E-privacy in 2nd Generation E-Commerce: Privacy Preferences versus actual Behavior

Sarah Spiekermann
Humboldt University Berlin
Institute of Information Systems
Spandauer Str. 1
10178 Berlin, Germany
sspiek@wiwi.hu-berlin.de

Jens Grossklags
Humboldt University Berlin
Institute of Information Systems
Spandauer Str. 1
10178 Berlin, Germany
jensg@wiwi.hu-berlin.de

Bettina Berendt
Humboldt University Berlin
Institute of Pedagogy and Informatics
Geschwister-Scholl-Str. 7
10099 Berlin, Germany
berendt@educat.hu-berlin.de

ABSTRACT

As electronic commerce environments become more and more interactive, privacy is a matter of increasing concern. Many surveys have investigated households' privacy attitudes and concerns, revealing a general desire among Internet users to protect their privacy. To complement these questionnaire-based studies, we conducted an experiment in which we compared self-reported privacy preferences of 171 participants with their actual disclosing behavior during an online shopping episode. Our results suggest that current approaches to protect online users' privacy, such as EU data protection regulation or P3P, may face difficulties to do so effectively. This is due to their underlying assumption that people are not only privacy conscious, but will also act accordingly. In our study, most individuals stated that privacy was important to them, with concern centering on the disclosure of different aspects of personal information. However, regardless of their specific privacy concerns, most participants did not live up to their self-reported privacy preferences. As participants were drawn into the sales dialogue with an anthropomorphic 3-D shopping bot, they answered a majority of questions, even if these were highly personal. Moreover, different privacy statements had no effect on the amount of information disclosed; in fact, the mentioning of EU regulation seemed to cause a feeling of 'false security'. The results suggest that people appreciate highly communicative EC environments and forget privacy concerns once they are 'inside the Web'.

Categories and Subject Descriptors

K.4.1 [**Computers and Society**]: Public Policy Issues – *Privacy*

General Terms

Management, Experimentation, Human Factors, Legal Aspects.

Keywords

Privacy, Automated Shopping and Trading, Legal Issues, Marketing and Advertising Technology, Social Implications, User Interface and Interaction Design

EC'01, October 14-17, 2001, Tampa, Florida, USA.

1. INTRODUCTION

Privacy is a hotly debated issue. It is at the center of the question who will have access to one of the online economy's major assets: customer data. Long-existing dreams of one-to-one marketing are close to coming true for marketers on the Internet. Through personalization, companies hope to improve customer retention, to build up stronger competitive boundaries and to increase revenue. Researchers in marketing, computer science, psychology and many other disciplines have therefore started to work in this direction, investigating opportunities inherent in agent technology [3,14,22,27,29], data mining [6,24], and interface design [9,17,23,25]. A core assumption is generally the availability of reliable customer data. Without a sufficient base of such data all these current marketing visions cannot be realized. The problem is that at this point a conflict arises: While companies are thirsty for ever more information they undermine the fundamental right to information privacy.

Three fundamental approaches have evolved over the past decade addressing the privacy issue: ensuring privacy through law, through self-regulation, or through technical standards. European countries rely very much on the force of regulation. The problem with regulation is that laws take an average of 10 years to go into effect, while the life cycle of information and communication goods is only 3-7 months [7, p.286]. So regulation risks to always be behind the technology deployed. Also, law enforcement is a huge challenge, not only because European countries have difficulties creating and financing appropriate control institutions [5,21], but also because imposing their national data practices on super powers such as the US proves rather difficult. The biggest problem of EU data protection law is that it propagates data collection parsimony [12] while the Internet is inherently a medium of 'data richness'. It also restricts the free trade of user data [12], although this asset has become one of the most valuable goods of the new economy [13], around which many business models are built [10]. As a result, it is questionable to what extent EU regulation will have the power to enforce its good visions practically.

The US has pursued a more liberal approach of self-regulation. US companies are focusing more on the use of privacy statements and privacy seals in Web sites. The main underlying assumption is that people are privacy conscious and that they trust published privacy statements and -seals. Many surveys have supported this view [1, 28, 19]. It is therefore argued that market forces will lead to the 'survival' of only those online companies that abide by acceptable privacy standards. The Platform for Privacy

Preferences Project (P3P) which is probably the best-supported privacy technology, is a product of this school of thought.[1] P3P will block access to Web sites or automatically notify the online user if a Web site's privacy statement is not in line with privacy preferences. The consumer is then left to decide whether he or she still wants to use the service. As most surveys gave evidence of online users privacy concerns, it is hoped that consumers will stop accessing sites that do not provide appropriate policies.

The problem is that the surveys conducted to prove users' privacy consciousness only asked for attitudes, but never measured actual behavior. In particular, no observations exist on how consumers will react to promising benefits of highly interactive Web sites that offer individualized content as well as highly communicative and entertaining value. This is particularly interesting in the current context, because it allows to anticipate the success of current initiatives to protect privacy and to generate ideas for valuable adjustments. The empirical study presented hereafter fills this research gap by asking people for their privacy preferences and contrasting these claims with subsequent behavior during an online shopping trip.

We begin with a description of the experimental set-up. In section 3, we present selected results obtained from a first questionnaire on privacy attitudes and preferences and compare these attitudes with self-disclosure practiced in communication with an anthropomorphic 3-D shopping bot that assisted participants in an online shopping trip for winter jackets and compact cameras. In the same section, we address the question whether different privacy attitudes lead to different navigational strategies. We also investigate the influence of different privacy statements on behavior. Section 4 then comprises a critical discussion of current approaches to protect privacy and some suggestions on how to render them more effective. Section 5 concludes with a summary of major findings and limitations of the study.

2. METHOD

In December 2000 an experiment was carried out at Humboldt University Berlin with the goal to investigate drivers and impediments of online interaction.[2] Privacy concerns were regarded as one major impediment of truthful and deep online interaction. In investigating privacy we focused on two issues: First, we wanted to contrast self-reported privacy preferences with actual self-disclosing behavior. Second, we wanted to find out whether different privacy statements would impact interaction and disclosure.

The experiments were designed to observe participants during an online shopping trip for a compact camera or a winter jacket. Participants had to spend their own money if they chose to buy in the shop. Before and after the shopping trip, they filled out a questionnaire. In order to encourage participants to investigate products 'neutrally', no brand information was displayed.

2.1 Participants

206 participants volunteered to participate in the experiments and to shop for one of two products, a compact camera or a winter jacket. Their main incentive was a 60% discount on the prices of all products offered in the experimental store.[3] 95% of the participants were students from different university faculties, while the remaining 5% participants held different jobs. 152 chose to shop for a camera, and 54 for a jacket.

2.2 Materials and Apparatus

The central material for the experiment were the online store and a questionnaire before and after the shopping session.

The online store was programmed for the experiment, using Meta-HTML and Java. It offered more than 50 compact camera models and 100 winter jackets for sale. All participants had high-speed access from a computer laboratory at Humboldt University. Participants were told that the store was hosted by an industrial partner who did not wish to be named and that all data would be directly transferred to this remote host.

The online shopping environment employed a 2nd generation e-commerce type of communication, in which an anthropomorphic 3-D shopping bot involved users in a sales dialogue and gave product recommendations. Unlike current shopping agents on the web, the bot not only focused on product attributes, but also asked 'soft questions' that can typically be found in offline sales conversations. 56 bot questions had been developed for this purpose in cooperation with human sales agents from a Berlin retail store. The goal of bot communication design was not to minimize a user's time cost, but, on the contrary, to include more questions and in particular more personal questions than one would expect customers to answer. In addition to product attribute questions like "How strong do you want the zoom of the camera to be?" we therefore integrated three further question categories: 1) Questions concerning the intended use of the product (e.g., "At what occasions do you usually take photos?"). 2) Questions that addressed the buyer personally, but would also influence product recommendation (e.g., "How important are trend models to you?"). And 3) personal questions independent of the product but still related to the sales context (e.g., "What do you do with your photographs?"). This latter category also included 'non-legitimate' extremes such as questions on how "photogenic" or "conceited" people considered themselves to be. Table 1 shows some selected bot questions for the 2 products.

[1] P3P is an initiative of the World Wide Web Consortium (W3C) in conjunction with many industry partners including Microsoft. For more information see: http://www.w3.org/P3P/

[2] For more information, cf. http://iwa.wiwi.hu-berlin.de

[3] Since project finances did not allow us to offer the 60% discount to all buyers, the incentive structure was such that a lottery after the shopping session decided on one out of 10 participants who would have the right to buy for 60% off. The remaining participants received a small financial compensation. If someone had not bought, but won the lottery, he or she would not receive anything.

Table 1: Selected bot questions

4 categories of bot questions	Camera	Jacket
product attribute questions	How strong do you want the zoom of the camera to be?	What size do you need for the jacket?
usage oriented questions	At what occasions do you usually take photos?	At what occasions do you want to wear the jacket?
personal questions supporting product selection	How important are relatively cheap photo development cost to you?	How important are trend models to you ?
personal questions independent of product selection	What is your motivation when taking photographs?	How often do you buy a new jacket?

All 56 questions had been tested in a pre-study with 39 participants who had rated their relative importance, legitimacy and difficulty [2]. This yielded, for each bot question, a mean legitimacy value and a mean importance value. On average, 32% of camera questions and 39% of jacket questions were judged as relatively non-legitimate, and 37% of camera questions as well as 50% of jacket questions as relatively unimportant.[4] However, Mann-Whitney test for the two product question catalogues showed non-significant differences between the distributions of mean question importance ($p=0.543$) and mean question legitimacy ($p=0.386$) in the two shops. This allowed us to pool data from the two product shopping sessions for privacy analysis.

All online interactions were logged, yielding, for each participant, the sequence and timestamps of all pages requested and answers given. In addition, all participants were asked to fill out a paper-and-pencil questionnaire before and after the experiment. Privacy-related questions accounted for 27% of the pre-shopping questions addressing the willingness to reveal certain types of private data in an Internet communication, the general trust in privacy statements, the value of privacy and answers on various privacy scenarios.

2.3 Procedure

On arrival at the laboratory, participants were told that the experiment's goal was to test interaction with a new product search engine developed for an industrial partner at the Institute of Information Systems at Humboldt University. During the experimental briefing, in which instructions were read aloud to all participants, one of our goals was to minimize sympathy with us as experimenters. This was done to avoid an 'experimenter effect' leading subjects to eventually trust our data handling policies more than they would in a normal navigation.Participants were then asked to fill out the paper-and-pencil questionnaire.

Participants were then presented with the online store's privacy statement in printed form. In the 'soft' privacy statement (type 1), participants were told that an industrial sponsor, a reputable European company which did not wish to be named, would receive all navigational data. Also, their rights according to the EU Directive 95/46/EC were stated in this privacy statement, including the right to know who makes use of the data, to view them and if necessary change or withdraw them. In the 'harsh' privacy statement (type 2), participants were told that their data would be handed on to an anonymous entity, and that we did not know what further use would be made of their data. 88 participants received the type 1 privacy statement, and 118 participants received the type 2 privacy statement. They had to sign that they had read and accepted this statement prior to shopping. All participants were told that it was not the purpose of the experiment "to collect dummy data", and that we expected them to give truthful answers because the search engine we had developed would not work adequately otherwise. We added that we would "prefer the refusal to answer to a lie".[5]

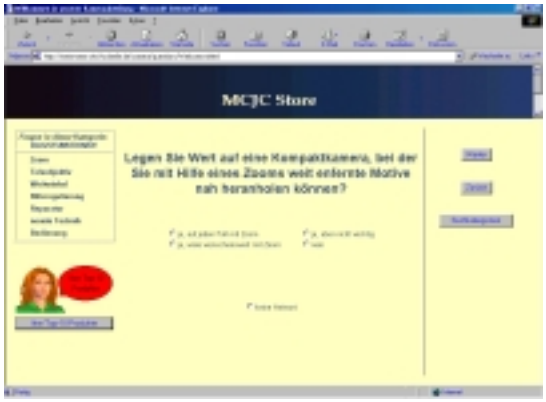
The navigation opportunities participants encountered in the store were similar to those in Web sites like ActiveBuyersGuide.com or PersonalLogic.com. The online store's starting page had been loaded into the Web browser by the experimenter. It displayed either a camera or a jacket storefront. After this starting page, users had the possibility to view all products one by one from a list, but would quickly find out that this way of searching was not very efficient. They were thus motivated to enter the search engine. Here, shopping bot Luci introduced herself and her purpose to the user. All users had to pass this page and were given the possibility to leave their home address. No reason was given on the page why they should enter it, but two 'proceed-buttons' were displayed: one labelled "save address, proceed" and the second right below entitled "no address specifications, proceed". The user was thus left to decide whether to reveal the address or not without any sanctions.

Once users passed Luci's introduction, navigation occurred at two levels: a communication level and an information level. On the communication level, participants could engage in a question-answer dialogue with Luci (based on multiple-choice). Luci offered users to answer the 56 questions discussed above. On the basis of any number of answers given, she could be asked to calculate a user's product ranking with graphical emphasis given to a 'Top-10' consideration set. On the information level, participants had the possibility to view product facts, marketing text an enlargeable photograph. Both navigational levels where accessible from all pages. Thus, recommendations could be obtained and products inspected at any time. The shopping process could be exited at any time and a purchasing decision could be made after the request for a product information page. Figure 1 provides some screenshots of the store environment.

[4] Legitimacy and importance were rated on a 0-10 point scale with 0 = totally non-legitimate/totally unimportant and 10 = very legitimate/very important; ratings referred to as 'relatively non-legitimate' or 'relatively unimportant' here were all judgements < 5

[5] We gave participants the option to refuse to answer any bot question by including a "no answer" button in each multiple-choice menu of answers.

Communication level: Bot questions, answers and Top-10 feedback



Information level: product photograph and description

Figure 1: Screenshots of 2 navigational levels

3. RESULTS

3.1 Data

As 6 of the 206 individual observations had missing data, analysis was based on 200 observations. Another group of 29 subjects was identified who did not see and consequently did not consciously answer or reject several bot questions. As we could not explain this behaviour and do not attribute it to any privacy concerns, we excluded these subjects from our analysis. Thus, further discussion in this paper is based on 171 observations.

Two data sources were used for analysis: questionnaire answers to discern privacy preferences and log files to analyze behavior.

3.2 Measures of Interaction Behavior

Self-disclosure is usually measured along two dimensions: its depth and breadth [18, p.328]. Breadth refers to the quantity of information exchanged and is measured here by the number or proportion of bot questions answered. Depth usually refers to the quality of information disclosed. We operationalized information quality with the help of an index called "personal consumer information cost" (PCIC). The index was developed on the basis of the pre-study mentioned above; more details are given there [2].

In the pre-study, 39 participants had been asked to rate a presented question's legitimacy and importance in the sales context, and the difficulty of answering it, as well as the "overall perceived information cost" of this question. This construct had been explained prior to the rating session as follows: "Information cost denotes the 'intuitive readiness' to truthfully answer the question of the search engine, i.e. the spontaneous feeling whether you would be willing to reveal the demanded information about yourself. 'No' information cost means that you would have no problem at all to answer the question truthfully. 'Very high' information cost means that you would, under no circumstances, give this type of information about yourself to a search engine." A regression analysis of the judgements of all 56 questions showed that PCIC decreased linearly with legitimacy and importance, and increased linearly with difficulty [2].

For the purposes of the current study, we computed $PCIC_j$, considering all the questions that participant j had answered (see Figure 2 for details).

$$PCIC_j = \sum_{i=1}^{k_\nu} \left(a - \alpha * Leg_i^\nu + \beta * I_i^\nu + \delta * Diff_i^\nu\right) + \sum_{i=1}^{k_\sigma} \left(b - \phi * Leg_i^\sigma + \gamma * I_i^\sigma + \rho * Diff_i^\sigma\right)$$

ν = questions of *type* ν focus either on the person or on envisaged product usage

σ = questions of *type* σ are questions concerned directly or indirectly with product attributes

i = a question answered by an online user j

k = total number of questions answered by user j

j = user

Leg_i^t = Mean perceived *legitimacy* of a question *i* of type *t*, $t \in \{\nu, \sigma\}$

I_i^t = Mean perceived *importance* of a question *i* of type *t*, $t \in \{\nu, \sigma\}$

$Diff_i^t$ = Mean perceived *difficulty* of a question *i* of type *t*, $t \in \{\nu, \sigma\}$

Figure 2: Computing a user's PCIC

The values of Leg, I, Diff as well as the 8 regression parameters ($a, b, \alpha, \beta, \delta, \phi, \gamma, \rho$) were taken from the pre-study.

For this study, it is important to know that PCIC aims to reflect an individual's perceived 'cost of disclosure' in a communication context. More precisely, we define it as the loss in utility a consumer perceives when disclosing a number of truthful information units about himself, assuming that his identity will afterwards be known to the organization hosting a site and that his data are collected for further usage. For example, when people decide to lie on the Internet, the cost of providing truthful information is obviously too high.

A user with a high PCIC answers many bot questions even though he perceives them as being rather non-legitimate, unimportant and difficult to answer. A user with low PCIC values answers few questions, most of which he perceives as legitimate and important and easy to answer.

3.3 Privacy attitudes and self-disclosure

As discussed above, privacy statements published on Web sites are an important baseline for today's advances in consumer protection. For the deployment of P3P, for example, it is assumed that users regard privacy policies as relatively trustworthy, consider their own privacy preferences and then act consciously in accordance with them.

To investigate privacy preferences, we built on earlier work presented by Ackermann et al. [1] and especially a questionnaire developed by this group of scholars to test privacy preferences. Like Ackerman et al., we employed standard multivariate clustering techniques (more specifically, k-means [6]) to investigate the data collected: Base variables used for clustering were extracted from the privacy-related questions asked prior to the shopping session and had to be z-transformed for the purpose of analysis. Hierarchical clustering outset the analysis of data. It revealed the existence of 4 distinct groups which were then pre-set as the target number of clusters for a k-means clustering process.

In contrast to Ackermann et al. [1], we not only identified privacy fundamentalists (cluster 4: 30%) as well as marginally concerned users (cluster 1: 24%), but also found two distinct groups whose privacy concerns focused either on the revelation of identity aspects such as name, address or e-mail (cluster 3: 20%) or on the profiling of interests, hobbies, health and other personal information (cluster 2: 25%). We were thus able to separate the "pragmatic majority" identified by Ackerman et al. [1] into two more meaningful groups which we called "identity concerned" and "profiling averse". Figure 3 gives an overview over the four clusters identified. Compared to the earlier study, privacy concerns appear to be stronger in our sample with a bigger proportion of "privacy fundamentalists" and a reduced group of "marginally concerned".

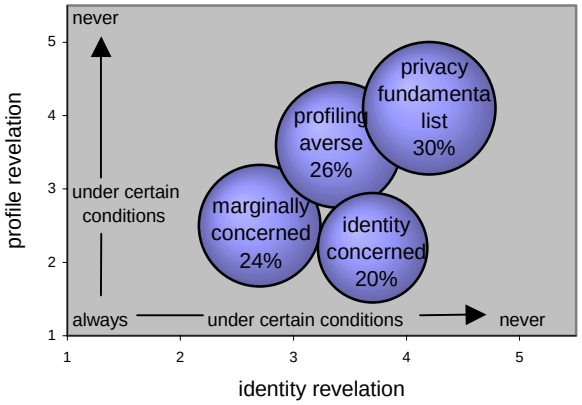


Figure 3: 4 clusters of privacy attitudes identified

We then investigated whether interaction behavior was consistent with the attitudes stated. Two aspects of interaction behavior were considered: (a) whether participants voluntarily communicated their address to Luci before entering the question-answer cycle, and (b) how many and what types of questions participants answered when communicating with Luci. The first variable is a measure of the willingness to satisfy an information request *separated* from the sales dialogue and linked to identification. We expected that 'identity concerned' users (cluster 3) would react particularly averse to this type of information provision. The second variable is a measure of the willingness to provide information *embedded* in a sales dialogue. As many personal and profile-sensitive questions are asked in this communication context, one would expect that here 'profiling averse' users (cluster 2) would be particularly reserved.

3.3.1 Address Provision

As expected from the nature of the cluster, marginally concerned users (cluster 1) had the lowest refusal rate in providing their home address for both privacy statements (30% for PS type 1 and 41% for PS type 2). Surprisingly, 24-28% of privacy fundamentalists voluntarily provided their address before interacting with the search engine. Identity concerned participants (cluster 3) also showed unexpected behavior. While under the condition of the first privacy statement 93% refused to provide their home address, only 65% did so under the even "harsher" conditions of PS type 2. However, cluster 3 was the smallest group, so more research is needed to investigate this finding. All observations are summarized in table 2.

Notably, across privacy statements there was an average of 35-40% of participants who gave their home address without any reason to do so. This raises the question how privacy conscious online users really are. In particular, the mentioning of the 'security providing' EU law, led to an increase in voluntary address provision, as can be seen for most clusters in table 2. The average difference of 5% more address provision with EU law citation (11% without the inconsistent group of cluster 3) was interesting, though not significant ($\chi^2(1)=0.33$, $p > 0.5$).

Table 2: Contrasting privacy attitudes with voluntary address provision

Cluster	PS type 1 (voluntary address provision)	PS type 1 (*no* voluntary address provision)	PS type 2 (voluntary address provision)	PS type 2 (*no* voluntary address provision)	Sum of partici-pants
CL1:marginally concerned	14	6	13	9	42
% of cluster	70%	30%	59%	41%	
CL2: profiling averse	9	10	7	19	45
% of cluster	47%	53%	27%	73%	
CL3:identity concerned	1	13	7	13	34
% of cluster	7%	93%	35%	65%	
CL4: fundamentalists	7	18	6	19	50
% of cluster	28%	72%	24%	76%	
sum tot	31	47	33	60	171
% of sum	40%	60%	35%	65%	

3.3.2 Revelations during the sales dialogue

To represent the depth of interaction with the sales bot, we used the PCIC index described above. The 171 PCIC index values where split into terciles, contrasting individuals with low, medium and high disclosure. Table 3 summarizes the findings. Table 3 shows that participants from all clusters had a strong tendency to self-disclose. 87% of users were in the group with maximum PCIC values. This behaviour could be observed across both product types, with 84% of camera shoppers and 98% of jacket shoppers in the highest PCIC group.

Averaging across clusters, an average of 85.8% of bot questions were answered (85.8% for cameras and 86.1% for jackets). As expected, however, the distribution of PCIC was different across clusters ($\chi^2(6)=16.57$, $p<0.05$).

An investigation of cluster details showed that privacy fundamentalists (cluster 4) in particular did not live up to their expressed attitude. 78% of them display high PCIC values and answered an average of 86% of the bot questions. With this, they only answered 10 percentage points fewer questions than marginally concerned participants (cluster 1). Comparing behaviour for the two product groups, we found that for cameras only 83% of privacy fundamentalists had a high PCIC value, while for jackets 95% of fundamentalists were in this group. A difference of 7% in self-disclosure between the two products can also be observed for cluster 2. The findings hint at the possibility that the product category may have an influence on the extent of information revelation.

Consistent with the expectations, profiling averse participants (cluster 2) gave less information during the shopping dialogue than identity concerned participants (cluster 3). With 'only' 78% of people being in the high PCIC group, cluster 2 and 4 turned out to be the groups with the most reserved behavior.

Table 3: Contrasting privacy attitudes with online communication behavior

Cluster	low PCIC	medium PCIC	high PCIC	Sum
CL1: marginally concerned	0	0	42	42
row %	0%	0%	100%	100%
total %	0%	0%	24%	24%
CL2: profiling averse	3	7	35	45
row %	7%	15%	78%	100%
total %	2%	4%	20%	26%
CL3: identity concerned	0	1	33	34
row %	0%	3%	97%	100%
total %	0%	1%	19%	20%
CL4: fundamentalists	3	8	39	50
row %	6%	16%	78%	100%
total %	2%	5%	23%	30%
Sum	6	16	149	171
total %	4%	9%	87%	100%

Mann-Whitney tests for different PCIC distributions across the two privacy statements generally ($p=0.969$) and for both products separately (camera: $p=0.526$; jackets: $p=0.227$) showed no significant differences in this obvious readiness of users to self-disclose. This is a surprising result as we would have expected the privacy statement to have a greater impact on disclosure.

3.3.3 Privacy attitudes and navigation

We investigated communication behaviour in relation to information behaviour with the help of two indices: The first index, the communication quota, is a set-based measure designed to express how much of the shopping process was dedicated to communicating with the shop bot versus obtaining information by looking at product descriptions (texts and photos). It is thus a measure of the extent to which participants referred to agent advice in contrast to self-initiated product search.

The communication quota Q is defined as

$Q = C / I$ with

C = total number of requests for a question page (including those that were not answered and return hits to correct initial answers given)

I = total number of requests for pages giving product information, photo enlargements and required return hits to the top-ten set

Q ranged from 0.02 to 5.9, with a mean value of 1.22.[6]

The second index, the communication flow, is a sequence-based measure designed to express how long agent Luci succeeded in involving the user in a continuous stretch of communication. It decreases with the frequency of interrupting the question-answer cycle to obtain the agent's recommendations or proceed to product inspection. The communication flow is defined as:

F = (C + I) / number of transitions from a communication page to the consideration set page.

F ranged from 13.33 to 233, with a mean value of 74.69. Q was correlated with F(r^2=-0.23, $p<0.01$). This was due to a correlation between these two measures in cluster 3 (r^2=-0.37, $p<0.05$); in the other clusters, the two measures were independent (each $p>0.23$). There was a comparatively small but significant correlation between F and the total number of questions answered, k in Figure 2 (r^2=0.18, $p<0.05$). No correlation was found between Q and k (r^2=0.04, $p>0.6$). These results may indicate that the more users let themselves be involved in dialog, the more answers they give.

The communication quota Q differed by cluster. However, an ANOVA showed that this was non-significant ($F(3,160)=0.194$, $p=0.9$). F also differed by cluster, a marginally significant trend ($F(3,160)=2.09$, $p=0.11$).

Inspecting the difference in communication flow between clusters, we found that profiling averse users (cluster 2) exhibited a smaller flow than all other groups ($\mu(c2)=67.62$ vs. $\mu(c1)=72.27$, $\mu(c3)=92.52$, and $\mu(c4)=70.8$) A closer analysis of these participants' navigation behavior showed that they seemed to try to control the bot dialog by frequently interrupting it, checking whether additional information provided would lead to a sufficiently satisfactory recommendation. They thus seemed to engage in a cost-benefit type of judgement on whether to continue revelation or to stop. However, in the end, they answered as many questions as users in clusters 3 and 4.

In contrast to cluster 2, users in cluster 3, concerned about disclosing identity information, showed the reverse navigation pattern. They exhibited the largest flow and engaged more than any other group in information-gathering behaviour (*Q*: $\mu(c3)=1.16$ vs. $\mu(c1)=1.21$, $\mu(c2)=1.32$, and $\mu(c4)=1.17$). This behaviour appears consistent with the fact that this group feared profiling less than identity related questions that were not part of the bot dialog. Figure 4 shows typical examples of these two types of navigation.[7] Users in cluster 4, who professed to be most concerned about all aspects of privacy, exhibited a comparatively small flow as well as quota, indicating a cautious communication / information strategy.

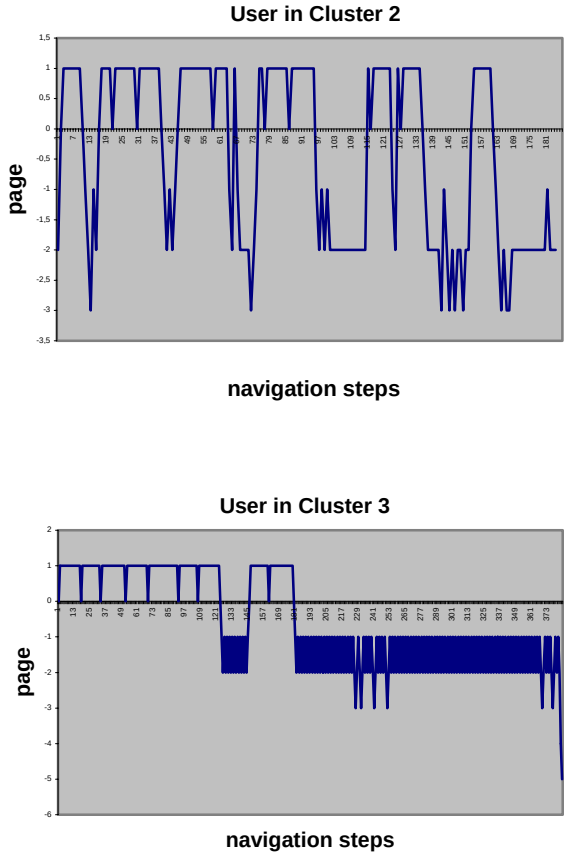


Figure 4: Individual stratograms to visualize clickstreams: (a) a user in cluster 2 with Q = 1.28 and F = 21.13, and (b) a user in cluster 3 with Q = 0.34 and F = 149

Taken together, the lack of a significant difference in communication quota across clusters indicates that regardless of

[6] In navigation analysis, the data of only 164 participants could be used, because of missing data in the recorded clickstreams.

[7] The figure contains individual 'stratograms' [4] that trace a single user's path through the site. The figure shows only those parts of the navigation process spent in communication or information as defined above, omitting the introductory phase as well as the purchase or exit phase. The x axis contains the steps in the navigation history, while the y axis represents the type of page requested. Values along the y axis are ordered to reflect the interaction process: 0 is the question category survey page, 1 is any question page, -1 is the consideration set, -2 is product information, and -3 more product information (photo enlargements). Thus, the figures show communicative behavior, in particular its phases "giving information" (the question-answer cycle) as a straight line in the upper quadrant, and "asking for feedback" (the request for the agent's current recommendations) as oblique lines proceeding from the upper quadrant into the lower quadrant. The figures show information-gathering behavior as continuous stretches in the lower quadrant.

privacy preferences, most users appear to choose a product based on the same general combination of communication and information, and welcome a rich communication with an online shopping agent.

The privacy statement had no influence on the communication quota ($F(1,162)=0.11$, $p>0.7$), and no influence on the communication flow ($F(1,162)=0.84$, $p>0.3$).

3.3.4 Overall judgements of agent interaction

In the debriefing questionnaire, most subjects indicated that they appreciated the type of soft communication employed. Even those individuals who had expressed privacy concerns in the first questionnaire and were not too fond of the recommendation quality wrote that they felt supported by agent Luci in "getting a feel" for the product, that the questions were not "too technical" and "easily comprehensible" and that they "felt personally addressed" in their concerns.

4. SUMMARY AND DISCUSSION OF RESULTS WITH A VIEW TO PRIVACY TECHNOLOGIES AND REGULATION

We conducted an experiment in which we compared self-reported privacy preferences of 171 participants with their actual self-disclosing behavior during an online shopping episode. Our initial hypothesis that users' privacy concerns impede the depth and breadth of truthful online interaction was not confirmed. In contrast, participants displayed a surprising readiness to reveal private and even highly personal information and to let themselves be 'drawn into' communication with the anthropomorphic 3-D bot.

The readiness of participants to reveal most of or even all of the information demanded from them during the sales dialogue with the shopping bot, and the widespread willingness to also provide their address, are alarming findings. The degree of inconsistent behavior found in the data among 'privacy aware' clusters 2-4 appears particularly problematic. The results are even more relevant when one considers the experimental conditions: after all, bot questions were designed to include many non-legitimate and unimportant personal questions. Participants also had to sign that they agreed to the selling of their data to an anonymous entity. During debriefing, efforts had been made to minimize sympathy with us as experimenters. The conditions under which participants 'revealed themselves' were therefore probably even more unfavorable in terms of privacy than a regular Internet interaction would be. This indicates that even though Internet users have some view on privacy, they do not act accordingly. A majority of persons who participated in the shopping experiment disclosed so much information about themselves that a relatively revealing profile could be constructed on the basis of only one shopping session. This result is not only alarming in itself, but even more so given that, for many participants, this behavior stands in sharp contrast to their self-reported privacy attitude (especially for the profiling averse and fundamentalist participants in clusters 2 and 4). It raises the question of how privacy can be protected effectively while at the same time avoiding tutelage.

4.1 Privacy statements and P3P

As was outlined above, privacy statements play an important role in addressing privacy through P3P. It was shown, however, that while people do tend to provide less identification information, they do not alter their communication behavior significantly in response to privacy statements, neither in disclosing their profile nor in navigation. Even privacy conscious users (clusters 2 and 4) seem to be 'drawn to reveal themselves' to the sales bot, and only 3 out of 171 avoided the dialogue offered (which is similar to blocking or avoiding promising communication in a P3P scenario).

Still, P3P has the potential to considerably enhance privacy standards: first, it may enhance user trust in privacy statements, because companies, by taking the burden of encoding their website practices, signal their willingness to respect their users' privacy. Privacy can thus become a recognized means of differentiation. Second, P3P is able to correspond to the different privacy preferences of users. For example, with P3P identity concerned users have the possibility to effectively exclude sites that demand information in the categories <physical>, <online> or <uniqueid>.[8] Third, P3P is a relatively open platform standard. It could easily be extended to prohibit or at least warn of communication processes such as the one we used in the current experiment. In order to address data categories dominant in interactive EC Web sites, P3P has so far only provided for the overall data categories <interactive> and <preferences> to signal the deployment of interactive features on a site. These 2 categories, however, provide marketers with the opportunity of implementing the very type of privacy-invading communication we offered in the experiment. Since online users do have a strong incentive to generally accept interactive and preference-demanding websites (because this is basically what makes e-commerce sites interesting), there is a considerable risk for online users to sacrifice their privacy as they did in the experiment presented above. Moreover, P3P (similar to legislation) would signal the trustworthiness of the site without really living up to this standard.

Based on this, an extension of the P3P protocol would appear desirable that takes this important type of application into consideration. For example, and thanks to the openness of XML (the basis of P3P) it would be relatively easy to break down the data category <interactive> into several sub-categories that signal the 'true nature' of interaction implemented in a site. One possible way to characterize a question-answer process with a sales bot would be to distinguish between the types of questions asked by the agent. For example, a differentiation could be made between product attribute questions, usage oriented questions, personal questions supporting the selection process, and finally personal questions that have no impact on product selection. Extending the data category <interactive> by this kind of sub-categories (which we also used to design the shopping bot) would give users a 'meaningful' choice to administer privacy when they interact with sales bots, because they gain an idea of what is hidden behind the term 'interactive'. For marketers who wish to inform users of their data collection practices, these proposed sub-categories are also a

[8] For more detail on the meaning of data categories in P3P please consult the description of the latest public version of P3P (paragraph 3.4) on http://www.w3.org/TR/P3P/

cost efficient way to signal the nature of communication, as the alternative would be to encode all information demanded into separate data entities.

4.2 EU regulation

The effect of citing EU regulation in privacy statement 1 revealed a potential drawback of this approach to protect privacy: it seemed to make people feel 'secure', leading between 5 and 11% more users to reveal their home address than in the less protected environment of privacy statement 2. Also, EU regulation would probably have impeded a 'real-world' implementation of the type of communication we proposed in the experiment, because it would probably not comply with the principle of 'purpose limitation' or data collection parsimony. However, the mostly positive reactions to agent Luci are interesting when one considers the question design and content described above. They suggest that online users would appreciate the kind of 'personal' online communication that is either prohibited by law today or avoided by marketers due to their fear of intruding on users' privacy too much. An important question for the current privacy debate and research initiatives in this field is therefore how e-privacy could be guaranteed to people while still allowing them to benefit from 'rich' and 'soft' online communication.

4.3 Pseudonymity, identity management systems and private credentials as a way out of the privacy dilemma?

Assuming that people want rich communication (as current results suggest) and are willing to 'chat' about themselves, EC environments should provide for this desire and offer more soft communication and interaction than is currently the case [23]. Fears of 'intruding' on users' privacy by asking them more personal questions online seem unfounded on the background of survey results presented above. However, even if consumers did not display a particularly privacy-conscious behaviour in our study, there are still many reasons for companies to care about the subject. Not only do they confront EU regulation (even if they are in the US), but in order to leverage the true benefits of 'e-loyalty' they should not build on the long-term persistence of their customers' current ignorance, but ensure that consumers feel free to communicate frankly and truthfully even as their privacy concerns are on the rise.

The way to realize both marketer benefits through data-intensive personalization on the one hand and e-privacy on the other may lie in the concept of pseudonymity [20]. As long as pseudonyms cannot be linked to the identity of a user (at least not for regular EC transactions) he or she can remain relatively anonymous in the online world and feel more at ease to interact. Personalization could then be applied to these pseudonyms while still reaching the customer in person. Of course, pseudonymity is not a new phenomenon to the online world as companies such as e-bay or Yahoo! already employ it in their Web sites. However, current use of pseudonyms is still in its infancy. Not only is pseudonymity sacrificed at the moment of buying when users reveal their true identity, but also the management of pseudonymity is cumbersome. Users have to manage the complexity of an ever-rising number of virtual identities, and marketers employing pseudonyms have to maintain a database of a rising number of 'lifeless' (unused) user equivalents. The approach of currently proposed, simple-to-use identity management systems may therefore represent an important privacy technology of the future [15,16]. They would be able to assist online users in controlling their virtual identities and also ensure that customers revisit sites under the same virtual identity if they wish to (situational pseudonyms). More importantly, however, they are envisaged to include anonymous authentication methods and private credentials [8] so that transactions are supported while users are not left alone with complex technology they do not understand [11].

5. OUTLOOK

The results obtained are important for the current privacy debate. Not only does the study in itself represent the biggest empirical observation of actual privacy behavior, but in its set-up it was also adapted to the 2nd generation E-commerce type of sales environment lying ahead. More importantly, it revealed a major misconception of the current privacy debate: that people behave in the way they say they will. This result suggests that the development of privacy technologies needs to take a twist into a new direction: they need to be designed in such a way that they allow even moderately computer-literate online users to protect themselves from the degree of self-disclosure they are afraid of.

In evaluating the results, some limitations should be taken into account. First, most participants were from a university environment. Their comparatively high level of education may have created a group that is actually more privacy-conscious than the average population. On the other hand, that group may have more trust in data protection regulations. The experimental setting may also have had an effect on the quality of online interaction. In particular, the high-bandwidth online connection may have induced participants to engage more actively in a question-answer dialogue than they would have done using a low-bandwidth modem at home.

ACKNOWLEDGEMENTS

We wish to thank Karstadt Quelle New Media (KQNM) for sponsoring the IWA experiments, Artificial Life for lending us their 3-D bot, Martin Strobel (Infonomics, The Netherlands) for assisting the experimental set-up and programming the store, Oliver Günther (Institute of Information Systems), Marit Köhntopp (Independent Centre for Privacy Protection Schleswig-Holstein, Germany), and Elke Brenstein (Institute of Pedagogy and Informatics) for helpful suggestions on earlier drafts. We are grateful to Humboldt University Berlin and the NaFög scholarship programme for financially supporting the authors.

REFERENCES

[1] Ackerman, M.S., L.F. Cranor and J. Reagle, "Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences", in: Proceedings of the ACM Conference on Electronic Commerce EC'99, 1999.

[2] Annacker, D., Spiekermann, S., Strobel, M., "E-privacy: A new search cost dimension in online environments", 14th Bled Conference of Electronic Commerce, June 2001, download: http://www.wiwi.hu-berlin.de/~sspiek/phdresearch.html

[3] Ansari A., Essegaier, S., Kohli, R., "Internet Recommender Systems", in: Journal of Marketing Research", Vol. 37, August 2000, pp. 363-375.
[4] Berendt, B. (2000). "Web usage mining, site semantics, and the support of navigation". In: Workshop "Web Mining for E-Commerce Challenges and Opportunities." KDD 2000, August 2000. Boston, MA. pp. 83-93.
[5] Bäumler, H., "Datenschutz im Internet", in: E-Privacy, ed. by Helmut Bäumler, Wiesbaden, 2000, pp. 1-8
[6] Berry, M., Linoff, G., "Data Mining Techniques for Marketing, Sales and Customer Support", Wiley, NY, 1997.
[7] Borking, J., "Erwartungen an die Datenschutz-beauftragten im Internet", in: E-Privacy, ed. by Helmut Bäumler, Wiesbaden, 2000, pp. 280-290.
[8] Brands, S., "Rethinking Public Key Infrastructure and Digital Certificates – Building in Privacy", Thesis, 1999, 2nd edition: The MIT Press, August 2000.
[9] Cassell, J., "Embodied Conversational Interface Agents", in: Communications of the ACM, Vol. 43, No. 4, April 2000, pp. 70-78.
[10] Chang, A., Kannan, P., Whinston, A., "The Economics of Freebies in Exchange for Consumer Information on the Internet: An Exploratory Study", in: Int. Journal of Electronic Commerce, Vol. 4, No. 1, Fall 1999, pp. 85-101.
[11] Clauß, S., Köhntopp, M., "Identity Management and Its Support of Multilateral Systems", accepted for publication in the Special Issue on 'Electronic Business Systems' of Computer Networks; until publication available directly from marit@koehntopp.de.
[12] 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: http://europa.eu.int/comm/internal_market/en/media/dataprot/law/index.htm.
[13] Hagel, J., Rayport, J., " The Coming Battle for Customer Information", in: Harvard Business Review, January-February 1997, pp.53-65.
[14] Häuble, G., Trifts,V., "Consumer Decision Making in Online Shopping Environments: The Effects of Interactive Decision Aids", in: Marketing Science, April 2000.
[15] Köhntopp, M., "Wie war noch gleich Ihr Name? – Schritte zu einem umfassenden Identitätsmanagement", accepted at the conference *VIS – Verlässliche IT-Systeme*, Kiel, Germany, September 2001.
[16] Köhntopp, M., Pfitzmann, A., "Datenschutz Next Generation", in: E-Privacy, ed. by Helmut Bäumler, Wiesbaden, 2000, pp. 316-322.
[17] Moon, Y.: The Interface Project: http://www.people.hbs.edu/ymoon/Interface/home.html
[18] Moon, Y., Intimate Exchanges: Using Computers to Elicit Self-Disclosure from Consumers, in: Journal of Consumer Research, Vol.27, No.4, March 2000.
[19] Pew Internet & American Life Project, Trust and Privacy Online: Why Americans Want to Rewrite the Rules, 2000-8-20, http://pewinternet.org/reports/toc.asp?Report=19.
[20] Pfitzmann, A., Köhntopp, M., "Anonymity, Unobservability, and Pseudonymity – A Proposal for Terminology", in: Designing Privacy Enhancing Technologies, *Proceedings of WS on Design Issues in Anonymity and Unobservability*, LNCS 2009, Heidelberg, 2001, revised version http://www.-koehntopp.de/marit/pub/anon/Anon_Terminology.pdf.
[21] Schaar, P., "Die Möglichkeiten der Datenschutzaufsichtsbehörden", in: E-Privacy, ed. by Helmut Bäumler, Wiesbaden, 2000, pp. 69-76.
[22] Schafer J., Konstan, J., Riedl, J., "RS in E-Commerce", in: Proceedings of the ACM Conference on Electronic Commerce EC'99, 1999, pp. 158-166.
[23] Spiekermann, S., Corina, P., "Motivating Human-Agent Interaction : Transferring Insights from Behavioral Marketing to Agent Design", in: Proc. of the 3rd International Conference on Telecommunications and Electronic Commerce, ICTEC3, 2000, pp. 387-402.
[24] Spiliopoulou, M., "Web Usage Mining for Web Site Evaluation – Making a site better fit its users", in: Communications of the ACM, No. 8, Vol. 43, August 2000, pp. 127-134.
[25] Urban, G., F. Sultan and W. Qualls, "Design and Evaluation of a Trust Based Advisor on the Internet", MIT, December 1999.
[26] Wells, N. and Wolfers, J., "Finance with a Personalized Touch", in: Communications of the ACM, No. 8, Vol. 43, August 2000, pp. 31-34.
[27] West P., D.Ariely, S.Bellman, E.Bradlow, J.Huber, E.Johnson, B.Kahn, J.Little and D.Schkade, "Agents to the Rescue?", HEC Invitational Choice Symposium, February 1999.
[28] Westin, A., "Harris-Equifax Consumer Privacy Survey", Atlanta, GA: Equifax Inc. (1996).
[29] Vulcan, N., "Economic Implications of Agent Technology and E-Commerce", in: The Economic Journal, February 1999, pp. 67-90.