Association for Information Systems
AIS Electronic Library (AISeL)

ECIS 2009 Proceedings

European Conference on Information Systems (ECIS)

2009

Consumers' acceptance and use of personal health record systems: A theoretical model

Mirella Lahteenmaki
Helsinki School of Economics, mirella.lahteenmaki@hse.fi

Johanna Bragge
Helsinki School of Economics, johanna.bragge@hse.fi

Anne Sunikka
Helsinki School of Economics, anne.sunikka@hse.fi

CONSUMERS' PERCEPTION OF CONTROL OVER ONLINE INFORMATION DISCLOSURE. AN ELECTRONIC FOCUS GROUP STUDY

Lähteenmäki, Mirella, Helsinki School of Economics, Runeberginkatu 14-16, 00100 Helsinki, Finland, mirella.lahteenmaki@hse.fi

Bragge, Johanna, Helsinki School of Economics, Runeberginkatu 14-16, 00100 Helsinki, Finland, johanna.bragge@hse.fi

Sunikka, Anne, Helsinki School of Economics, Runeberginkatu 14-16, 00100 Helsinki, Finland, anne.sunikka@hse.fi

Abstract

This study focuses on consumers' perception of control over personal information disclosure on the Internet. Specifically, we examine how consumers perceive controlling their personal data that online companies collect for marketing and customer relationship management purposes. We aim to answer this research problem by clarifying 1) how do consumers express the perception of control over their personal information, and 2) how do consumers perceive controlling their personal information disclosure. Our empirical data is based on four computer-mediated focus group interviews. Our findings show that the perception of control is combined with all stages of personal data utilization: collection, storage and usage. Thus, consumers keep these stages in mind when thinking about their attitudes towards the collection and offering of their personal information. The interviewees also spontaneously mentioned various means with which they control personal data. Perceived trust towards companies, own initiative and permission-based marketing were also combined to the control speech. In summary, the interviewees mostly perceived that they were not controlling their personal data on the Internet. Only when they were talking about control methods of the information disclosure stage, they expressed the perception of control.

Keywords: Privacy, Online self-disclosure, Perception of control, Focus groups.

1 INTRODUCTION

The development and adoption of information and communication technologies (ICT) among consumers have enabled large-scale utilization of personal data for marketing purposes (Moon 2000). With personal data we mean information that can be connected to an identifiable individual (Culnan & Milberg 1998). This information can be grouped to identifier information (such as an e-mail address), sensitive personal data (information concerning e.g. health), and preference information (e.g. hobbies) (Andrare, Kaltcheva & Weitz 2002). Especially in the Internet, consumers increasingly face situations in which they have to provide personal data for some purpose (Heikkinen et al. 2004). Ordering and buying products, experimenting and adopting e-services, and registering into various loyalty customer programs are typical examples of situations in which submission of personal data is required. The data collection is often well justifiable from the consumer's point of view; for example an e-commerce site needs customers' contact information in order to deliver purchases, or to inform customers about possible delivery problems. However, companies collect personal data also for other purposes, for example to be able to advertise their products, or to utilize data in some other way in the future. This is usually acceptable, sometimes even good customer service. However, the customer should be aware 1) that her personal data is utilized, and 2) of the rights granted to her by legislation (e.g. the rights of inspecting, correcting, and prohibiting the usage of personal data). Customers should be able to execute these rights also in practice (Personal Data Act 1999, Velasquez 2006: 290-291).

According to several studies (e.g. Sayre & Horne 2000, Dommeyer & Gross 2003, Chellapa & Sin 2005), most consumers accept the collection and utilization of their personal data for marketing and customer relationship management (CRM) purposes in return for proper benefits. However, privacy questions have received much attention during the last few years (Milne 2000). According to several studies (e.g. Phelps et al. 2000, Eurobarometer 2008, Privacy & American Business 2004) consumers are concerned about their privacy, especially in the Internet. To some extent, the Internet is experienced as an unreliable and unsecure environment (e.g. Knights et al. 2001, Suh & Han 2003, Jensen et al. 2005).

Privacy itself is a multidimensional and ambiguous concept, the definition of which is often based on sociologist Alan Westin (1967, p. 7): Privacy is both control over 1) information disclosure and 2) the environment in which transactions occur. The first dimension is concerned with control over own information, while the latter with the control over one's own state and of protection from different external intrusions, such as spam. In this study, we concentrate on the first dimension, on control over providing personal data, which, according to Goodwin (1991), can be seen to include also other control aspects than just disclosure regarding personal data utilization. Posner (1981), for example, refers to privacy violation when observing an individual without disturbing her concretely.

Research over personal information control has traditionally emphasized control over the consumers' environment, for instance the intruding nature of direct marketing (e.g. O'Malley et al. 1997, Evans et al. 2001, Morimoto & Chang 2006). This area has been regulated, e.g., by establishing prohibition registers for marketing measures. Nevertheless, ICT-enabled interactive marketing actions pose more serious threats to consumers' personal data control. Goodwin (1991) includes the risk of potentially harmful usage to the control over personal data – it is for instance possible to combine separate pieces of personal data and registers together. In that case, the decision whether to disclose or not a single piece of data will be of minor significance with respect to data protection.

The control over disclosing personal data has been examined in connection with several studies (e.g. in Phelps et al. 2000, Sheehan & Hoy 2000, Evans et al. 2001), where it has been found an important factor affecting the provision of data. However, the control over disclosure has seldom been the main focus in privacy studies, apart from a few exceptions. For example, Goodwin (1991) has examined privacy conceptually as the control over personal data and own environment, whereas Olivero and Lunt (2004) have studied whether the consciousness data collection influences the control and trust of consumers. On the other hand, the methods consumers are using to control their personal data have been widely studied (e.g. Foxman & Kilcoyne 1993, Cranor et al. 1999, Dommeyer & Gross 2003).

The objective of our research is to increase the understanding of consumers' perceived control over their personal data that companies operating on the Internet collect for marketing and CRM purposes (see e.g. Milne 2000, Romano & Fjermestad 2003). Consequently, we restrict our study to this business-to-consumer context as distinct, for example, from authority transactions or criminal operations. We aim to answer our research problem by investigating 1) *how do consumers express the perception of control over their personal data*, and 2) *how do consumers perceive controlling their personal information disclosure*. Next, we will present the research methodology and data, after which we discuss our results in Section 3. The study finishes with discussion and conclusions.

2 RESEARCH METHODOLOGY AND DATA

A number of research techniques have been developed in order to better understand consumers, and to assess their desires and preferences. These techniques include surveys, focus groups, statistical modeling, and video ethnography (Prahalad & Ramaswamy 2004). As control over information disclosure has been previously studied mostly in connection with privacy surveys (see review in Kobsa 2007), we felt that an in-depth qualitative study is warranted in order to get a more comprehensive view on the topic. Thus, we chose focus groups as our research method.

The research data was collected in Finland in September 2006 through focus group interviews that were conducted electronically via computers in the same-time – same-place mode (Kontio et al. 2007). That is, the participants were invited to a computerized meeting room to answer structured questions presented by the researchers, and also to comment on each others' thoughts. This mode represents focus group *interviews* instead of focus group *discussions* (see Boddy 2005), as we wanted to receive answers from every participant, and also to prevent the derailing from the issue that easily happens in more free-form discussions. We utilized a group support system (GSS) called GroupSystems® MeetingRoom, which has originally been designed to support teamwork and group decision making (Nunamaker et al. 1991), but which can equally well be used for carrying out of focus group interviews or discussions (Clapper & Massey 1996, Kontio et al. 2007, Tellefsen et al. 2005). A typical GSS meeting consists of 10-30 networked computers in the same room, which gives the facilitator and the interviewees the opportunity to communicate also verbally with each other. It is also possible to conduct fully virtual meetings via the Internet (Klein et al. 2005, Kontio et al. 2007), but these require usually audio or web conferencing support in addition. The utilization of different computer-mediated systems in marketing and consumer research has been steadily increasing (see e.g. Montoya-Weiss et al. 1998, Sweet 2001, O'Connor & Madge, 2003).

Our study comprised of four group sessions, each lasting 2.5 hours, with 11-14 interviewees in each group. The sessions were administered by the same main facilitator and two other adjunct facilitators. The interviewees were posed a small set of related questions at a time, and they were allowed to answer them in the order they wished, before the facilitator let them proceed to the next bundle of questions. The interviewees saw each others' answers, and they were allowed to comment on them or to further deliberate on their own answers. We opted to carry out the sessions fully anonymously so that all the comments remained individual. After each session ended, all the interview answers were immediately available in writing using the automated reporting function of the GSS tool. This was one important reason for selecting computer-mediated instead of traditional focus groups as the research method, as our research partner (retail bank) needed to have the preliminary results as soon as possible in order to plan a subsequent field experiment at its online bank (see Bragge et al. 2007 for details).

The computer-mediated focus group interviews can be seen as an intermediate form between traditional face-to-face and fully virtual focus groups (Kontio et al. 2007). Some of the strengths of the method compared to traditional oral interviews are, for example, their efficiency (enabling bigger group sizes, simultaneous communication, and automated reporting), digital group memory during and after the sessions, as well as anonymity. The advantages compared to a fully virtual implementation are the possibilities to detail questions further, to interact verbally, as well as to present confidential or physical support material (such as product prototypes) during the sessions. The weaknesses of the method compared to traditional groups are certain deficiencies in expression (the lack of gestures and facial expressions in communication), the need for special premises and technical expertise, and the possibility for technical problems. Compared to fully virtual discussions the computer-mediated same-place settings place restrictions on the participants' geographical recruiting and are more expensive with respect to travelling expenses and venue costs (Klein et al. 2005, Kontio et al. 2007). As the topic of online information disclosure and the control thereof is fairly abstract, we did not consider fully virtual focus groups. In face-to-face settings possible ambiguities can be easier clarified.

Altogether 53 persons participated in our interviews in four groups, which is considered as a good amount for focus groups (Morgan 1996). The pilot group consisted of 14 business university students using online banking services. The other interviewees were randomly selected from among the online customers of a Finnish retail bank. Thus, the interviewees had at least basic computer skills to be able to participate in the electronically mediated interviews, in addition to which they were able to draw from their own experience when asked opinions about online information disclosure. Furthermore, the previous online bank usage made it possible for the interviewees to refer to a concrete context regarding the questions that might otherwise have felt too abstract for them. Thirty of the participants were female and 23 were male, all between the ages of 21 and 49. Occupationally, the interviewees were mainly higher or lower level officials (26), students (20) or workers (11). The majority of the interviewees used Internet daily (46); either at home (33), at work (28) and/or at their study place (11).

The underlying setting was a situation in which a reliable company (for example a bank) collects information online in order to utilize it for marketing and CRM purposes (e.g. for personalized advertising or services). This way we wanted to guarantee that the context experienced by all interviewees would be similar, and that no extreme context or experience (e.g. a foreign e-auction) would affect the answers too much. Furthermore, we were able to inquire their attitude also for the collection of sensitive personal data (concerning e.g. financial situation). Our questioning frame covered the following themes: 1) attitudes towards the collection of personal data on the Internet; 2) the recognition and control over collection and utilization of personal data online; 3) the understanding of the privacy protection concept. Thus, we were able to examine the control and disclosure of personal data both with direct questions and indirectly, without prompting the interviewees too much.

We asked the interviewees' attitudes also towards the personalization of online services and to the utilization of personal data especially in the banking sector (see Sunikka et al. 2007). These questions are here dealt with only in so far as they are related to the control over information disclosure.

The content analysis of our data started from the question that was presented to the interviewees: "*Do you perceive that you are in control over the collection and utilization of your personal information on the Internet*?". Utilization, which consumers often understand as usage was brought up in addition to collection, because one can see that the purpose of usage affects the disclosure of personal data (cf. Andrare et al. 2002). First, we developed conceptual labels attached to the interviewees' verbatim descriptions. Second, based on these conceptual labels, categories were formed at a more abstract level of classification. At the same time, the labels were constantly revised by merging categories expressing similar concepts, or by splitting a category representing different concepts (cf. Olivero & Lunt 2004). The categories thus formed were **1) disclosing, 2) storing, 3) usage,** and **4) control methods of personal data**. Finally, these main categories were studied thoroughly using the whole data that was collected. This was done by coding the data according to the formed categorization.

3 RESULTS

We will next present the analysis of the empirical findings of this study. Firstly, we will examine what kind of expressions the interviewees used when talking about the control over personal information on the Internet. Secondly, we will examine how the control over personal information in the Internet context is perceived by the interviewees.

3.1 The conception of control over personal data

The control over personal data proved to be an important theme. The interviewees brought it up when asked directly; in 39 of 56 comments the interviewees stated that they do not perceive that they are in control over the collection and utilization of their personal data online. Furthermore, the interviewees spontaneously expressed their concerns about the storage of personal data indicating a fear that third parties could get a hold on the information. This fear was mentioned in 31 (out of 55) comments for the question that inquired the interviewees' own definition of data privacy protection. Furthermore, 14 comments were connected to the protection from undesirable usage. From the viewpoint of companies, the collection, storing and usage of personal data forms a *process of personal data utilization*, about which the interviewees thus talked with a negative tone because of their perceived lack of control.

The interviewees talked positively mainly about the methods of control, such as restricting the disclosure of their personal data. Thus, when talking about the control methods, the interviewees expressed the control perception of their data. The methods of control were connected mainly to the offering stage, and the main method was the decision not to disclose personal data. In most answers, the methods of control were blended with expressions of the control perception. In a couple of cases the interviewees, however, expressed both the lack of control and the deployment of control methods somewhat conflictingly at the same time: *"I do not perceive well enough [that I am in control over the collection and utilization of my personal information on the Internet]. On the other hand, a huge amount of issues can be found out, but one must be critical herself and choose whom to believe".*

The interviewees also talked about own initiative and permission-based marketing, which can be seen as one type of control manifestations (see Milne & Gordon 1993, Evans et al. 2001). With own initiative the interviewees referred mainly to the desire to make the first move themselves in instigating a customer relationship (pull approach), and not just being a passive target for advertising. If customers perceive themselves as objects of push marketing, personal data is not willingly disclosed: *"…one must still always be careful, where to provide personal information. It is always better if you have created the contact yourself, than if it would be an impulsive answer to some advertisement."* The motives behind taking own initiative were the control over own environment (e.g. restricting targeted advertising), and control over own information: when consumers take the initiative themselves, it is easier for them to act deliberately. This view is compatible with the contemporary conception of an active consumer (Pavlou et al. 2002).

Regarding permission-based marketing the interviewees expressed their desire to make a conscious decision of whether to accept the utilization of personal data, and to control their own information this way. The benefits gained from providing personal data were emphasized. *"It is rather understandable [that companies collect information from and about you], but the protection of privacy is, of course, put to the test. To become a victim of, for example, advertising or spamming, is slowing down the computer and thus really strenuous. If the information I receive is related to my own interests, and approved by me, then it is quite OK".* A few interviewees (8/55 comments) associated the permission-based marketing system with their perception on privacy protection. In general, the fact that permission is asked before collecting and utilizing data for marketing purposes was appreciated.

Finally, the trustworthiness of a company (also its familiarity, or an existing customer relationship) added the willingness to disclose personal data. In addition to personal experiences, the interviewees' trust was increased if the company is known or domestic, in which case the reputation of a company and the legislative environment (domesticity) increased the feeling of safety. A similar typology of trust was presented also by Milne & Boza (1998) regarding consumers' views on utilizing personal data in marketing. In their study, the trust was manifested in earlier experiences of the company, in the reputation of the company, and in the confidence which is based on regulation or agreement.

Trust in a company was often mentioned as a prerequisite for the disclosure of personal data. We could interpret from the interviewees' comments that trust increases the perception of control, in other words trust itself is a control method, which is also a prevailing view in the literature (see for example Cranor et al. 1999): *"The disclosure of data to small, unknown companies nearly always raises doubts about where the information is used. If a piece of information seems irrelevant to the issue at hand, I will not usually disclose it."* On the other hand, trust compensates the need for control on the pursuit of privacy protection, especially on the Internet (e.g. Milne & Boza 1998, Olivero & Lunt 2004).

The different manifestations of the control speech are presented in Figure 1. The interviewees expressed the control perception of their personal information mainly through control methods, such as restricting the disclosure of personal data. The control perception was manifested also by the interviewees' own initiative, by permission-based marketing, and by the trust in the company. The methods of control were applied especially to the disclosure of data, which was otherwise experienced to be poorly in control. Merely with the decision whether or not to disclose data the interviewees control their own data and their privacy. On the other hand, the interviewees did not perceive that they were in control over the storage or usage of personal data, not even when utilizing control methods.

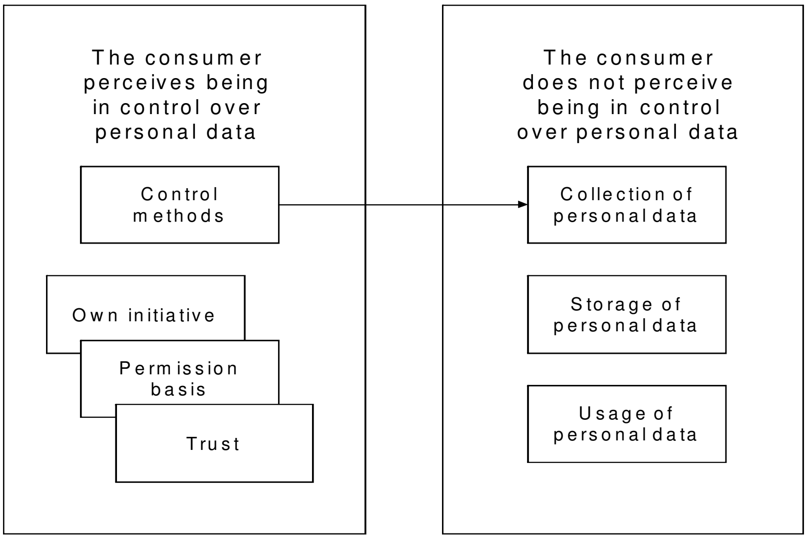
The consumer perceives being in control over personal data
Control methods
Own initiative
Permission basis
Trust
The consumer does not perceive being in control over personal data
Collection of personal data
Storage of personal data
Usage of personal data

Figure 1. The manifestations of the control speech among the interviewees.

In the following four sections we will deliberate on the four main classes we found when analyzing our interviews: (1) disclosure, (2) storage, (3) usage and (4) control methods of personal data.

3.2 Avoidance of disclosure of personal data to companies on the Internet is difficult

The interviewees experienced that it is difficult to avoid the disclosure of personal data on the Internet since personal data is collected everywhere, even when the consumers do not notice it. In the interviewees' opinion, companies can too easily access the personal data of consumers. Additionally, there are more and more situations in which information must be disclosed, even though one would not want to. According to several interviewees, the companies in general collect too many personal data. Similar results were obtained also in a study by Statistics Finland (Muttilainen 2007), in which 28 per cent of the respondents experienced having given too much information of themselves. Alike thoughts were presented already in the 1970's in opinion polls (see e.g. Katz & Tassone 1990). Thus, the attitudes seem to have remained comparable in spite of the increase in the digital data collection.

The interviewees often experienced that the data collection is not always necessary. *"I understand the objectives of companies to get the best possible picture and profile from the customers, but there should be sensible limits to it. One could think that the information on what are my hobbies or which country I have last visited would hardly be useful to anyone."* The interviewees' views are supported by numerous studies (e.g. Sayre & Horne 2000, Dommeyer & Gross 2003, Chellapa & Sin 2005, White et al. 2008), according to which consumers want to gain more in exchange for the disclosure of their personal information. Furthermore, unnecessary inquiries are regarded as time-consuming and irritating. In our study, the perceived purposelessness of the data collection was the most common reason for not disclosing personal information.

The data registers were regarded as problematic: a few interviewees felt that the storing of personal data in registers is uncomfortable. Furthermore, some felt it difficult to remember afterwards what information they had given and to whom. The interviewees commented that they did not know any more what the companies knew about them, or whether this information was up-to-date. They hoped for the possibility to access their own data and also to edit or delete it, when wanted. Thus, the interviewees were not particularly aware of their own rights (e.g. to inspect personal data in registers), or the exercise of the rights was regarded as difficult in practice. On the other hand, the online data collection was regarded as a more reliable method of acquiring data than other means, as the data did not disappear or change when processed (e.g. when using traditional forms). In the opinion of a few interviewees, the privacy protection requires also the consumers' own activity and carefulness: *"Firms get a lot of data easily; it is given without thinking about it too much."* On the other hand, they admitted that they are sometimes careless themselves and disclose data without consideration.

Several interviewees experienced that a lot of personal data is collected without telling it to the consumers, of which they disapproved: *"In a way I perceive that I am in control over the collection of information. However, the information can be gathered in a way that one does not notice it, one does not even always understand how the collection of information on something might be significant ...".* In this comment, the possibility of disclosing information accidentally emerged; consumers do not always understand the consequences of information collection. Also the risk of information acquisition by combining data from several registers was mentioned. Furthermore, the interviewees were worried about data collection that is enabled by recording and analysing click-stream data, or using other methods. In general, the interviewees felt uncomfortable being observed.

The majority of the interviewees (46 of 57 comments) were not sufficiently aware of the collection of personal data online or the usage of the information when asked directly. Especially the purpose of use of personal information puzzled most interviewees. It was also challenging to stay ahead of the technological development; for example cookies were experienced as threatening. The reasons for the unawareness were both consumer-driven (e.g. lack of interest and passiveness) and company-driven (e.g. the difficulty of getting information when one needs it).

Finally, several interviewees commented that one is occasionally compelled to give information to service providers. Companies might request information that is essential for the functionality of the service (e.g. alert services), and then the data collection was regarded as justified. Often the interviewees, however, experienced that they had to give information of lesser importance or of sensitive nature to be able to conduct transactions, even if they would not have wanted that: *"If I took the initiative myself, then I would react neutrally to the fact that a company needs information e.g. for granting a loan decision. If, on the other hand, the company has phished my contact information, or if I am otherwise unable to proceed on a company's website without answering all required questions, that is really irritating. I don't like it either if a really long form with many compulsory fields must be filled in (especially when asking home address, social security number, children's names etc.) in order to be able to register as a user to some service."* In this example the usability of the answer form (e.g. the plenitude of compulsory questions) has an effect, too. However, the interviewees said that they are disclosing their personal data to companies even when compelled, but still with certain terms only.

3.3 Controlling third party access to stored own data is challenging

With regard to the control over personal information the interviewees were worried over the collection of data and what happened to the data after it. The majority of these instances were related to a third party's access to own data when it already was in the possession of the company. The worries included the forwarding of data to external parties without permission, the uncontrolled spreading of personal data online, and to whom one's personal information eventually ends up on the Internet. Some of the observations made were connected to data security issues. Firstly, the interviewees were uncertain about where their data eventually ends up after its disclosure, and whether some third party can have access to this data: *"I do not [perceive that I am in control over the collection and utilization of my personal information on the Internet]. Every now and then I fill in for example various surveys, but I always have to think where my information eventually goes."*

The interviewees were especially worried that their information might end up 'in the wrong hands', for example to conmen. They hoped that the companies informed them better of who has access to their data; they wished more openness and honesty. On the other hand, the interviewees did not necessarily trust the information provided by companies even though the mere existence of data protection statements already aroused the confidence in a few interviewees (see discussion also in Kobsa 2007). The data protection statement is a report given by the registrar about how it acts with the personal data it has acquired in its possession, what are the data protection rights of the person being registered, and how the rights are implemented in practice (Data Protection Ombudsman 2008).

Several interviewees also experienced that personal data spreads easily on the Internet. When own information is disclosed online, it is perceived to spread everywhere without any means of controlling it: *"Frighteningly poorly [I perceive that I am in control over the collection and utilization of my information on the Internet]. One can only be amazed by the ways with which information travels online, and suddenly, for example, your e-mail is flooding with spam."*. Whereas the uncontrolled spreading of information was connected especially to the Internet, the disclosure of personal data or selling that systematically to third parties, usually for advertising purposes, was seen as a problem also outside the Internet realm: *"Yes, most of the time [I perceive that I am in control over the collection and utilization of my personal information on the Internet], I always consider carefully where I disclose my information. The problem is naturally the fact that companies can pass on or sell the information, if, e.g., the forwarding of information for marketing purposes has not been forbidden."*

The deliberate forwarding of personal data was strongly disapproved, especially in the financial sector. In general, the interviewees trusted the banking sector actors with regard to the use of personal data. This is in line with the latest Eurobarometer (2008), according to which 90% of the Finns trust banks and financial institutions in this respect, which is 24% more than the EU-27 average. However, the recent value network developments (e.g. increased co-operation between banks, insurance companies and real estate agencies) caused some hesitation. Finally, what comes to third parties' possibilities to get a hold on personal data, several interviewees expressed their concern about data security: *"In e-commerce it is handy to use your credit card. However, the problem is the risk that the credit card number can be stolen at the data transmit stage. The site must be reliable."* The interviewees were willing to disclose sensitive personal data only in secured connections. In spite of the cautious attitudes many interviewees said that they had given their credit card number on the Internet also in unsecured connections, e.g. when booking a hotel reservation. However, the events had troubled them afterwards. Regarding information security the media appears to have an effect on the consumers; a few interviewees mentioned cases that had been reported recently by the media, for example fake websites with which information is phished for criminal purposes.

3.4 Control over the usage of personal information is difficult

The interviewees discussed in several occasions the usage of their personal data. When making a decision whether to disclose information or not, they felt uncertainty about the purposes of their personal data usage, and considered it difficult to control the usage. The interviewees did not perceive being sufficiently aware of how and to which purposes personal information is utilized: *"I do not [perceive that I am in control over the collection and utilization of my personal information on the Internet]. I disclose information very randomly, depending on which sites I happen to end up. I can of course decide where and what kind of data to provide, but later on I am not able to remember or identify what I have given. Especially the usage of information can remain totally murky."* In these uncertain situations, a few interviewees were unwilling to disclose their personal data to companies. They wanted to know clearly how their information would be used. On the other hand, a few admitted that they were too unconcerned regarding the usage of their personal data. However, several interviewees thought that personal data is utilized without informing the consumers properly, and even though companies would give information about how they use consumers' personal data, most consumers would not believe that the companies would do as they say.

Secondly, the interviewees felt that it is difficult to control the usage of personal data; when information is disclosed, the control over it is easily lost. In any case alertness is required from the consumer with the control over personal information. Thus, in practice, the possibility to control personal information is connected only to the disclosure of data: *"It is quite impossible to control fully [the collection and utilization of my personal information on the Internet] except for the information you provide. On the other hand the information is obscured into the data mass so it will not necessarily hurt you personally."* Once again, the control perception of the consumers' personal information and their actual rights do not seem to meet each other. Thus, the consumers should be more informed of their own data protection rights.

3.5 Methods of control regarding personal data

The control methods of personal data utilized by consumers can be divided into *active* (invoking options) and *passive* (avoiding practices) means (see e.g. Givens 1997). The active means require deliberate actions from consumers, e.g. signing up to a prohibition register of direct mail advertising. Conversely, the passive means denote that something is not done, that is, restricting the disclosure of personal data in different ways, for example, by avoiding shopping on the Internet altogether.

The methods of control mentioned by the interviewees were limited mainly to the passive means, which, according to previous studies (e.g. Dommeyer & Gross 2003) are also best known by the customers. A critical attitude towards information disclosure was mentioned as the main passive means. In addition, awareness of companies' actions was emphasized. Based on the consumers' ability to distinguish reliable marketers from suspicious ones, consumers can decide to whom personal information is disclosed and what services are used. Many interviewees actually restricted the disclosure of their information in some way. A part of the interviewees avoided the disclosure of certain information (e.g. own name), whereas a few provided as few information as possible: *"The less information you disclose, the better you are able to control that. But the information that I already have disclosed, I am not able to control that, but I trust that the firms use it confidentially."* Some of the interviewees conditionally disclosed their information in some ways, for example by forbidding the forwarding of their personal data to other parties. The majority of the interviewees disclosed information only to companies that they considered reliable.

Regarding the active means, only lying and making up false details were mentioned: *"With surveys to some extent [I perceive that I am in control over the collection and utilization of my personal data]. Sometimes a service which I want or must use is asking to fill in compulsory information that I would not like to give. Within certain limits you may give something else than your truthful information."* This was expected to some extent as most control methods that require actions are in fact connected to the control over own environment rather than that of own information. For example, the marketing prohibition registers protect the consumer from direct mail advertising, not from the processing of personal data. On the other hand, not a single interviewee mentioned using a commercial e-mail account (Hotmail etc.) for the control over own information even though their usage is quite common.

4 DISCUSSION AND CONCLUSIONS

This study contributes to the area of privacy protection by offering a comprehensive view on how consumers perceive controlling their personal information disclosure on the Internet regarding marketing and CRM contexts. This topic has not been previously studied separately, but rather in connection with related research questions; thus our study produces valuable knowledge to the discussion of consumers' control perceptions in the online context. Our categorization of the control perceptions experienced by online consumers to four separate themes - or problem situations and control methods - supplements especially the work of Goodwin (1991) regarding the control over personal information disclosure.

The findings of our study show that the consumers perceive the control over their information relating to data collection as a part of a wider whole; when considering whether to disclose information, most consumers think about its sensible and safe storage and purpose of use. On the other hand, it is clearly difficult to control, or even grasp, the utilization of personal information in its entirety. Consumers look at the utilization of personal information from different viewpoints: one emphasizes data and channel security, and the other ponders on the reliability of the company that utilizes the personal information. Even though the interviewees said that they were not in control over their personal information, they, however, demonstrated the perception of control by utilizing control methods suitable for themselves. The lack of control, however, did not necessarily disturb all the interviewees. In future research, control should thus be examined more thoroughly paying attention to the different approaches employed by consumers.

One of the central themes of the interviewees' control speech was trust, which can also be considered on the basis of our data as one method of control, or as a factor that increases the perception of control. Alternatively, trust can be regarded as a compensating factor for the need of control, as preliminarily presented by Olivero and Lunt (2004). According to our qualitative data, both assumptions are supported. On one hand, several interviewees mentioned trust as a prerequisite for disclosing personal information, especially sensitive one, thus referring to a method of control. On the other hand, the interviewees who did not generally trust the Internet, however, disclosed their information using other methods of control, e.g. restricting the disclosure of information with certain conditions. The significance of trust in the control over the consumers' personal information is definitely an important topic for further research.

As for the limitations of this research, we should note that there might be differences between the stated and actual behaviour regarding online information disclosure (see discussion in Kobsa 2007 and Jensen et al. 2005). However, we believe that a survey would be more prone to this distortion than anonymous focus group discussions, as many of our interviewees admitted that they had disclosed information in situations where they in principle would not state to do that. Furthermore, the focus group interviews were carried out only in Finland, and with relatively homogenous sample of participants (online banking customers of age 21-49) which might lower the generalizability of our results. In Finland, online banking is the third most popular application on the Internet, thus almost three out of four Internet users are online banking customers (Statistics Finland 2008). According to the latest Eurobarometer (2008) survey, Finns (as well as other Nordic citizens in general) have higher confidence than the 27 EU countries on average to all market actors and public authorities regarding the usage of their personal information in an appropriate way. Only the market and opinion research companies are trusted equally little in Finland as in the other EU countries on average (33%). Thus, future research might examine the perception of control over online information disclosure in some other parts of the Europe or in the USA, and compare the results to the present study. Moreover, additional research is warranted that studies control in relation to personal information that is provided in consumer-to-consumer relationships (e.g. in social networks or via google mail), as companies exploit increasingly also this information in their marketing efforts.

References

Andrare, E. B., Kaltcheva, V. & Weitz, B. (2002). Self-Disclosure on the web: The impact of privacy policy, reward, and company reputation, Advances in Consumer Research, 29, 350-353.

Boddy, C. (2005) A rose by any other name may smell as sweet but “group discussion” is not another name for a “focus group” nor should it b. Qualitative Market Research, 8 (3), 248-255.

Bragge, J., Kallio, H. and Sunikka, A. (2008). Personalized Marketing Messages in an Online Banking Context: Does Anybody Notice?, Proceedings of the European Conference on Information Systems, (ECIS), Galway, Ireland, June 9-11, 1-12.

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

Clapper, D. L. & Massey, A. P. (1996). Electronic focus groups: A framework for exploration. Information & Management, 30 (1), 43-50.

Cranor, L. F., Reagle, J. & Ackerman, M. S. (1999). Beyond concern: Understanding net users' attitudes about online privacy. AT&T Labs - Research Technical Report, TR 99.4.3.

Culnan, M. J. (2000). Protecting privacy online: Is self-regulation working? Journal of Public Policy & Marketing, 19 (1), 20-26.

Culnan, M. J. & Milberg, S. J. (1998). The second exchange: Managing customer information in marketing relationships. Working paper, McDonough School of Business, Georgetown University.

Dommeyer, C. J. & Gross, B. L. (2003). What consumers know and what they do: An investigation of consumer knowledge, awareness, and use of privacy protection strategies. Journal of Interactive Marketing, 17 (2), 34-51.

Eurobarometer (2008). Data protection in the European Union – Citizens' Perceptions. European Commission, Flash Eurobarometer Series 226.

Evans, M., Patterson, M. & O'Malley, L. (2001). The direct marketing – direct consumer gap: Qualitative insights. Qualitative Market Research, 4 (1), 17-24.

Foxman, E. & Kilcoyne, P. (1993). Information technology, marketing practice, and consumer privacy: Ethical issues. Journal of Public Policy & Marketing, 12 (1), 106-119.

Givens, B. (1997). The privacy rights handbook: How to take control over your personal information. New York: Avon.

Goodwin, C. (1991). Privacy: Recognition of a consumer right. Journal of Public Policy & Marketing, 10 (1), 149-166.

Heikkinen, K., Eerola, J., Jäppinen, P. & Porras, J. (2004). Personalized view of personal information. WSEAS Transactions on Communications, 1 (4), 50-55.

Jensen, C., Potts, C. & Jensen, C. (2005). Privacy practices of internet users: Self-reports versus observed behavior. International Journal of Human-Computer Studies, 63: 203-227.

Katz, J. E. & Tassone, A. R. (1990). Public opinion trends: Privacy and information technology. Public Opinion Quarterly, 54 (April), 125-143.

Klein, E. E., Tellefsen, T. & Herskovitz, P. J. (2005). The use of group support systems in focus groups: information technology meets qualitative research. Zarb School of Business Working Papers, Hofstra University. http://www.hofstra.edu/pdf/BIZ_mlc_workingpaper5.pdf (2.11.2008).

Knights, D., Noble, F., Vurdubakis, T. & Willmot, H. (2001). Chasing shadows: Control, virtuality and the production of trust. Organization Studies, 22 (2), 311-336.

Kobsa, A. (2007). Privacy-Enhanced Web Personalization. In Brusilovsky, P., Kobsa, A. and Nejdl, W. (Eds.): The Adaptive Web. Lecture Notes in Computer Science 4321, Springer, 628-670.

Kontio, J., Bragge, J. & Lehtola, L., (2007) The Focus Group Method as an Empirical Tool in Software Engineering. In Shull, F., Singer, J. and Sjøberg, D. I. K., Guide to Advanced Empirical Software Engineering, Springer-Verlag London, 93-116

Milne, G. R. (2000). Privacy and ethical issues in database/interactive marketing and public policy: A research framework and overview of the special issue. Journal of Public Policy & Marketing, 19 (1), 1-6.

Milne, G. R. & Gordon, M. E. (1993). Direct Mail Privacy-Efficiency Trade-offs within an implied social contract framework. Journal of Public Policy & Marketing, 12 (2), 206-215.

Milne, G. R. & Boza, M. E. (1998). Trust and concern in consumers' perceptions of marketing information management practices. Journal of Interactive Marketing, 13 (1), 5-24.

Montoya-Weiss, M.M., Massey, A.P. & Clapper, D.L. (1998). On-line focus groups: Conceptual issues and a research tool. European Journal of Marketing, 32 (7/8), 713-723.

Moon, Y. (2000). Intimate exchanges: Using computers to elicit self-disclosure from consumers. Journal of consumer research, 26 (March), 323-339.

Morgan, D.L. (1996), Focus Groups. Annual Review of Sociology, 22 (August), 129-152.

Morimoto, M. & Chang, S. (2006). Consumers' attitudes toward unsolicited commercial e-mail and postal direct mail marketing methods: Intrusiveness, perceived loss of control, and irritation. Journal of Interactive Advertising, 7 (1), 8-20.

Muttilainen, V. (2007). Finns' views about data protection 2004-2006. In Nurmela, J., Sirkiä, T. & Muttilainen, V. (Ed.). Finns in the information society 2006. Statistics Finland, Helsinki, 43-50.

Nunamaker, J. F., Dennis, A.R., Valacich, J. S., Vogel, D. R. & George, J. F. (1991). Electronic meeting systems to support group work. Communications of the ACM, 34 (3), 40-61.

O'Connor, H. & Madge, C. (2003). Focus groups in cyberspace: Using the Internet for qualitative research. Qualitative Market Research, 6 (2), 133-143.

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.

O'Malley, L., Patterson, M. & Evans, M. (1997). Intimacy or intrusion? The privacy dilemma for relationship marketing in consumer markets. Journal of Marketing Management, 13 (6), 541-559.

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

Personal Data Act (1999). http://www.finlex.fi/en/laki/kaannokset/1999/en19990523.pdf (3.10.2008).

Posner, R. (1981) The Economics of Justice. Cambridge, MA: Harvard University Press.

Prahalad, C. K. & Ramaswamy V. (2004), Co-creation experiences: The next practice in value creation. Journal of Interactive Marketing, 18 (3), 5-14.

Privacy & American Business (2004). New national survey on consumer privacy attitudes to be released at Privacy & American Business Landmark Conference. Press Release.

Romano, N.C., and J. Fjermestad (2003). Electronic Commerce Customer Relationship Management: A Research Agenda. Information Technology and Management 4 (2-3), 233-258.

Sayre, S. & Horne, D. (2000). Trading secrets for savings: How concerned are consumers about club cards and privacy threat? Advances in Consumer Research, 27: 151-155.

Sheehan, K. B. & Hoy, M. G. (2000). Dimensions of privacy concerns among online consumers. Journal of Public Policy and Marketing, 19 (1), 62-73.

Statistics Finland (2008) Number of Internet users up from the year before, 25 August 2008. Available at: http://www.stat.fi/til/sutivi/2008/sutivi_2008_2008-08-25_tie_001_en.html (23 October 2008).

Steiner, I. D. (1972), Group Process and Productivity, Academic Press, New York.

Suh, B. & Han, I. (2003). The impact of customer trust and perception of security control on the acceptance of electronic commerce. International Journal of Electronic Commerce, 7 (3), 135-162.

Sunikka, A., Lähteenmäki, M. and Bragge, J. (2007), Perceived Benefits and Costs of Personalized Marketing Messages. Case Online Bank. Proceedings of the 36th European Marketing Academy Conference EMAC, May 22-25, 2007, Reykjavik, Iceland.

Sweet, C. (2001). Designing and conducting virtual focus groups. Qualitative Market Research, 4 (3), 130-135.

Data Protection Ombudsman (2008) Vocabulary, http://www.tietosuoja.fi/27247.htm (29.10.2008).

Velasquez, M. G. (2006) Business ethics: Concepts and cases. (6. ed.). NJ, Upper Saddle River: Pearson Education Inc.

Westin, A. (1967). The origin of modern claims to privacy. In Westin, A. (ed.) Privacy and freedom. Association of the Bar of the City of New York. London: Bodley Head.

White, T. B., Zahay D. L., Thorbjørnsen, H. & Shavitt, S. (2008). Getting too personal: Reactance to highly personalized email solicitations. Marketing Letters, 19(1), 39-50.