Electronic Privacy, Trust and Self-Disclosure in E-Recruitment

Jennifer Nickel
Freie Universität Berlin
Center for Media Research
Malteserstr. 74-100
12249 Berlin, Germany
jenickel@zedat.fu-berlin.de

Heike Schaumburg
Humboldt Universität zu Berlin
General Education and Instructional Research
Unter den Linden 6
10099 Berlin, Germany
heike.schaumburg@staff.hu-berlin.de

ABSTRACT
The present study extends the research on user trust in e-commerce to the area of e-recruitment, focusing specifically on the importance of perceived privacy to evoke user trust and self-disclosure. Two websites of a fictitious online recruitment site were compared, which differed only in their level of perceived privacy. It was found that an interface conveying a high level of privacy significantly increased user trust. Although users with high trust scores also disclosed more and more sensitive information than users with low trust scores, this could not be attributed solely to the perceived privacy of the online job bank.

Categories & Subject Descriptors: K.4.1. [Computers and Society] Public Policy Issues -- Privacy, K4.3 [Computers and Society] Organizational Impacts -- Employment, K.4.4 [Computers and Society] Electronic Commerce -- Electronic Data Interchange, Security

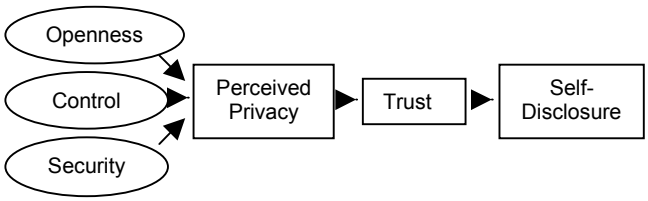
Categories & Subject Descriptors: Human Factors

Keywords: Trust, self-disclosure, online experiment, control of personal data, e-recruitment

INTRODUCTION

E-recruitment is becoming increasingly popular among employment services as well as individual companies looking for qualified applicants to fill their open positions. In order to successfully screen candidates and match them to the jobs available, it is indispensable that applicants enter informative profiles including a substantial amount of personal data into a job database. Yet, many studies conclude that Internet users have serious doubts about data security and e-privacy and are hesitant to disclose personal data via the Internet [7, 8]. E-privacy is seen as a crucial factor for building user trust in Internet applications, specifically in e-commerce websites [3, 4]. While the relationship of e-privacy and user trust has been examined extensively, there is only little research on self-disclosure. Also, the majority of studies to date is survey-based, whereas the actual behavior of users when faced with a potential violation of their electronic privacy has been investigated much less. Finally, the bulk of existing studies has been conducted in the area of online shopping [6], while there is almost no research investigating e-recruitment, where the disclosure of even more and more sensitive data is demanded of the user. The present study was designed to shed light on the importance of e-privacy for user trust and actual self-disclosure in e-recruitment

CHI 2004, April 24–29, 2004, Vienna, Austria.
ACM 1-58113-703-6/04/0004.



Based on the work of Egger [4], Tan and Thoen [9], Altman [1] and Laukka [7] we suggest that the level of self-disclosure depends on the user's trust in a given website, which in turn is influenced by the level of perceived privacy of the website (see figure 1).

Figure 1: Suggested factors influencing self-disclosure

We assume that there are essentially three dimensions affecting the perceived privacy of an online recruitment site: openness, control and data security. *Openness* has already been introduced by Egger [4] in his trust model (labeled there as "privacy"). Openness means that the website provides information on the kind of data gathered and the purpose it will be used for, on the identifiability of the customer on the basis of his data and on the techniques of data collection. Also, relevant information on the provider's electronic privacy policy should be understandable and easily accessible. *Control* means that the user is able to easily revise and delete his personal data, that data will be given to a third party only with the user's expressed consent and that the user is immediately being informed about changes in the e-privacy policy. *Data security* finally refers to the technical security of the data transfer as well as the secure storage and processing of the customer's personal data.

According to the model of Tan and Thoen [9] each individual has a personal threshold to acting trustfully and will only engage in an online transaction if her trust level

exceeds this personal threshold. We assume that perceived privacy is crucial in building trust beyond this threshold. The higher the perceived privacy of a given website, the more likely it is that the user will trust the e-recruiter and consequently disclose personal information.

Altman [1] defines the level of self-disclosure as a mental state of a person that decides if she is willing to share personal information in a given situation. How much information is shared is highly dependent on the person's trust in the other party. In a face-to-face situation, a person has different mechanisms to regulate the level of self-disclosure. In an online environment, these can be reduced to three options: the user can fully disclose his personal information, he can withhold personal information or he can give false statements [7]. In our experiment we focus on the first two options, i. e. the amount of personal information disclosed as a result of perceived privacy of a given website.

METHOD

The model was tested with an online experiment comparing two versions of a fictitious online recruitment site (see figure 2 and 3), which differed only in their perceived privacy (high privacy vs. low privacy).

Figure 2: Homepage of the online recruitment site (low privacy version)

The interface of the high privacy version was designed to convey a maximum level of perceived privacy according to the above-mentioned dimensions. For example, the users were assured that data was not forwarded to a third party (openness), they were able to edit their information (control) and data was transmitted through a secure connection (security). The low privacy version explicitly stated that data could be used for purposes beyond recruitment, it did not allow the users any control over what happened to their personal data once it was submitted and data was never transmitted through a secure connection.

The effectiveness of the treatment in evoking a different amount of perceived privacy was verified through a pre-test. 12 participants were randomly assigned to one of the two conditions and asked to rate the privacy of the online recruitment site using a 7-item scale developed and validated by Kammerer [5]. Additionally, they were asked to rate the subjective information cost for disclosing different information items (e. g. name, age, current income) on a scale from 1 (low information cost) to 5 (high information cost). Following Annacker, Spiekermann and Strobel [2], information cost was defined as "'intuitive readiness' to truthfully answer a given item" (p. 5) in the job bank. The procedure for determining user cost was also adapted from Annacker et al.

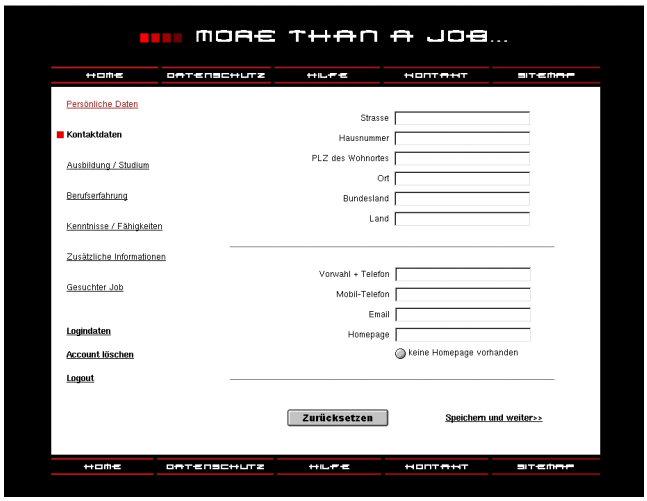


Figure 3: Personal data entry form of the recruitment site (low privacy version)

In the subsequent web-based experiment with a different group of participants subjects were led to believe that they took part in a usability test for a newly developed online recruitment site, which would go online shortly. They were told that as participants of this study, they had the opportunity to enter their data into the job bank and use the e-recruitment service for free. Subjects were again randomly assigned to the high vs. low privacy version of the website. Of the 39 persons who logged on to the experiment, 30 persons filled out the subsequent online questionnaires and were hence included in the study. User trust was determined with two scales developed by Kammerer [5] measuring *trust attitude* and *projected trust behavior*. In his study, Kammerer reports excellent reliability scores for these scales (α= .95 and .97).

Self-disclosure was measured quantitatively and qualitatively. The *quantity of self-disclosure* was defined as the number of information items of the recruitment site that the person had filled in. The *quality of self-disclosure* was calculated by weighing the items the person had filled in according to the information cost values determined in the pre-test. The *general trust level*, the *experience of the subjects with the WWW and online recruitment sites* as well as the subjects' *general attitude towards Internet privacy* were included in the experiment as control variables.

RESULTS

The data of the pre-test was analyzed using an independent samples *t*-test to determine if there was a difference in perceived privacy between the two websites. The results confirmed the effectiveness of the treatment: the two websites differed significantly in perceived privacy ($t_{5,913}$=6.90; p<.05). On average, participants had only medium to low concerns to answer the items of the online recruitment site truthfully (x=2.36; SD=0.95). The information cost was rated lowest for the items *mother*

tongue, first name, last name and *year of graduation from school* whereas the items *membership in an organization, telephone number* and *current income* had the highest information cost.

To test the hypothesis of the main experiment that the perceived privacy would impact user trust, a covariance analysis was calculated with the website version as fixed factor and the above-mentioned control variables as covariates. The control variables did not have any significant effect on the dependent variables.

The results of the main experiment provide evidence for the assumption that the perceived privacy of an online recruitment site enhances user trust. Users of the high privacy website had significantly higher scores on the two variables *trust attitude* ($F_{1,25}$=4.372; p<.05) and *projected trust behavior* ($F_{1,25}$=4.653; p<.05) than users of the low privacy website (see figure 4).

Figure 4: Average trust scores in treatment groups

As mentioned above, we assumed that perceived privacy affects trust and subsequently the quantitative and qualitative self-disclosure of the users. To test this assumption, trust attitude and projected trust behavior were collapsed into one scale and participants were divided by the median of that scale into a high and a low trust group. The new variable *overall trust* was included into the covariance analysis as a second factor.

The main effect of overall trust proved to be statistically significant for quantitative ($F_{1,23}$=5.140; p<.01) as well as for qualitative self-disclosure ($F_{1,23}$=4.517; p<.01). However, as can be seen from figure 5, it cannot be concluded that high privacy yields trust, which in turn causes a high level of self-disclosure. In fact, it seems that privacy and trust can compensate one another: If the perceived level of privacy is high even users with otherwise low trust disclose a high level of personal information and similarly, when the perceived privacy is low users still disclose personal information if the websites succeeds in otherwise evoking user trust. Only if both, perceived privacy *and* user trust are low the willingness to disclose personal information is minimal. This interaction of perceived privacy and trust could not be confirmed in the variance analysis however, neither for quantitative ($F_{1,23}$=1.843; p>.05) nor for qualitative self-disclosure ($F_{1,23}$=1.843; p>.05). The non-significance may be due to the small number of cases in the analysis.

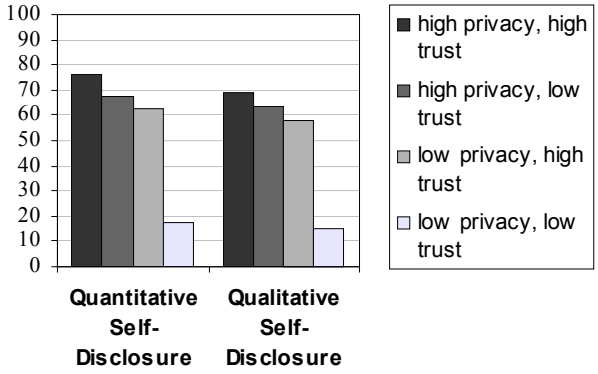


Figure 5: Quantitative and qualitative self-disclosure

DISCUSSION

The present study yields some interesting insights in the mechanisms underlying disclosure of information by Internet users. It could be shown that perceived e-privacy is an important factor in the trust building process. This finding, which is well established from previous research in e-commerce, was replicated in this study for e-recruitment. Trust, in turn proved to be of significant importance for self-disclosure. However, further analysis revealed that privacy and trust do not have to concur to evoke a high level of self-disclosure but rather seem to compensate each other.

Thus, our initial model needs to be altered (see figure 6). First, perceived privacy not only influences trust (and thereby self-disclosure) but there also seems be a direct impact of perceived privacy on self-disclosure. Second, there are obviously other factors, which have an impact of similar strength on user trust and self-disclosure. Thus, further factors influencing user trust should be included in the model and it has to be assumed that these factors can override the effect of perceived privacy.

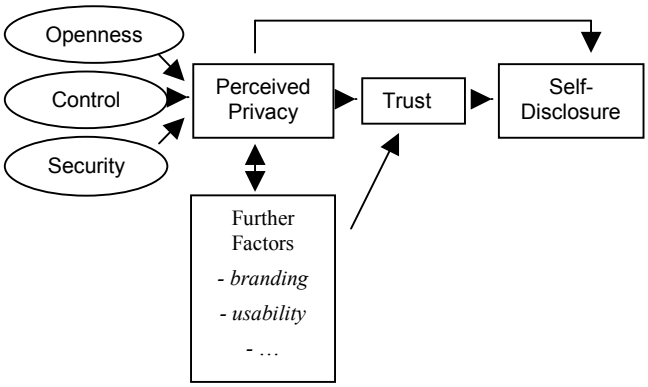


Figure 6: Revised model of factors influencing self-disclosure

It is concluded that self-disclosure depends on multiple inter-related factors. Future studies should further explore the conditions under which users are encouraged to disclose personal information. A suitable starting point for this

endeavor could be existing research and theory on trust in e-commerce, e g. [3, 4]. The sources of trust postulated in these studies should be explored for their importance in eliciting self-disclosure. Looking at different causal factors simultaneously would provide valuable information on their interactions and would thus expand and advance our current knowledge on user trust and self-disclosure.

From a practical perspective, the results of the present study suggest that website providers like e-recruiters who rely heavily on the personal self-disclosure of their customers should take special care of privacy issues. Yet, privacy is only one factor influencing self-disclosure. It could be shown that self-disclosure was high as long as the users trusted the website they were using. Therefore, providers of online recruitment sites should also take measures in addition to providing a high level of e-privacy to evoke user trust. These could be actions like establishing a brand name or ensuring a good usability of the website, which have proved to be relevant factors for building user trust in e-commerce [3, 4].

Because e-recruiters on the one hand are necessarily interested in getting as much valid information of their customers as possible and because users on the other hand increasingly distrust data collection on the Internet the ability to build user trust will be a decisive competitive advantage of e-recruitment sites in the future.

ACKNOWLEDGEMENTS

We would like to thank M. Schmitz for technical support in this project.

REFERENCES

1.Altman, I. (1975). *The environment and social behavior: Privacy, personal space, territory, crowding.* Monterey, CA: Brooks/Cole.

2. Annacker, D. Spiekermann, S. & Strobel, M. (2001). E-privacy: A new search cost dimension in online environments. *Proceedings of the 14th Conference of Electronic Commerce*, Bled, Slovenia, June 25-26. [Online: http://www.wiwi.hu-berlin.de/~sspiek/artikel/Bled_final.pdf].

3.U.S. Public Interest Research Group. .Public Comment on Barriers to Electronic Commerce. Response to call by U.S. Department of Commerce (65 Federal Register 15898), April 25, 2000.

4. Egger, F. N. (2000). "Trust me. I'm an online vendor": Towards a model of trust for e-commerce system design. *CHI 2000 Extended Abstracts*, The Hague, The Netherlands, April 1-6. [Online: http://www.zurich.ibm.com/~mrs/chi2000/contributions/egger.html].

5.Kammerer, M. (2000). *Die Bestimmung von Vertrauen in Internetangebote.* Lizensiatsarbeit der Philosophischen Fakultät der Universität Zürich.

6.Ku, Y. C,. Liu, C. Marchewka, J. & Mackie, B. (2000). A study of consumer's trust in privacy in electronic commerce. *Proceedings of the 12th International Conference on Comparative Management.* Kaohsiung, Taiwan, May, 23-25.

7. Laukka, M. (2000). Criteria for privacy supporting system. *Proceedings of the 5 th Nordic Workshop on Secure IT Systems,* Reykjavik, Iseland, Oct. 12-13. [Online: http://www.tml.hut.fi/Research/TeSSA/Papers/Laukka/Laukka_nordsec2000.pdf]

8.Novak, T.P., Hoffman, D.L. & Peralta, M.A. (1999). Building consumer trust online. *Communications of the ACM, 42, 4,* 80-85.

9.Tan, Y-H. & Thoen, W. (2000). Formal aspects of a generic model of trust for electronic commerce. *Proceedings of the 33rd Hawaii International Conference on System Sciences*, Maui, Hawaii, Jan. 4-7. [Online: http://www.computer.org/proceedings/hicss/0493/04936/04936006.pdf]..