Sharing in the Dark? Target Memory and Risk Awareness in Online Communication

Ricarda Moll (r.moll@uni-muenster.de)
Stephanie Pieschl (pieschl@uni-muenster.de)
Rainer Bromme (bromme@uni-muenster.de)
Department of Psychology, Westfälische Wilhelms-Universität Münster
Fliednerstr. 21, 48149 Muenster, Germany

Abstract

A high degree of self-disclosure in Online Social Networks (OSNs) is associated with several risks. This raises an important question: Why don´t many users protect their personal data more eagerly? We propose that a lack of memory for what information has been disclosed to which audience contributes to this privacy-neglecting behavior in OSNs. We transferred the paradigm of target monitoring to a fictitious OSN and varied the degree of risk associated with self-disclosure. In a 2x2 experiment we varied both audience size (large vs. small) and information intimacy (personal vs. non-personal). We used recognition tests for the association of audience and disclosed information to assess memory performance. Results show that item memory (the memory for what information has been disclosed) exceeded target memory and that target memory improved in vulnerable situations (for large audiences and personal information). Our findings widen the realm of offline memory research and expand our knowledge about which cognitive factors impact privacy-related behavior in online environments.

Keywords: Target Memory, Online Self-Disclosure, Risk Awareness

Introduction

Self-Disclosure in OSNs

Self-disclosure is an important mechanism in relationship formation and trust development (Jourard & Lasakow, 1958). Lately much research has investigated the benefits of sharing personal information on OSNs-platforms i.e. in terms of self-esteem and identity formation (Valkenburg & Peter, 2011). At the same time this behavior is associated with several risks. For example, it is not uncommon that employers retrieve information of their job applicants through an online search that includes profile information on OSNs. This information often decides to whom the announced job position is offered (Zeidner, 2007). Interestingly, many users actually are concerned about potential data misuse but nevertheless choose to reveal personal information in OSNs, a pattern that is known as privacy paradox (Norberg, Horne, & Horne, 2007). Some scholars argue that privacy related decisions result from a logical calculation in which risks and benefits of self-disclosure are rationally weighed against each other (Xu, Teo, Tan, & Agarwal, 2010). If users self-disclose despite their concerns, the benefits must be larger and/or more probable than the associated risks. However, we argue that privacy-related calculations might be biased, because users could lack important information to assess the actual amount of vulnerability: Online revelation of personal information is usually done over and over again and while the single event is indeed not that risky, its repetition produces a cumulative amount of online information about the user (indicating a corresponding amount of cumulative risk). One important detail that is crucial for the assessment of this cumulative risk is the *memory* for which information has been disclosed, and to whom it is available.

Target Memory in Offline Interactions

Recently it has been shown that people struggle to remember the targets of their messages in offline contexts. For example, in one of their experiments Gopie and MacLeod (2009) investigated how well people remember having disclosed fifty personal facts to pictures of famous people in comparison to impersonal facts. Results show that people successfully identified the facts they had disclosed (item memory) but had problems associating facts and targets (target memory); they did not remember to whom they disclosed what. In another study Marsh and Hicks (2002) let participants repeatedly choose to whom they wanted to give different kinds of objects. The authors conclude that this decisional aspect leads to a deeper elaboration of the situational context which then facilitates subsequent retrieval. Finally, Brown, Hornstein, and Memon (2006) let participants tell various pieces of information to five different celebrity pictures on five subsequent days. On-line and retrospective target memory declined with the number of previous “interactions”, indicating a confusion of which information was given to whom.

In the light of these findings it seems plausible to assume that target memory problems also exist online. Therefore, we transferred the paradigm of target monitoring to the environment of OSNs. As a prerequisite for further analysis we assumed that participants remember what information they disclosed but struggle remembering to whom. We thus

hypothesized that item memory exceeds target memory (hypothesis 1).

Risk Cues in Online Communication

There has been much discussion on how online environments change the nature of communication and information processing (Kiesler, Siegel, & McGuire, 1984). However, while OSNs environments are somewhat deprived of conventional context cues that could support the encoding and decoding of information, other situational factors could be more relevant for target memory in OSNs. For example, the elaboration likelihood model (Petty, Cacioppo, & Kasmer, 1988) argues that when people are motivated they process information in a more elaborate way. It seems plausible that people are more motivated if they feel at risk. People could therefore process risky situations more thoroughly than neutral ones. This could be especially true for online interactions since the accessibility and distribution of information is inherently more difficult to control. Furthermore, studies in associative memory research have demonstrated that the emotional intensity of an event has a major impact on memory performance (LaBar & Cabeza, 2006). As we can assume that perceived risk does cause some sort of arousal or emotion (Slovic & Peters, 2006) it seems plausible that risk cues could have a positive impact on target memory performance in OSNs. In this study we focused on two major aspects that could influence perceived vulnerability: a) the kind of information that is disclosed and b) the kind of audience that gains access to the information.

Information Gopie and MacLeod (2009) found that target memory performance was worse when people disclosed personal facts in comparison to impersonal facts. In line with Koriat, Ben-Zur, and Druch (1991) the authors argue that revealing personal details increases self-focus which prevents people from integrating the outer environment as a reference point of that event. Impersonal information on the other hand would not trigger the same amount of self-focus resulting in better target memory performance. However, we believe that in OSNs the degree of intimacy of information serves as a distinct risk cue, because disclosing personal information gives the audience´s members more opportunities for personal judgment and information misuse. We therefore predicted that target memory would improve when the disclosed information is personal rather than impersonal (hypothesis 2).

Audience Perceived vulnerability does not only vary with the nature of the information but also with the nature of the target. Thus, perceived vulnerability seems to increase with the number of people who have access to this information (Bateman, Pike, & Butler, 2011). Slonje and Smith (2008) similarly showed that cyberbullying victims experience the unwanted disclosure by others as especially harmful when a large group gains access. Naturally, a larger group is not only more difficult to control but necessarily contains more members that are less trusted. Publicity thus seems to be an important factor for risk awareness during online self-disclosure. Therefore, we assumed better target memory for larger than for smaller audiences (hypothesis 3).

Hypotheses

To summarize, this study addresses two different aspects of risk awareness and memory performance in online self-disclosure. On the one hand we assumed that overall target memory problems also exist online. We predicted that people easily remember what information they disclosed (item memory), but not to which audience (target memory; hypothesis 1). On the other hand we presumed that people cognitively react to *specific* risk cues like the intimacy of the disclosed information (personal vs. impersonal information) and the size of the audience that receives the message (small vs. large audience). We therefore hypothesized that target memory would improve when information is personal rather than impersonal (hypothesis 2) and when the receiving audience is large rather than small (hypothesis 3).

Method

Participants

Participants were senior students from high schools in the area of Münster, Germany. We excluded two participants from data analysis, because they did not follow the instructions as requested. Thus, our sample consists of 99 participants (34 males, 65 females) with a mean age of 17.59 years (SD = 2.08).

Materials

Scenario Students entered a fictitious social networking site of the local university**.** Within this site participants entered a sham discussion group where they would be posting information concerning the topic of the group. Students were aware that they were part of an experimental study.

Information In the personal condition students entered the fictitious discussion group “to get to know each other”. Items in the personal condition were partly taken from former studies about relationship formation (Joinson, 2001; Jourard & Lasakow, 1958), partly taken from what is typically disclosed in online profiles (e.g. “your favorite music”) and partly self-created (e.g. “what is the meaning of life in your opinion”). In the non-personal condition students entered the sham group “information about the city of Münster”. Items in this condition were taken from an online tourist brochure about the city of Münster (e.g. “famous band from Muenster - H-Blockx” or “founding year of the city of Muenster - 793”).

Audiences The disclosed information would be sent to either everyone in the students´ semester (*large* audience;

180 people) or only to their future study group (*small* audience; five people). We defined the size of the audiences to approximate how online social networks are arranged. In 2011 the average network of a Facebook user consisted of around 190 Facebook-friends (Ugander, Karrer, Backstrom, & Marlow, 2011). Usually, a core group of these people are active contacts the user communicates with on a frequent basis (strong ties). The rest of the network constitutes weak ties – users passively keep in touch with these contacts, but not necessarily interact with them on a regular basis (Ellison, Steinfield, & Lampe, 2007). Please note that the audiences in this experiment did not constitute strong and weak ties per se since participants had no actual relation to the displayed people whatsoever.

Communication Task The communication task consisted of 20 randomized slides. On each slide students saw two facts at the top of the page (personal or non-personal). They decided which one they wanted to disclose and marked that one. In the personal condition we paired facts with a similar degree of intimacy. In the impersonal condition we paired facts that both contained either numerical or textual information. The audience (small or large) was saliently displayed underneath these two facts via a collection of small-scaled photos that matched the number of the announced audience size. Participants were instructed to choose one of the two facts and disclose it at the bottom of the page where they wrote the information into an empty text field. Ten facts were disclosed to a *small* target audience, ten facts to a *large* target audience and thus twenty facts were *not disclosed* because they were not chosen. While the students could choose which one out of the two facts they wanted to disclose, the audience was predetermined and could not be selected. We incorporated this decisional aspect to enhance the external validity of our experiment: People presumably choose more or less carefully what information they disclose (Marsh & Hicks, 2002) - not only for privacy reasons but also because this information becomes an inherent part of their self-presentational strategy. Interestingly, many Facebook users would rather decide *what* to disclose, instead of to whom, since many report that they make all their information and actions visible to all of their Facebook-friends. Therefore, participants in our experiment could decide what information they wished to disclose but not to which audience.

Memory Task The memory task consisted of 50 randomly presented test slides that contained the forty facts of the communication task plus ten completely new facts. For each displayed fact the students indicated if they had disclosed this fact to a *small* target audience, a *large* target audience, if it was a fact they hadn´t seen before (*new*) or if they had encountered this fact but *not disclosed* it (each of the first three options was correct in 10 times of the cases, the last option in 20 times of the cases). Items that were new or had not been chosen to be disclosed in the learning phase were treated as distractors.[1]

Internet Literacy Questionnaire The internet literacy questionnaire (Stodt, Moll, Polzer, Pieschl, & Brand, 2013) consists of twenty items measuring online literacy in terms of technical skills, online empathy, online interactions, and privacy-related attitudes and behaviors.[2] This questionnaire was incorporated to create latency between the communication task and the memory task and to thus weaken short term memory effects.

Procedure

Students were recruited during an open day of the Westfälische Wilhelms-Universität Münster. Groups of students sat down in front of a computer screen to participate in the experiment. We conducted a 2x2 experiment with *information* (*personal* versus *impersonal*) as a between-subject factor and *audience size (small* versus *large)* as a within-subject factor. After being welcomed the students were randomly assigned to the information conditions. They received a short description of the scenario and entered the communication task. Afterwards students answered the internet literacy questionnaire as a short filler task, being followed by an explanation on how to work on the subsequent memory task. After this memory task students shortly answered questions about their OSNs-usage and socio-demographic details. After completing the experiment students were offered the chance of winning one out of six gift cards for the online shop *Amazon*. Students were encouraged to leave an email-address so we could explain the purpose of the experiment after data analysis had been completed. They were then thanked for their participation and dismissed.

Results

The random assignment to between-subject conditions was successful. Demographic details in the *personal* condition (n = 49; 31 females, 18 males; M = 17.55 years, SD = 1.02) did not differ significantly from the *impersonal* condition, (n = 50; 34 females, 16 males; M = 17.62 years, SD = 2.76).

Target Memory

As a prerequisite for further analysis we assessed if there actually is a target memory problem in comparison to item memory. In order to do so, we compared the mean number of correct audience identifications (*small* and *large*

[1] Additionally, students indicated on 5-point Likert-scales how confident they were about the correctness of each of their answers. These results are not reported here as they addressed a different research question that due to space constraints cannot be reported in this paper.

[2] The results of this questionnaire are not part of this report as no meaningful factor structure could be found in this sample.

audiences) as indicator of target memory with the mean number of correct distractor identifications (*not disclosed* and *new* facts) as indicator of item memory in a repeated-measure ANOVA. *Information* was the between-subject factor. Item memory significantly exceeded target memory across both information conditions, $F(1,98) = 262.08$, $p < .001$ $\eta_p^2 = .73$ (see Figure 1), indicating better memory for which information had (not) been disclosed than to which audience it was disclosed.

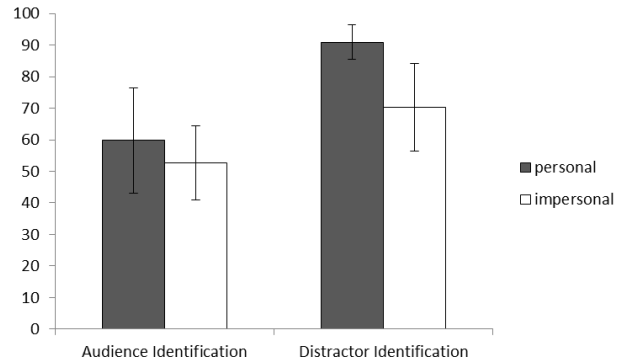

Figure 1: Percentage of correctly identified audiences and distractors per *information* condition (error bars indicate standard deviations).

We also found a significant main effect for *information*, $F(1,97) = 46.25$, $p < .001$, $\eta_p^2 = .32$ as well as a significant interaction between the two factors, $F(1,97) = 19.89$, $p < .001$, $\eta_p^2 = .17$. The difference of correct audience and distractor identification was larger in the *personal* condition than in the *impersonal* condition.

Risk Cues

To test hypotheses two (target memory improves for *personal* in comparison to *impersonal* information) and three (target memory improves for *large* audiences in comparison to *small* audiences) we computed a 2x2 repeated-measure ANOVA with audience size (*small* vs. *large*) as repeated-measure factor and information (*personal* vs. *impersonal*) as between-subject factor. Our dependent variable was the mean number of correct target identifications in each condition. We found a significant main effect of *information*, $F(1,97) = 6.15$, $p < .015$, $\eta_p^2 = .06$. Memory performance in the *personal* condition exceeded performance in the *impersonal* condition regardless of audience size (see Figure 2). Furthermore, we found a significant main effect for *audience size*, $F(1,97) = 51.044$, $p < .001$, $\eta_p^2 = .35$. Memory performance was better when the target audience was *large* opposed to *small* - regardless of information (see Figure 2). The interaction of the two factors was not significant, $F(1,97) = .43$, $p = .51$, $\eta_p^2 = .00$. The descriptive results of the memory test also indicate that students had a general answering bias; students in both *information* conditions overall answered "large audience" more frequently than "small audience" (see row "Total chosen" in Table 1).

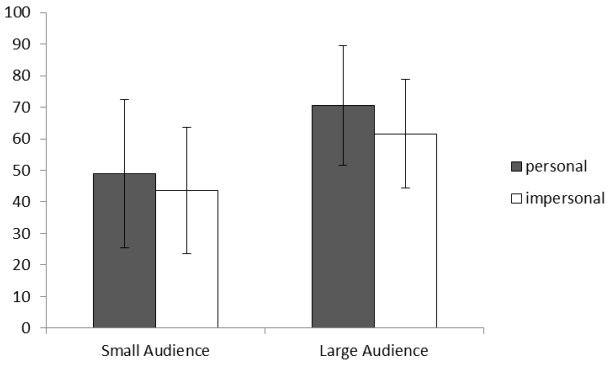

Figure 2: Percentage of correctly identified targets for the experimental factors *audience* (X-axis) and *information* (error bars indicate standard deviations).

Discussion

Overall Target Memory

Participants correctly identified significantly more distractors (*new* and *not disclosed* facts) than they identified the associated audiences of disclosed information (*small* and *large* audience). We thus confirmed our first hypothesis that item memory would be superior to target memory: Students struggled to remember what information they had disclosed to which audience. Thus our study shows that target memory problems exist online and might contribute to repeated privacy-neglecting behavior in OSNs: Without the memory of what audience has access to which information the cumulative risk of online self-disclosure must be constructed on an abstract level that is weighed out by the immediate benefits of the same behavior. Our study thus not only expands the realm of target memory research but also contributes to further explanations of the circumstances under which privacy-related decisions are made in online environments. Interestingly, error rate analysis shows that participants mainly confused the audiences *or* the distractors, but rarely identified a disclosed piece of information as a distractor or a distractor as having been disclosed (see Table 1). Thus participants were well aware of *what* they disclosed, but had trouble remembering to whom. This finding holds the encouraging notion that OSNs users are not blindly "sharing in the dark" – they are not disclosing information without any memory of past revelations whatsoever.

Table 1: Percentages of chosen options per information condition in the memory task.

	Correct Response	Responses given by participants			
		Small	Large	Not Discl.	New
Personal Information	Small	**49%**	43%	7%	1%
	Large	27%	**71%**	1%	1%
	Not Discl.	3%	3%	**84%**	10%
	New	1%	0%	1%	**98%**
	Total chosen	17%	24%	35%	24%
Impersonal Information	Small	**44%**	46%	5%	5%
	Large	29%	**62%**	6%	3%
	Not Discl.	4%	5%	**51%**	40%
	New	1%	1%	9%	**89%**
	Total chosen	16%	24%	25%	35%

Note: All percentages pertain to rows; for 'Small', 'Large', and 'New' 10 answers were given per participant, for 'Not Discl.' 20 answers were given; 'Not Discl.' is the abbreviation of 'Not Disclosed'; bold marked numbers indicate percentages of correct identifications.

The Impact of Risk Cues on Target Memory

Participants identified more target audiences correctly when they informed the audiences about something *personal* in comparison to *impersonal* information. We hereby confirmed our second hypothesis. In line with this finding we also found that distractor identification in the personal condition was superior to the impersonal condition (see Figure 1). In line with hypothesis 3, target memory performance also varied with the target audience of the disclosed message. Participants remembered more targets correctly when the audience was *large*. Furthermore, response rates show that the risk of disclosing something to a large audience seems to be especially salient, since participants more often chose "large audience" in the memory task than "small audience". We can conclude from our results that people are not oblivious to online risks but show a direct cognitive reaction to situational vulnerabilities like telling personal information or telling something to a large audience. It might be that people process the association of target and information in a more elaborate way when they feel vulnerable or when they cannot trust their interaction partners.

Limitations

Naturally, this experiment has limitations that we need to consider when interpreting our results. For one, our sample is a non-representative convenience sample. Thus, we do not know if our results can be generalized to other age and educational groups. Furthermore, in order to transfer the paradigm of target memory to the environment of OSNs we had to make several alterations from the conventional offline paradigm. These alterations restrict a direct comparison of our findings with results from former studies but substantially enhance the ecological validity of our experiment: First, as we could not find an up-to-date validated collection of intimacy-rated items we created new stimulus material for the information conditions. We thereby focused on information that is typically disclosed in online profiles as well as on details about participants´ biographical and attitudinal characteristics. The intimacy of these items varies substantially and further research is needed to assess the perceived intimacy of information in different interaction contexts as well as the role of possible self-reference effects in online environments. Second, we changed the classic operationalization of the target in our experiment. Usually a target consists of one single person represented by a photo or name. However, in OSNs users seldom communicate in one-to-one situations but rather address different kinds of audiences. Therefore, it seemed appropriate to adjust the receiving targets so that information would be disclosed to two different kinds of audiences (*small* vs. *large*). In this respect it also seems important to note that our experimental design did not allow manipulations of audience familiarity. Therefore, future research is needed to assess the generalizability of our results to real social network communication where people

usually know their audience´s members from offline contexts. Finally, our results do not fully explain the underlying cognitive mechanisms that contribute to better memory performance in risk situations. Future studies should therefore attempt to clarify this issue, for example by controlling for decision times in the communication task.

Implications

Our results show that users of OSNs actually do react to specific risk circumstances, if these are salient enough to be grasped. This indicates that users probably do not just claim to be concerned about their data (which often contradicts their behavior) but seem to automatically pay more attention to vulnerable situations in online communication. This possibility of a more thorough elaboration offers a direct practical link: From a technical view, privacy-supporting web applications should work on a less subtle and more realistic representation of the potential audience of the to-be-disclosed information. Furthermore, it seems useful to work on ways in which people get a quick overview about what they have disclosed in the past and to whom it is visible. From an educational standpoint, internet literacy programs should sensitize participants to rather subtle online risk cues, for example the degree of publicity. However, these measures cannot and should not stop users from self-disclosing in OSNs altogether since a considerable amount of research also suggests that OSNs-users benefit both emotionally and socially from their usage. The aim of design alterations and educational measures should rather be to achieve a natural consciousness so that privacy-related decisions can be beneficial after all.

Acknowledgements

This study was funded by the Research Training Group 1712/1 “Trust and Communication in a Digitized World” of the German Research Foundation (DFG). We would like to thank Christina Wohlers and Franziska Thon for their comments on this manuscript.

References

Bateman, P. J., Pike, J. C., & Butler, B. S. (2011). To disclose or not: publicness in social networking sites. *Information Technology & People, 24*(1), 78-100.

Brown, A., Hornstein, S., & Memon, A. (2006). Tracking Conversational Repetition: An Evaluation of Target Monitoring Ability. *Applied Cognitive Psychology, 20*, 85-95.

Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The benefits of Facebook 'friends:' Social capital and college students' use of online social network sites. *Journal Of Computer-Mediated Communication, 12*(4), 1143-1168.

Gopie, N., & MacLeod, C. M. (2009). Destination Memory - Stop me if I told you this before. *Psychological Science, 20*(12), 1492-1499.

Joinson, A. N. (2001). Knowing me, knowing you: Reciprocal self-disclosure in Internet-based surveys. *Cyberpsychology & Behavior, 4*(5), 587-591.

Jourard, S. M., & Lasakow, P. (1958). Some factors in self-disclosure. *Journal of Abnormal and Social Psychology, 56*(1), 91.

Kiesler, S., Siegel, J., & McGuire, T. W. (1984). Social Psychological Aspects of Computer-Mediated Communication. *American Psychologist, 39*(10), 1123-1134.

Koriat, A., Ben-Zur, H., & Druch, A. (1991). The contextualization of input and output events in memory. *Psychological Research, 53*, 260-270.

LaBar, K. S., & Cabeza, R. (2006). Cognitive neuroscience of emotional memory. *Nat Rev Neurosci 7*, 54–64.

Marsh, R. L., & Hicks, J. L. (2002). Comparisons of Target Output Monitoring and Source Input Monitoring. *Applied Cognitive Psychology 16* 845–862

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *The Journal of Consumer Affairs, 41*(1), 100-126.

Petty, R. E., Cacioppo, J. T., & Kasmer, J. A. (1988). The role of affect in the elaboration likelihood model of persuasion. In L. Donohew, H. E. Sypher & E. Higgins (Eds.), *Communication, social cognition, and affect*. Hillsdale, NJ England: Lawrence Erlbaum Associates, Inc.

Slonje, R., & Smith, P. K. (2008). Cyberbullying: Another main type of bullying? *Scandinavian Journal of Psychology, 49*, 147–154.

Slovic, P., & Peters, E. (2006). Risk Perception and Affect. *Current Directions In Psychological Science, 15*(6), 322-325.

Stodt, B., Moll, R., Polzer, C., Pieschl, S., & Brand, M. (2013). *First results of a new questionnaire to assess Internet literacy: Correlations to pathological Internet use and risk-taking behavior*. Paper presented at the TeaP, Vienna.

Ugander, J., Karrer, B., Backstrom, L., & Marlow, C. (2011). The Anatomy of the Facebook Social Graph. *arXiv:1111.4503*, 1-17.

Valkenburg, P. M., & Peter, J. (2011). Online Communication Among Adolescents: An Integrated Model of Its Attraction, Opportunities, and Risks. *Journal of Adolescent Health 48*, 121-127.

Xu, H., Teo, H.-H., Tan, B. C. Y., & Agarwal, R. (2010). The Role of Push–Pull Technology in Privacy Calculus: The Case of Location-Based Services. *Journal of Management Information Systems, 26*(3), 135-173

Zeidner, R. (2007). How Deep Can You Probe. *HR Magazine, 52*(10), 57–60.