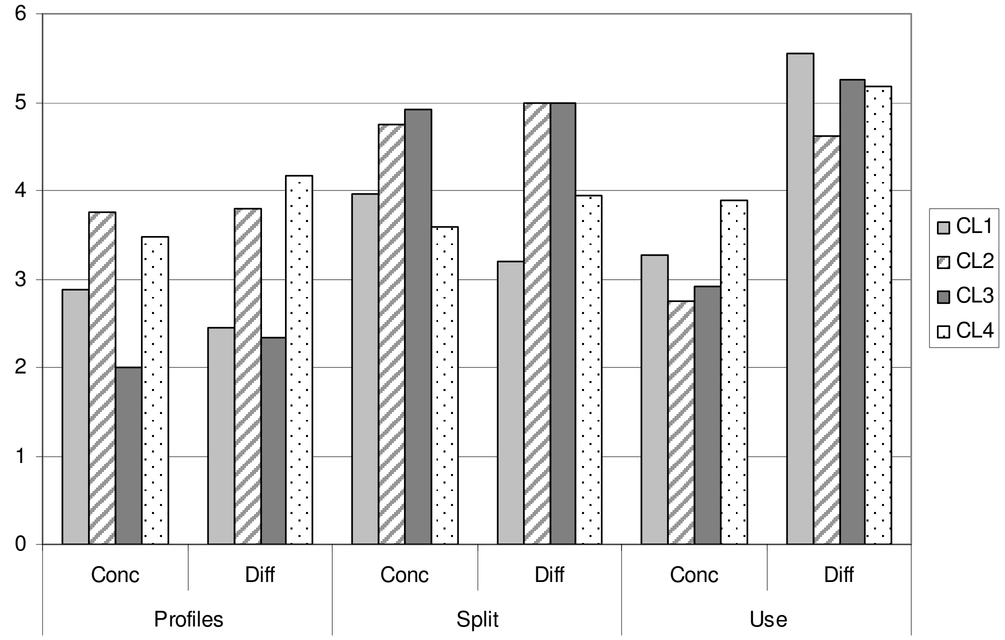


Figure E.10. Spread in level of concern & ease of use among the clusters



Note: Conc = Concern, which is evaluated after first use. Diff = Ease of use is expressed as level of difficulty, which is evaluated after second use.

Separate evaluation interfaces

Figure E.10 shows the spread in perceived concern after the first use of the interfaces and the perceived difficulty after the second use of the interfaces. It shows that the perception of concern and difficulty among clusters is quite similar for the Use UI and more distinct for the Profiles UI and the Split UI. With regard to the Profiles UI participants of cluster 2 and 4 express high concerns (3.8 and 3.5) and difficulty (3.8 and 4.2) in comparison to the other two clusters (2.9 and 2.0 for concern and 2.4 and 2.3 for difficulty). With regard to the Split UI cluster 2 and cluster 3 tend to perceive high concern (4.8 and 4.9) and high difficulty (both 5.0) in comparison to the other clusters (4.0 and 3.6 for concern and 3.2 and 3.9 for difficulty).

Looking at each cluster separately, it shows that for cluster 1 in terms of concern the Profiles UI is most preferred (2.9) and the Split UI least (4.0), and with regard to difficulty the Profiles UI (2.4) is preferred and the Use UI least (5.6). Cluster 2 most prefers the Use UI in terms of concern (2.8) and the Profiles UI in terms of difficulty (3.8). The Split UI is least preferred by cluster 2 (4.8 for concern and 5.0 for difficulty). For cluster 3 the Profiles UI is most preferred (2.0 for concern and 2.3 for difficulty), and least preferred are the Split UI in terms of concern (4.9), and the Use UI in terms of difficulty (5.3). The Use UI is least preferred by cluster 4 (3.9 for concern and 5.2 for difficulty), whereas the other two interfaces score somewhat better and fairly similar.

Privacy concerns per cluster

Participants were asked to list their concerns with regard to the 5 scenarios presented. There are some differences between the concerns mentioned by the different clusters. The amount of concerns mentioned on average by each cluster varied as well. Cluster 3 mentioned most concerns namely 14.5 on average, whereas for the other clusters this ranged from 11.8 to 12.8.

For all clusters Recipient_Info is mentioned most frequently as a concern. The other 3 most frequently mentioned concerns for each cluster are:
- Cluster 1: privacy, recipient and control.
- Cluster 2: both service disliked & recipient, then control (privacy is not mentioned as a top 4 concern).
- Cluster 3: purpose, followed by both service disliked & control (privacy is not a top 4 concern).
- Cluster 4: control, recipient and privacy.

So, for all clusters both the recipient and control are very important. However, when looked at the actual distinctions between the four different clusters in frequently mentioned concerns then it seems that for cluster 1 particularly privacy and security are important. Cluster 2 tends to stress the downsides of the services depicted such as that the service is disliked or that a lot of effort is involved. Cluster 3 particularly mentions the purpose and the own freedom.

Remaining qualitative data per cluster

Table E.1 shows for each cluster which comments are made most frequently with regard to a specific interface. In this analysis the comments made by at least 10 participants were taken into account (see Table 4.5 page 129) as well as two additional comments, namely control and trustworthiness (the degree of control/trustworthiness provided by the interface). The frequently mentioned comments will be referred to by the code name for consistency.

It shows that for cluster 1:
- The Split UI is neutrally perceived (particularly easy to use and generally appreciated).
- The Use UI is negatively perceived (generally unclear, consequences settings unclear, not easy to understand).
- The Profiles UI is positively perceived (clear, combinations, easy to use, easy to understand/learn, generally liked, overview appreciated, precision).

For cluster 2:
- The Split UI is negatively perceived (only cluster that does not refer to interface as easy to use, it finds the interface difficult to understand or learn in comparison to other clusters, and is negative about its trustworthiness).
- The Use UI is positively perceived (in comparison to other clusters only few participants mention it is unclear, availability default mentioned a lot, consequences settings clear, quite positive about the combinations possible, generally liked, positive about its safety and speed in comparison to other clusters).
- The Profiles UI is slightly positively perceived (lack of default, consequences settings unclear, precision and control appreciated).

For cluster 3:
- The Split UI is negatively perceived (especially mentioned by this cluster is the lack of specificity, besides the UI is generally disliked, and perceived to have limited possibilities).
- The Use UI is negatively perceived (not easy to use, limited possibilities, lack of safety, lack of specificity and control).
- The Profiles UI is positively perceived (clear, easy to use, possibilities, specificity, control, trustworthiness).

For cluster 4:
- The Split UI is neutrally perceived (clear, easy to use, but meaning elements unclear, lack of overview and possibilities)
- The Use UI is negatively perceived (combinations disliked, meaning elements unclear, limited possibilities).
- The Profiles UI is slightly positively perceived (less positive in general and in comparison to other clusters finds it less easy to use).

Table E.1. Differences in perception of interfaces between clusters

	Cluster 1			Cluster 2			Cluster 3			Cluster 4		
	Split	Use	Prof	Split	Use	Prof	Split	Use	Prof	Split	Use	Prof
Availability default					PPP	NN						
Clear		NNN	PP	NNN			NNN	NN	PPP	P	NNN	
Combinations	N		PPP	NNN	P	PP	N		PPP	NN	NN	N/PP
Consequences settings		NN	N	NNN	N/P	NN	NNN	N	NN/P	N		P
Easy to use	PPP	N	PPP		PP	PP	PP	PP	PPP	PPP	P	P
Easy to understand/learn		NN	P	NNN				N			N	
Foolproof	N	N		N				N			N	
General	PP	N	PPP	N	PP	PPP	N	N/P	PPP		N	P
Meaning elements		NN						N		N	NN	
Overview		N	PPP	N		PPP			P	N	N	PP
Possibilities		NN	NN/P		NN/P	N	N	NNN	PPP	N	NNN	
Precision	N		P			P						
Safety					PP			NN			N	
Specificity	N		P				NN	N	PPP			
Speed			N	P	P	NNN			NNN	P		NN
Control						P		N	PP			
Trustworthiness				N					P			
Negative	4	15	4	16	3	8	11	14	5	6	15	3
Positive	5	0	18	1	13	12	2	3	23	5	1	7

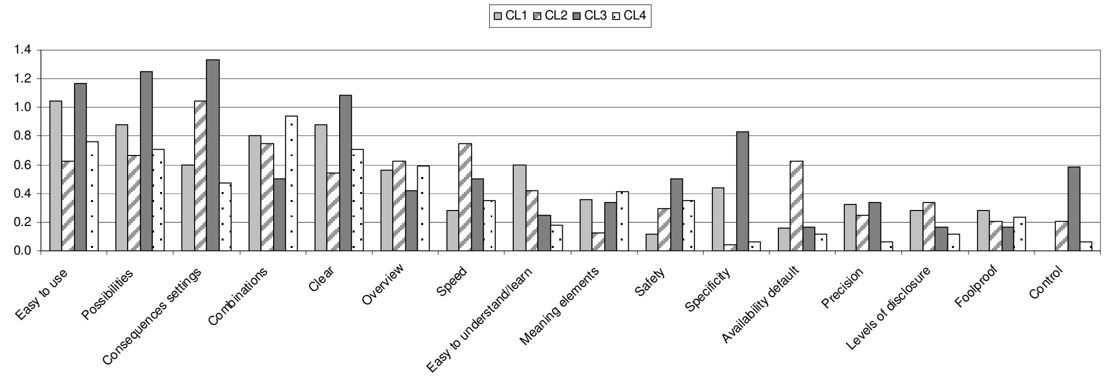
Note: Based on qualitative comments. N/P = extent to which participants express negative or positive evaluation of an interface; Prof = Profiles UI.

Ignoring the reference to a specific interface, or the direction of the comment (i.e. positive or negative), than it is possible to investigate the number of times each comment is mentioned by participants of a particular cluster. Figure E.11 shows the results. This figure shows the 16 most frequently mentioned specific comments (general liking or suggestions for improvement, unclear comments are disregarded).

For cluster 1 the most frequently mentioned comments are easy to use (high frequency in comparison to other clusters: 1.04 vs. 0.85), possibilities of the interface (0.88), the clarity of the interface (0.88), the possible combinations (0.80), the consequences of the settings (low frequency in comparison to other clusters: 0.60 vs. 0.95), and whether the interface is easy to understand or learn (high frequency in comparison to other clusters: 0.60 vs. 0.28).

For cluster 2 most frequently mentioned comments are the consequences of the settings (high in comparison to other clusters: 1.04 vs. 0.80), the possible combinations (0.75), the speed (high in comparison to other clusters: 0.75 vs. 0.38), the possibilities (low in comparison to other clusters: 0.67 vs. 0.95), easy to use (low in comparison to other clusters: 0.63 vs. 0.99), the overview provided by the interface (0.63), and the availability of default settings (high in comparison to other clusters: 0.63 vs. 0.15).

Figure E.11. Average number of times specific comments are mentioned per participant per cluster



And for cluster 3 the most frequently mentioned comments are all frequently mentioned in comparison to the other clusters, namely the consequences of the settings (1.33 vs. 0.70), the possibilities (1.25 vs. 0.75), easy to use (1.17 vs. 0.81), the clarity of the interface (1.08 vs. 0.71), the specificity (0.83 vs. 0.18), and the amount of control provided by the interface (0.58 vs. 0.09).

Cluster 4 specifically mentions the possible combinations of the interface (high frequency in comparison to other clusters: 0.94 vs. 0.68), easy to use (0.76), the possibilities of the interface (0.93), the clarity of the interface (0.71), the overview provided by the interface (0.59) and the consequences of the settings (low frequency in comparison to other clusters: 0.47 vs. 0.99).

A short typology of issues that are apparently important to each of the clusters is as follows.

- Cluster 1 values an interface that is (initially) easy to use and that provides a lot of options.
- Cluster 2 also values a lot of options and prefers a quick/fast interface.
- For cluster 3 an interface that is easy to use or clear is important, as well as control/safety and the level of detail available.
- Cluster 4 values the combinations & possibilities of an interface, ease of use, and clarity of an interface.

Final Description Cluster 4

Cluster 4 is in between the other clusters regarding age of its members. It consists of few females (29%). It is the least educated cluster. It uses somewhat outdated communication technologies, and has short time experience on the Internet. The participants of this cluster find themselves to be somewhat conscientious. This cluster is least concerned about their privacy as based on the PSI index. Concerns raised by this cluster are control, recipient and privacy. In comparison to other clusters also info type is important. This cluster has no particular preference for any of the conceptual models, although the Split UI seems slightly preferred. Table E.2 shows the main differences between all clusters in compact form.

Table E.2. Summary of differences between the clusters

	CL1	CL2	CL3	Cl4
Age	Low	Low	High	High
Proportion females	High	Low	High	Low
Education level	Intermediate	High	Intermediate	Low
Internet experience (yrs)	High	Low	High	Low
Personality	Least Conscientious	Least Extravert	Most Conscientious	Most Conscientious
Privacy Concern (PSI)	Intermediate	Intermediate	High	Low
Realism & Concern scenarios	Intermediate	Intermediate	High	Intermediate
Concern & Difficulty UIs	Low: Profiles	High: Split	Low: Profiles	High: Use
Main concerns	Privacy & Security	Downsides of services	Purpose of use Own freedom	Control Recipient Type of info
Evaluation Profiles UI	Positive	Positive	Positive	Neutral
Evaluation Use UI	Negative	Positive	Negative	Neutral
Evaluation Split UI	Neutral	Negative	Negative	Neutral
Main characteristics	Easy to use Options	Combinations Quick to set interface	Easy to use Clarity Control/Safety Level of Detail	Options Easy to use Clarity
Intention to Use influenced by	Usefulness Ease of Use	Usefulness	Usefulness Trust	Usefulness Ease of Use