Scandinavian Journal of Information Systems

Volume 21 | Issue 1 Article 1

2009

Consumers' Views on Privacy in E-Commerce

Taina Kaapu
University of Tampere, Finland, taina.kaapu@uta.fi

Tarja Tiainen
University of Tampere, Finland, tarja@cs.uta.fi

Consumers' Views on Privacy in E-Commerce

Taina Kaapu
Department of Computer Sciences, University of Tampere, Finland
taina.kaapu@uta.fi

Tarja Tiainen
Department of Computer Sciences, University of Tampere, Finland
tarja@cs.uta.fi

Abstract. Information privacy protection and invasion of privacy in e-commerce have become important topics in both everyday activities and scientific discussions. The aim of this study is to understand how consumers regard privacy in business-to-consumer e-commerce. As this study focuses on consumers' own interpretations of privacy, the research approach is empirical, rather than theoretical. Based on a phenomenographical analysis of consumer interviews, we identify different layers of understanding by focusing on the referential objects and the structural components of information privacy. The result includes 25 different privacy conceptions, showing that consumers' view of privacy is situated and constantly under construction as the consumer gets new information or experiences.

Key words: information privacy, consumer, e-commerce, phenomenography.

1 Introduction

Understanding consumer behaviour is vitally important in online shopping. One precondition for the growth of e-commerce is that the consumers use online channels. These channels are chosen at each stage in the purchase process: requirements determination, vendor selection, purchase, and after-sales service (Choughury and Karahanna 2008). The process is connected to the consumers' trust in e-purchase and e-vendors, and to the consumers' perceptions of risk (Choughury and Karahanna 2008; Verhagen et al. 2006). The number of online consumers has grown; at the same time, the fears regarding information privacy have also increased (Malhotra et al. 2004). The biggest concerns to Internet users are viruses, spam, spyware and hackers (Paine et al. 2007). If these problems are not solved, the consumers whose privacy concerns have not

© Scandinavian Journal of Information Systems, 2009, 21(1), 3–22

been addressed may delay their purchases or even forgo them, and some concerned consumers might prefer traditional ways of purchasing (Prabhaker 2000).

To deal with these concerns, privacy enhancing technologies (PETs) have been developed: software programs, hardware devices and even publications, which help users to regain their privacy lost on the Internet (Camp and Osorio 2003). Legal instruments for increased security have been formulated as well: for example, the European Union (EU) requires all its member states to legislate to ensure that their citizens have a right to privacy (Directive 95/46/EC).

On a practical level, e-vendors work to increase online purchasing. Research in information systems (IS) and consumer studies aims to increase understanding about e-commerce and consumers' online behaviour (see e.g., Cassidy and Chae 2006; Hui et al. 2007; Malhotra et al. 2004). Our paper belongs to the same research area, although we focus solely on information privacy. According to the traditional definition, information privacy is the ability of the individuals to control information about themselves (Westin 1967). Instead of concentrating on traditional and direct marketing, as done in several former studies (e.g., Smith et al. 1996, Stewart and Segars 2002), we seek to understand how consumers view information privacy in business-to-consumer (B2C) e-commerce. In doing so we aim to present and discuss the subject matter so that business and legislative authorities can adequately respond to and address these consumers' needs and fears. This is necessary to allow maximizing the potential of e-commerce.

Theory testing with surveys is a commonly used research method in studying Internet privacy. A typical study asks about informants' attitudes towards specific privacy statements with fixed scale (e.g., Cassidy and Chae 2006; Malhotra et al. 2004). In theory testing studies, the researcher—based on the theory under testing—defines how information privacy is conceptualized. However, it is important to take a step back and investigate how consumers understand privacy in everyday practice.

To fill this gap in the literature, we decided to use a qualitative research approach for getting a richer picture of consumers' views. Instead of seeking the dominant view or an average one, we focus on the differences in views. We decided to concentrate on the variation of consumers' interpretations as consumers are not a homogenous group. In most consumer studies, consumers are divided to groups based on their demographical variables, income or attitudes. Westin categorized consumers based on their attitudes towards privacy; to categories of privacy fundamentalists (who feel that they have lost their privacy), privacy pragmatists (who protect their personal information), and privacy unconcerned (who have no real concerns about privacy) (Taylor 2003).

Our aim is to focus on all types of consumers' views on information privacy without categorizing consumers beforehand. First, we seek what earlier studies say on consumers' interpretations of information privacy. In doing this, we briefly describe the concept of privacy as discussed in the previous literature. Then, we describe the research methods used in our study: as we look for alternative views, we use phenomenography and consumer interviews. After the methodological part, we offer the results in a form of categorization of consumers' views based on the analysis of the interview material. The results show that consumers' interpretation of information privacy is situated; it varies between familiar, trusted cases and unknown cases perceived as suspicious. Finally, we present the discussion and conclusion.

2 Research background

In this section, we describe the scope of Internet privacy studies for locating our study to the appropriate scientific field. Privacy is characterized according to the traditional definition 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" (Westin 1967, (pp. 6-7). Invasions of privacy occur when individuals cannot maintain an adequate degree of control over their personal information and its use (Chung 2003). We follow the generally accepted view of information privacy by seeing it as the ability of individuals to control information about themselves (e.g., Cheung and Lee 2006; Graeff and Harmon 2002; Udo 2001).

Online information privacy has been studied in the disciplines of law and public policy, marketing, organisational behaviour, and IS (Malhotra et al. 2004). One way to see privacy is to understand it as a legal concept (e.g., Curran and Richards 2004). Although the concept of privacy itself may sound straightforward, the regulatory laws vary between cultures (Milberg et al. 1995). Developed societies have made different assumptions about privacy in their societal regulatory approaches. The societies can be roughly sorted into two categories: First, to those who view privacy as a human right, as is the case in the EU (Bygrave 1998), for example, where measures that address all the data collection and use within society are being introduced. Second, to societies which view privacy as a matter for contractual negotiation, such as the United States and Japan, for example, where the laws are specific to various sectors (e.g., medical data) (Smith 2004).

There exist contradictory views on privacy and benefits for consumers, for example about the collection of personal information. It can be seen as a positive matter, since personalized services cannot be created without personal information. However, consumers' hopes in this area are paradoxical: easy, personalized services are in demand but collecting personal information is resisted (Awad and Krishnan 2006). While the freedom of movement of information and its benefits to the general public have been emphasized (e.g., Bergkamp 2002; Rubin and Lenard 2002), the somewhat opposite view sees personal information registers as unreliable, and the aim of the laws has been to limit their use. Thus, the latter view focuses on threats such as more widespread profiling when handling personal information (e.g., Graeff and Harmon 2002; Liu et al. 2005) and consumers' continuous on-line monitoring (e.g., Kruck et al. 2002; McRobb and Rogerson 2004; Smith 2004).

Consumers' lack of trust constitutes a major psychological barrier to the adoption of e-commerce (Cheung and Lee 2006). Consumers' privacy concerns have been studied with theoretically based surveys, with varying results (e.g., Udo 2001; Malhotra et al. 2004). For example, consumers' privacy concerns are stated to be related to the following aspects of data collection and use (Smith et al. 1996; Stewart and Segars 2002): 1) unauthorized collection, 2) errors related to the integrity of databases, 3) unauthorized secondary use, and 4) improper access to personal data. Some studies present concerns in a more concrete way, as listed in the following (e.g., Cassidy and Chae 2006; Chung 2003):

1. Visits to websites might be secretly tracked.
2. E-mail addresses and other personal information could be taken and used without permission for marketing or other purposes.
3. Personal information could be sold without permission to third parties.
4. Credit card information could be stolen.

One of the other types of categorizations is presented by Paine et al. (2007), which states that the consumers' main concerns about online privacy are viruses, spam, spyware and hackers. Malhotra et al. (2004) conceptualize Internet users' information privacy concerns as

> The degree to which an Internet user is concerned about online marketers' collection of personal information, the user's control over the collected information, and the user's awareness of how the collected information is used (Malhotra et al, p. 338).

They also developed a causal model to describe how concerns influence a consumer's decision to release or not release personally identifiable data.

E-vendors can do a lot for mitigating the consumers' fears related to privacy. Information on how companies maintain and use personal information increases consumers' trust (Liu et al. 2005). The presence of a vendor's online privacy policy decreases consumers' privacy concerns (Hui et al. 2007; Jensen et al. 2005; Pan and Zinkhan 2006). At least in some cases, consumers trust e-vendors (e.g., Gefen et al. 2003) and are not afraid of privacy problems with them, such as e-vendors selling personal information to third parties (Cheung and Lee 2006).

The above studies present at least partly contradictory findings, which makes consumers' views on information privacy an important issue to study further. Consumers' behaviour is usually studied in a conventional direct marketing environment (Phelps et al. 2000). These studies are most often based on demographical factors, and the differences that are found include (Graeff and Harmon 2002):

- Gender differences: men are less concerned about privacy issues than women, and men have more faith in purchasing on the Internet;
- Class differences: the consumers with high incomes want to know more about their information after collection than other consumers;
- Age differences: older people are less likely to believe that their information might be sold to others for marketing purposes.

Furthermore, the global nature of e-commerce makes privacy issues even more complex, because the perceptions of privacy and fair information practices depend on government regulations and vary across cultures (Bellman et al. 2004; Milberg et al. 1995).

Information privacy is focused in different areas, such as consumers' behaviour (see Table 1 for a summary). Although some studies (e.g., Jensen et al. 2005; Paine et al. 2007) ask for a deeper understanding of consumers' thought-models, almost all studies have used a theory-testing research approach with surveys or laboratory tests. The only exception we could find is the study by Hui et al. (2007), in which field observations were made in a local firm focusing on privacy statements. Our study belongs to the same empirically based approach among qualitative studies, focusing on the consumers' own interpretations of information privacy. In this ap-

proach, rather than building our research on some earlier studies with their underlying assumptions, we must be as open minded as possible to reach the consumers' own thought-models. Our aim is to find out what these consumers exactly mean when they discuss information privacy.

However, the concept of information privacy may signify different issues or concerns to different people. This paper aims to clarify this with the help of a categorization of consumers' views of information privacy in e-commerce. The study has both theoretical and practical contributions. On the theoretical side, we discuss the consequences of our empirical results vis-à-vis the existing literature. On the practical side, we give important guidelines in order to understand consumers' concerns about privacy in the online environment.

Areas of information privacy studies	*Example references*
1. Defining privacy	Westin 1967
2. Legal issues about privacy	Bygrave 1998 Cassidy and Chae 2006
3. Technology for privacy (Privacy Enhancing Technologies)	Camp and Osorio 2003
4. Vendors' actions to increase privacy	McRobb and Rogerson 2004 Prabhaker 2000
5. Consumers' actions in relations to privacy, which is studied based on: - Consumers' demographic factors - Consumers' attitudes, values and behavior	Awad and Krishnan 2006 Graeff and Harmon 2002 Taylor 2003
6. Consumers' privacy concerns: - Personal information: collection, unauthorized secondary use, improper access, errors, stealing - On-line monitoring - Viruses, spam, spyware and hackers	Chung 2003 Malhotra et al. 2004 Paine et al. 2007 Stewart and Segars 2002

Table 1: Focal areas of information privacy studies

3 Methodology

Our aim is to understand how consumers see privacy and to describe the differences in their views in e-commerce. For studying people's own interpretations of a concept (information privacy in this case) a qualitative method which focuses on people's narration is needed. Individuals' views are socially constructed; however, the individuals' own background, including their education and experience, can also have effect on their views. Methods such as discourse analysis, grounded theory (GT), and phenomenography can thus be considered. In choosing the research method, we discarded discourse analysis, since it has its focus on social interaction, such as shared (communal) views and argumentations (Alvesson and Karreman 2000).

A decision between GT and phenomenography was made based on their different study aims. Although they both itemize individuals' talk to its elements, the target of that process

is different. GT re-ties the elements together for a whole picture of the phenomenon under study (Glaser and Strauss 1973), whereas phenomenography aims for reaching all the alternative views or the structures of individual thought-models (Marton and Booth 1997). As some thought-models are richer and more versatile than others, the result forms a hierarchical structure. Phenomenography is about individual meaning construction, which results in a conception referring to conceiving and understanding something. Humans' experience of the world is constituted as an internal relation between the experiencing people and the world (Marton 1981). Conceptions are regarded as ground for action (Säljö 1994).

Phenomenography was introduced by educational researchers (Marton 1982). It has been used for educational studies also in the IS field in clarifying computer science students' conceptions of recursion (Booth 1992) and in finding out about moral conflicts in the project work course (Vartiainen 2007). The method is also used for analysing IS professionals' assumptions about the human being (e.g., Isomäki 2002). Here we use the method for analysing IS users' views. Our study focuses on non-professional people whose knowledge of technology is limited; they might have erronous views about what is possible and what is not over the Internet. Regardless, in this study we do not evaluate the workability of their presented assumptions. It is enough that the informant believes in them, and that they thus may affect his/her behaviour. These concepts will be made explicit to allow IS professionals to understand them.

In phenomenography, empirical material is typically collected by interviewing a relatively small number of relevant informants. The main point when choosing these is to reach the largest possible differentiation in their views (Marton and Booth 1997), similar to theoretical samples in other qualitative methods (see e.g., Glauser and Strauss 1973). We maximize the differentiation in privacy conceptions with the help of two interview settings. The first one focused on privacy, and the views there were directly elicited from the interviewees: they were asked to describe privacy in the Internet setting in their own words. When a question about a phenomenon is asked directly, there is a chance that the informants repeat the dominant discourse of the issue; this can be regarded as the shared view by the society (Hynes et al. 2006). In this study the aim was to reach all the alternative views: therefore, besides of direct asking, we also discussed privacy indirectly. The second interview focused on the use of electronic services; privacy was expected to be an underlying assumption to emerge in the interviews.

The interviewees were sought in several ways. One criterion in the selection was age. Unlike in many studies that use young informants (e.g., Cheung and Lee 2006; Gefen et al. 2003), we also sought older people's views. Having them in our interview group increased the chance of eliciting a larger variety of concepts: the older people seem to be the most passive in data protection issues while well-educated, young, heavy Internet users are the most active group (Grable and Joo 1999; Muttilainen 2006).

In the first interview set, individuals known by the researchers were directly asked for interviews. Also, the snowball method was used; the interviewees were asked to name other possible interviewees, especially those who might have (different) opinions on privacy. The first interview set based on direct questions about information privacy included twelve interviews.

For the second interview set, volunteers were found by advertising on a local newspaper's website and in an e-commerce seminar. Volunteers needed to fill in an Internet form indicating their age, sex, and values. For identifying the values, the volunteers rated each of the listed values and specified the most and the least important values. The list of values included: 1. sense of

belonging, 2. excitement, 3. warm relationship with others, 4. self-fulfillment, 5. being well-respected, 6. fun and enjoyment in life, 7. security, 8. self-respect, and 9. sense of accomplishment (based on List of Values (LOV) by Kahle et al. 1986). In the selection of interviewees our aim was to maximize the differentiation in participants' views. As the former studies highlight information privacy concerns, we decided to use two values that are related to safety (security and excitement). Of the twenty volunteers who filled in the form we selected five security-minded and five excitement-minded consumers. Their interview focused on the use of e-services.

We did not study the relationship between the interviewees' background and the privacy view, so the interviewees' backgrounds are not significant for the analysis. However, we are aware that the variation among interviewees' background might help in reaching the largest possible variation in views. A brief description of their backgrounds is shown in Table 2. This may help the reader to better understand the empirical base of this study.

The aim of phenomenographical study is to describe the differentiation between individuals as regards the phenomenon under study. In collecting data, the interview situation affects what people say and how they say it; furthermore, due to bias caused by personal education and other background, researchers may ignore some ideas mentioned by the informants (Eriksen 2001). To minimize this problem, we varied the interview situation: in the first interview set there was one interviewer, and in the second set there were two interviewers.

Interviewees	*Female*	*Male*	*Total*
Age			
Between 25 and 35 years	4	4	8
Between 36 and 54 years	4	1	5
Between 55 and 66 years	5	4	9
Total	13	9	22
Occupational background			
Business and administration	4	4	8
Health and social affairs	4	2	6
Teaching and education	3	1	4
Technological sector	2	1	3
Agriculture	-	1	1
Total	13	9	22

Table 2: Consumers interviewed

Otherwise, the interviewing progress was alike in both of the interview sets. The individual interviews were open-ended, and only the topics were decided beforehand. The interviews started from a general discussion about the interviewees' backgrounds (as consumers in e-commerce) and were followed by a discussion about the main issue (which concerned, in the first set, privacy issues in e-commerce and, in the second set, e-services in the form of e-journals and e-commerce). The duration of the interview situations varied from thirty minutes up to two hours and thirty minutes. The interviewer's role was to follow the interviewees' ideas and explore their narration.

The interviews were collected during spring and summer 2004 in Finland. They were transcribed and their text then analysed. In phenomenographical studies, the analysis focuses on two components in the informants' experiences of the phenomenon; the referential component—which describes what the phenomenon means in everyday language—and the structural component—which refers to a deeper level of phenomenal meaning (Marton and Booth 1997). The *what* aspect directs individuals' thought to the object, which can be physical or mental by nature. The *how* aspect refers to the thought processes by which an object of thought is limited in relation to its environment (Marton 1981). In phenomenography, the conceptions are intentional with respect to the two intertwined aspects, which signify the qualitative differences among conceptions. The aspects render the relation that a conception constitutes between an individual and the surrounding world as contextual (Marton and Booth 1997).

In our study, at first the focus in analysis was on the referential component, i.e., on what the interviewees meant with privacy on the level of everyday language. They described the details of privacy and the problems related to keeping their privacy. The interview texts were split in small items—each of them included one aspect or a problem of privacy. The items were categorized in order to obtain a single dimension of the categorization at time—first, the *what* aspect of the final categorization. The analysis continued by focusing on the structural component of privacy views. Structure is reached by analysing the target of the referential component. In the final categorization, this is the *how* aspect.

4 Result: Categorization of consumers' views

Our study deals with how consumers see information privacy. The results present different layers of understanding in two dimensions. The first dimension is the referential component which focuses on the meaning of privacy in the interviewees' everyday language (Table 3 columns A-E; *What*). The second dimension is the structural component which focuses on the form of

What / *How*	*A. Use and misuse of customer information*	*B. Monitoring consumers*	*C. Threat of spam*	*D. Danger of hackers and viruses*	*E. Risk with payment*
1. Product and e-vendor	1A	1B	1C	1D	1E
2. Technology	2A	2B	2C	2D	2E
3. Societal norms	3A	3B	3C	3D	3E
4. Consumer him/herself	4A	4B	4C	4D	4E
5. Fellow men	5A	5B	5C	5D	5E

Table 3: Summary of the categorization of consumers' information privacy conceptions in e-commerce

thought when the interviewees talk about privacy (Table 3 rows 1-5; *How*). By the two dimensions we identify a total of 25 different privacy conceptions. Table 4 includes one example of each conception to illustrate the content.

The referential component (the *what* aspect) of information privacy consists of five objects. *Use and misuse of customer information* includes consumers' personal information and how it is used, especially concerning its misuse. The second object, *monitoring consumers,* refers to monitoring consumers' actions when they are using e-commerce systems. *Threat of spam* refers to e-mails that a consumer interprets as spam as a part of privacy demands. *Danger of hackers and viruses* relates to hackers (who spread viruses) as a factor to intrude privacy. *Risk with payment* refers to issues related to making payments on the Internet that can create problems of privacy. The other dimension, structural components (rows in Table 3, or the *how* aspect) shows different forms of thought and stress the structural aspect of the conceptions. It includes five objects. When a consumer gives personal information in order to purchase a product in a certain e-shop, the focus is on products and maybe also on the e-vendor. Furthermore, there are systems (or technology) to deliver the product to the right person. It may be regarded as safer to order from the home country than from abroad (societal norms), the consumer may make an error when writing the order (consumer him/herself), and there may be a family member watching over his/her shoulder (fellow men).

4.1 Referential objects of information privacy

The referential objects (Table 3: columns) are presented in the order of which they were emphasized by the interviewees as a group, taking into account how much they discussed each object:

- All (22) interviewees talked about use and misuse of customer information.
- 20 interviewees talked about monitoring consumers.
- 15 interviewees talked about threat of spam.
- 14 interviewees talked about danger of hackers and viruses.
- 9 interviewees talked about risk with payment.

When the interviewees described information privacy, in most of the cases they connected it to possible problems. Four categories of the referential components focus on problems only and just one on both use and misuse. The result of our study does not state anything about the frequency of specific views among the whole population; however, all the five referential objects exist in people's thinking about privacy.

Object A: Use and misuse of customer information. In the interviews, the consumers mostly discuss their personal information as customer information. This is information which e-vendors collect by asking it from consumers. Some of the interviewees use the concept "customer information", others underline their own viewpoint by talking about "my information that my e-vendor has or knows". In general, the interviewees are reluctant to give their information and they are afraid of misuse of their personal information – but only if they do not know the e-vendor beforehand. Nevertheless, the consumers interviewed also understand the benefits of

	Conception	*Content illustrated with an example from the interviews*
Use and misuse of customer information	1A (product)	*The consumer gives personal details, e.g., when:* - he/she is familiar with the product.
	2A (technology)	- the system of registration is easy to use.
	3A (soc norms)	- he/she feels that laws ensure security.
	4A (consumer)	- he/she can give as little information as possible.
	5A (fellow men)	- his/her son helps to log in to e-vendor's pages.
Monitoring consumers	1B (product)	*The consumer feels that the use of e-commerce and personal information are monitored when:* - he/she is interested in products such as explosives.
	2B (technology)	- he/she thinks that the e-vendor gets logs of web visits without consumers' knowledge.
	3B (soc norms)	- a certain intelligence service may be monitoring.
	4B (consumer)	- he/she is not able to see the statistics of visits.
	5B (fellow men)	- a family member is watching over the shoulder.
Threat of spam	1C (product)	*The consumer receives mail that disturbs and invades personal privacy when:* - he/she participates in the e-vendor's lotteries.
	2C (technology)	- the system in his/her computer does not work properly.
	3C (soc norms)	- he/she uses foreign e-services, for example, newspapers.
	4C (consumer)	- until he/she started to use the filter program.
	5C (fellow men)	- until the son installed the filter program.
Danger of hackers and viruses	1D (product)	*The consumer believes that hackers use viruses to steal personal information when:* - the consumer uses "some strange" e-services.
	2D (technology)	- the computer is using a wireless connection.
	3D (soc norms)	- the consumer uses foreign e-vendors.
	4D (consumer)	- the consumer does not have a firewall.
	5D (fellow men)	- the son hasn't installed virus protection.
Risk with payment	1E (product)	*The consumer is not afraid to use e-bank and give personal information when:* - he/she knows that the e-vendor is reliable.
	2E (technology)	- the payment system uses secure actions.
	3E (soc norms)	- the payment transaction is conducted within one's own country.
	4E (consumer)	- he/she is familiar with the secure transactions.
	5E (fellow men)	- he/she asks advice from a net community.

Table 4: The contents of the conceptions illustrated with interview examples

getting personalized offers from e-vendors. One problem is that giving information is complicated (Conception 2A):

> But it (the registration) must not be made too difficult or complicated. There are so many registration forms; fill in this field, this one, that one, so I won't do it. I think, leave it. Anyway, I can't stand writing my whole biography to some registration (forms).

Object B: Monitoring consumers. The interviewees describe two kinds of monitoring. They tell that some one may watch when they are using the computer. This is the same as traditional monitoring: the one who is monitored and the one who monitors are in the same physical space. Besides of the traditional monitoring the interviewees are concerned if there exists virtual monitoring which happens over the Internet. For example, the interviewees state that some e-vendors keep an eye on consumer purchase behaviour or that the police monitors the Internet. Virtual monitoring means that the visits to websites are monitored secretly and information about Internet use is added to visitors' personal information. The interviewees claim that it should be a fundamental right (of Internet privacy) to visit web pages anonymously.

Some of the interviewees are more afraid of monitoring than others. The most careless ones say that monitoring occurs only on a small scale or that their personal information is not relevant to strangers. Some interviewees admit that they do not know enough – and they also do not like giving their personal information, because they do not actually know what happens to the information or what is possible to do over the Internet. One of the interviewees gives an example where her own level of knowledge about technology affects her concerns with consumer monitoring (Conception 2B):

> I've heard about user tracing. When I hadn't used the net for a very long time I got a notification saying 'you are running out of ink'. Oh my god, I thought, did I run out of ink so fast? Then I realized that it was an advertisement. I'm still wondering if they could know whether I was running out of ink.

Object C: Threat of spam. All the interviewees agree that unwanted e-mail is annoying and most of them see a conflict between spam and privacy. However, they clearly differentiate between spam and other uses of customer information (object: use and misuse of customer information); especially when the unsolicited mail or directed ads originate from their own e-vendor, it seems acceptable. We use the word "spam' because the interviewees cite the term; in addition, "garbage" and "junk" were also used. Spam usually refers to unwanted e-mails, which causes harm at least by filling, and occasionally choking (malicious attacks), one's mailbox. Still, it is difficult to determine whether an e-mail is wanted or not; for defining that, the recipients' interpretation is needed. Besides of defining what spam is, protection against it, and the consumers' own actions are important, as seen in the next quotation (Conception 3C):

> Of course, one factor is that if lots of spam start coming. -- But I haven't done any business with unfamiliar vendors and I have indeed avoided foreign firms - any contacts to them.

Object D: Danger of hackers and viruses. The concept of hacker is used here because the interviewees use it. They usually add that hackers use viruses to get their personal information

from e-vendors. While the interviewees trust in their own e-vendors' (in believing that they do not misuse consumers' personal information), the trust to the e-vendors' ability to protect consumers' information is rather low. The interviewees blame the e-vendors of not taking good care of their information. The next quotation from among the interviews presents an example (Conception 2D):

> If someone gets my personal information and can take money from my bank account. ... The way anyone can get to one's files and find whatever from them. Then someone indeed might empty my bank account … my empty bank account.

In the interviews, the danger of hackers and viruses is mentioned often, but the interviewees do not specify their views, not even when probed by the interviewer.

Object E: Risk with payment. This object refers to how issues related to making payment on the Internet entail privacy problems: the interviewees are concerned that credit card information can be stolen or used somewhere without their permission. Only a few of the interviewees report having used their credit cards on the web. Although most of them frequently use Internet banking, they do not talk about it in a context of risk with payments; the bank is seen as an institution that can be trusted it seems. E-shopping could be paid in two main ways according to the interviewees: with a credit card or in a post office when the consumer receives the product. The interviewees said that now it is also possible to pay e-shopping directly via an Internet bank.

The interview quoted below shows that even though some of the consumers interviewed may feel afraid using their credit cards, they have nevertheless used them because of the benefits perceived (Conception 1E):

> When you use some trustworthy and large vendors you get (the ordered product) in a week or so… Then you will get the right product at the right time, and the bill comes at the same time (with the product). When you pay with a Visa (credit card) it is chancy. I wouldn't otherwise use it (Visa credit card), but you have to use it (for paying) abroad. The products are cheaper there.

4.2 Structural components of information privacy

Besides the above mentioned referential objects, the categorization includes a second dimension, the structural components of information privacy. The components show different modes of thought and stress the structural aspect of the conceptions.

Component 1: Product and e-vendor. When privacy is understood as related to the component of the product and the e-vendor, all interviewees express very similar opinions. They say that it is easier to order and give information if you know exactly what you are getting and who the e-vendor is. First, the interviewees underline that they trust well-known e-vendors. They mentioned many familiar Finnish brands – such as Veikkaus (a betting company, also working online) and NetAnttila (an e-shop for clothes and household goods) – as places whereto it is safe

to give their personal information. The main principle seemed to be: you can only trust some companies on the web, not all.

Besides the familiarity of the e-vendor, the familiarity of the product also matters. It is easiest to buy online if the product is familiar and standard, as the following interview quotation illustrates (Conception 1E):

> If I want to order a bottle of Scotch once a month then I could type it there… as a payment to any international bank account. But if you do not know anything about the product…

Component 2: Technology. In the second component, privacy is understood through technology. The interviewees refer to technology using words such as "the system", "their computer", "my computer", and "e-vendors' register". In addition, the e-vendor's www-pages and their maintenance are understood as technology. The interviewees usually claim that information security, as far as privacy is concerned, refers to the security of a bank account or the confidentiality of a credit card number; they also mention firewalls or virus protection. However, the interviewees also mention many positive sides of e-commerce systems: for example, a system can check if there are typing errors; it is easier to compare different products; the use of an e-commerce system may be cheaper and faster. The use of technology may also be worthwhile from the consumer's viewpoint (Conception 2A):

> Computers are good, as they can check right away that you are doing the right thing. With a person, mistakes may happen. A computer admits without scruples when something is not working. If there was a person, it would take time before getting a comment that something is wrong.

Component 3: Societal norms. The interviewees describe that differences in national laws and behavioural norms affect on their actions in e-commerce. The third component is called *Societal norms* since it concentrates on others' expected behaviour based on images of commerce habits and technological expertise in certain countries. The interviewees have very strong views on security in different countries and the opinions are similar among all interviewees. They note that ordering from abroad is not safe; in other words, they would not give their personal information abroad. The interviewees emphasize their perception that information security is better in Finland, and that it is easier to give personal information to Finnish vendors than to others (Conception 3D):

> I have been interested in high quality artistic tools. And there (abroad) are plenty of them (artistic tools) that are not available here (in Finland). Sometimes I have tried to order them. However, there is still this problem of privacy... Some hacker may steal my information and I don't receive my packet at all.

Component 4: Consumer him/herself. The interviewees can also understand the implications of their own actions regarding privacy in e-commerce. The interviewees describe problems and how their own behaviour can provide solutions. The problems mentioned in this respect are

connected to the use of e-services, for example, to the difficulties of changing one's own personal information or remembering user names and passwords. The interviewees' policies vary. One solution is to avoid giving any information to the e-vendor, thus refusing to deal with e-commerce—the reason stated can be: "it is not safe". Another solution is to avoid giving one's own personal information, using a fake personality instead, such as Donald Duck. The third solution is to use the power of a community, which is easier via the Internet, as explained in the following quotation (Conception 4E):

> I've often noted that it (virtual community) is a very good deterrence. If after buying you go somewhere (to a virtual community) and you ask whether this should be really so and so… Usually when the firm finds out that somebody has been making inquiries about their products, the service can improve suddenly.

Component 5: Fellow men. Besides of the interviewee's own actions there are other people whose actions affect the interviewee's privacy situation. Focusing on the whole interviewing situation the interviewees also described what problems other people could cause to them. In the category of Fellow men, the people are known by name and they belong to the same community as the interviewee. They can be family members, work colleagues, or friends – also from a virtual community. These known persons can help in the use of e-commerce, but they can also cause harm, as in the next interview quoted, in which the interviewee discusses monitoring which injures privacy (Conception 5B):

> When I am using the computer, there can be so-called distractions. I find them disturbing. (-) Sometimes my husband is trying to peek at what I am doing.

5 Discussion

Our study dealt with how consumers view information privacy. The result is a categorization, which reveals consumers' anxiety in the referential objects of privacy (use and misuse of customer information, monitoring consumers, threat of spam, danger of hackers and viruses, risk with payment). When we discussed privacy with the interviewees, they pointed our several risks and threats. In the categorization, only one object, use and misuse of customer information, contains both positive and negative sides of privacy; all other objects of privacy are regarded as rather negative. Besides of the objects, we also identified the structural components of thought about privacy. These were: product and e-vendor, technology, societal norms, consumer him/herself, and fellow men.

As we described earlier, there are contradictory views about consumers' fears of information privacy. While several studies (Cassidy and Chae 2006; Chung 2003; Liu et al. 2005) state that consumers are worried of their personal information use in e-commerce, Cheung and Lee (2006) state that consumers are not afraid of invasions of privacy. Our study explains one reason for the contradictory findings. Cheung and Lee studied the fears of privacy concerns in the con-

text of e-commerce with known e-vendors. The consumers were asked to evaluate the following statements (Cheung and Lee 2006):

1. Internet vendors will sell my personal information to third parties without my permission,
2. Internet vendors' are concerned about consumers' privacy,
3. Internet vendors will not divulge consumers' personal data to other parties.

Cheung and Lee (2006) found that consumers trust the e-vendor with who they make commerce and have no fear of the e-vendor misusing their personal information. Our study verifies that only few consumers fear invasion of privacy caused directly by their own vendors. Nevertheless, this does not mean that consumers do not have any concerns. Instead, the interviewees were afraid of anonymous surveillance, spam (other than that related to their vendors) and hackers using viruses – which might be the context of other information privacy studies.

Already before our study, we knew that consumers' privacy behaviour varies. Westin presented three types of people in this respect: privacy fundamentalists, unconcerned and pragmatists (Taylor 2003). Westin's segmentation is a useful conceptual framework when thinking about how an e-service might be used; however, it does not work when the focus is a consumers' point of view. The consumers interviewed about privacy do not demonstrate a single attitude; instead, they act differently in different situations and contexts.

Our study indicates that Internet privacy is not a stable and homogenous concept to consumers. While in one case the interviewee described herself as being careful about what information she gave to an e-vendor, in another case she was not that concerned about information privacy. She was not concerned when she acted with her own bank and e-supplier, since she had used their e-services several times. She seemed to feel safe in familiar situations, but in a new situation with an unknown vendor she is careful and does not provide whatever information. To get a good idea of the consumer's privacy views, the informant needs to be asked to describe both familiar situations, such as e-banking and e-actions with a long-standing vendor, and new situations in which the vendor is unknown as in casual Internet purchasing activities. In some studies (e.g., Cheung and Lee 2006) this differentiation was not used.

Furthermore, the chosen method (phenomenography) focuses on the second-order perspective, which means that we described consumers' views on privacy in e-commerce as perceived by a certain group of people. This kind of approach helps to understand the variety of conceptions of privacy. When the nature of the concerns is understood, it offers building blocks for further research. For example, the researchers have to take situationality into account also in the case of information privacy.

In phenomenography the world is described the way informants see it. The validity of the study is based on that some informants (or at least one informant) see the phenomena via the described conceptions. However, some of the conceptions can be totally unrealistic and against the current scientific knowledge about the phenomenon. For example, one of the interviewees quoted previously was wondering whether somebody, through the Internet, could know when the ink was running short in her printer. The example illustrates how consumers' unjustified fears might affect their judgement. Thus, unrealistic statements forming part of (some) consum-

ers' views on the phenomenon, need to be analysed as well in order to understand the variety of consumers' thought-models.

Our experiences indicate that the method of phenomenography is rich and rewarding, but at the same time, that the method requires time and hard work. Since there are no formal data gathering and analysis methods (for example as compared to grounded theory) and as the research is conducted phase by phase, phenomenography demands good organizing skills from the researcher.

Phenomenography is a qualitative method, and is therefore prone to the same potential limitations as other qualitative studies. One of these limitations is the impossibility of determining when the number of informants is sufficiently large. About twenty informants is said to be a large enough group for a theoretical saturation (e.g., Alexandersson 1994). We had 22 interviewees which seem to be enough, since the same objects and views were repeated, and the last informants did not contribute new elements to the categorization.

For e-vendors, the results of this study show that it is crucially important to understand online consumers' concerns about privacy in order to maximize the potential of e-commerce. Understanding how consumers view privacy issues provides a means to understand whether people would be open to marketing efforts which require information sharing and information exchange. In addition, the results help to understand what safeguards and other actions must be in place to ensure that consumers are willing to give their information and use e-commerce systems. The interviewees regard e-vendors as benevolent but not sufficiently competent in taking care of information privacy. For taking better care about privacy and making the care-taking visible to their customers the e-vendors should:

- describe how consumers' personal information is taken care of and used,
- give consumers more advice on giving and handling personal information safely,
- state if some third party is allowed to use their personal information for marketing purposes,
- take good care of their own brands, reputation and usability,
- enable their customers to check, correct and delete their own personal information, and
- be worthy of trust.

6 Conclusion

The aim of this study is to describe the differences in how consumers view privacy in e-commerce. In privacy issues we need more understanding from a consumer viewpoint (Cassidy and Chae 2006; Dinev et al. 2006; Malhotra et al. 2004). The result of our study is a categorization of consumers' views on information privacy. It includes different layers of understanding by focusing on referential objects and structural components of information privacy.

Besides of the categorization itself, an important finding is that consumers' views on privacy (and privacy concerns) are situated; it depends on the context. A familiar situation—e.g., acting with a known e-vendor—is regarded as safe, whereas a new, unknown situation is seen as fearful and risky. New experiences (e.g., using a new web site several times) and new information (e.g., from media) affect the consumer's behaviour. The view of privacy should thus not be regarded as stable, but as constantly under social construction.

7 Acknowledgment

The authors would like to gratefully acknowledge the helpful comments on earlier versions of this paper from the Associate Editor, Professor Bjørn Erik Munkvold, the three anonymous reviewers, Dr Hannakaisa Isomäki, Professor Pertti Järvinen, Dr Minna-Kristiina Paakki, Dr Tero Vartiainen, and the members of Dr Viveca Asproth's working group in IRIS28 - 2005, Kristiansand, Norway. We thank Steve Legrand for making our English more readable.

8 References

Alexandersson, M., *Metod och medvetande, (Method and Awareness, in Swedish),* Acta Universitatis Gothoburgensis, Göteborg, 1994.

Alvesson M., and Karreman, D., "Varieties of discourse: On the study of organizations through discourse analysis", *Human Relation,* (53:9), 2000, pp. 1125-1149.

Awad, N. F. and Krishnan, M. S., "The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to be Profiled Online for Personalization", *MIS Quarterly,* (30:1), 2006, pp. 13-28.

Bellman, S., Johnson, E. J., Kobrin, S. J., and Lohse, G. L., "International differences in information privacy concerns: a global survey of consumers", *The Information Society,* (20), 2004, pp. 313-324.

Bergkamp, L., "EU data protection policy. The privacy fallacy: adverse effects of Europe's data protection policy in an information-driven economy", *Computer Law & Security Report,* (18:1), 2002, pp. 31-47.

Booth, S. A., *Learning to program: A phenomenographic perspective*, Acta Universitatis Gothoburgensis, Göteborg, 1992.

Bygrave, L. A. "Data Protection Pursuant to the Right to Privacy in Human Rights Treaties", *International Journal of Law and Information Technology,* (6), 1998, pp. 247-284

Camp, L. J., and Osorio, C., *Privacy Enhancing Technologies for Internet Commerce,* Trust in the Network Economy, Springer-Verlag, Berlin, Germany, 2003.

Cassidy, C. M., and Chae, B., "Consumer Information Use and Misuse in Electronic Business: An Alternative to Privacy Regulation", *Information Systems Management,* Summer 2006, pp. 75-87.

Cheung, C. M. K., and Lee, M. K. O., "Understanding Consumer Trust in Internet Shopping: A Multidisciplinary Approach", *Journal of the American Society for Information Science and Technology,* (57:4), 2006, pp. 479-492.

Choughury, V. and Karahanna, E., "The Relative Advantage of Electronic Channels: A Multidimensional View", *MIS Quarterly* (32:1), 2008, pp. 179-200.

Chung, W., "A Snoop at Privacy Issues on the Internet in New Zealand", *Business Review*, University of Auckland, (4:3), 2003, pp. 2-15.

Curran, C. M., and Richards, J. I., "Misplaced Marketing. Public Privacy and Politics", *Journal of Consumer Marketing*, (21:1), 2004, pp. 7-9.

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

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.

Eriksen, T. H., *Small Places, Big Issues. An Introduction to Social and Cultural Anthropology,* Pluto Press, London, UK, 2001.

Gefen, D., Karahanna, E., and Straub, D. W., "Trust and TAM in Online Shopping: an Integrated Model", *Management Information Systems Quarterly*, (27:1), 2003, pp. 51-90.

Glaser, B. G., and Strauss, A., *The Discovery of Grounded Theory, Strategies for Qualitative Research,* Aldine publishing company, Chicago, 1973.

Grable, J. E. and Joo, S., "Factors related to risk tolerance: a further examination", *Consumer Interests Annual,* (45), 1999, pp. 53-58.

Graeff, T. R., and Harmon, S., "Collecting and using personal data: consumers' awareness and concerns", *Journal of Consumer Marketing,* (19:4), 2002, pp. 302-318.

Hui, K.-L., Teo, H. H., and Lee, S.-Y. T., "The Value of Privacy Assurance: An Exploratory Field Experiment, *MIS Quarterly* (31:1), 2007, pp. 19-33.

Hynes, D., Tiainen, T., Koivunen, E.-R., and Paakki, M.-K., "Articulating ICT Use Narratives in Everyday Life", In EM Trauth (Ed.), *Encyclopedia of Gender and Information Technology*. Idea Group Reference, London, UK. 2006, pp. 37-43.

Isomäki, H., *The Prevailing Conceptions of the Human Being in Information Systems Development: Systems Designers' Reflection,* Department of computer and information sciences, University of Tampere, Tampere, 2002.

Jensen, C., Potts, C., and Jensen, C., "Privacy practices of Internet users: Self-reports versus observed behavior", *International Journal of Human-Computer Studies* (63), 2005, pp. 203-227.

Kahle, L. R., Beatty, S. E., and Homer, P, "Alternative Measurement Approaches to Consumer Values: The List of Values (LOV) and Values and Life Style (VALS)", *Journal of Consumer Research,* (13), 1986, pp. 405-409.

Kruck, S. E., Gottovi, D., Moghadami, F., Broom, R., and Forcht, K. A. "Protecting personal privacy on the Internet", *Information Management & Computer Security,* (10:2), 2002, pp. 77-84.

Liu, C., Marchewka, J. T., Lu, J., and Yu, C-S., "Beyond concern—a privacy-trust-behavioral intention model of electronic commerce", *Information and Management,* (42), 2005, pp. 289-304.

Malhotra, N. K., Kim, S. S., and Agarwal, J., "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model", *Information Systems Research,* (15:4), 2004, pp. 336-355.

Marton, F., "Phenomenography – describing conceptions of the world around us", *Instructional science*, (10), 1981, pp. 177-200.

Marton, F., *Towards phenomenography of learning, Integratial experiments aspects,* University of Gothenburg Dept. Education, Gothenburg, 1982.

Marton, F., and Booth, S., *Learning and awareness.* Mahwah, N.J.: Lawrence Erlbaum, 1997.

McRobb, S., and Rogerson, S., "Are they really listening? An investigation into published online privacy policies at the beginning of the third millennium", *Information Technology & People,* (17:4), 2004, pp. 442-461.

Milberg, S. J., Burke, S. J., Smith, H. J., and Kallman, E. A., "Values, personal information privacy concerns, and regulatory approaches", *Comm. ACM*, (38:12), 1995, pp. 65-74.

Muttilainen, V., "Suomalaiset ja henkilötietojen suoja. Kyselytutkimusten ja viranomaistilastojen tietoja 1990-luvulta ja 2000-luvun alusta", (Finnish people and security of personal information. Surveys and statistics of state authority 1990's and in the beginning of 2000, in Finnish), Oikeuspoliittisen tutkimuslaitoksen julkaisuja, (218), Oikeuspoliittinen tutkimuslaitos, Helsinki, 2006.

Paine, C., Reips, U.-D., Stieger, S., Joinson, A., and Buchanan, T., "Internet users' perceptions of 'privacy concerns' and 'privacy actions'", *International Journal of Human-Computer Studies*, (65), 2007, pp. 526-536.

Pan, Y. and Zinkhan, G. M., "Exploring the impact of online privacy disclosures on consumer trust", *Journal of Retailing Volume* (82:4), 2006, pp. 331-338.

Phelps, J., Nowak, G., and Ferrell, E. "Privacy Concerns and Consumer Willingness to provide Personal Information", *Journal of Public Policy Marketing,* (19:1), 2000, pp. 27-41.

Prabhaker, P. R., "Who owns the online consumer?", *Journal of Consumer Marketing,* (17:2), 2000, pp. 158-171.

Rubin, P. H., and Lenard, T. M., *Privacy and the commercial use of personal information,* Boston: The Progress & Freedom Foundation / Kluwer Academic Publishers, 2002.

Smith, H. J., "Information Privacy and Its Management", *MIS Quarterly Executive,* (3:4), 2004, pp. 291-313.

Smith, H. J., Milberg, S. J., and Burke, S. J., "Information privacy: Measuring individuals' concerns about organizational practices", *MIS Quarterly,* (20:2), 1996, pp. 167-196.

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

Säljö, R., "Minding action. Conceiving the world versus participating in cultural practices", *Nordisk Pedagogik*, (14), 1994, pp. 71-80.

Taylor, H., "Most people are "privacy pragmatists" who, while concerned about privacy, will sometimes trade it off for other benefits", *The Harris Poll,* (17), 2003, March 19.

Udo, G. J., "Privacy and security concerns as major barriers for e-commerce: a survey study", *Information Management & Computer Security,* (9:4), 2001, pp. 165-174.

Vartiainen, T., "Moral Conflicts in Teaching Project Work: A Job Burdened by Role Strains", *Communications of the Association for Information Systems,* (20, article 43), 2007.

Verhagen, T., Meents, S., and Tan, Y.-H., "Perceived risk and trust associated with purchasing at electronic marketplaces", *European Journal of Information Systems* (15), 2006, pp. 542–555.

Westin, A. F., *Privacy and Freedom*, Atheneum, New York, 1967.