JOURNAL OF COMPUTER-MEDIATED COMMUNICATION

Journal of Computer-Mediated Communication

The 'Privacy Paradox' in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure[1]*

Monika Taddicken

Institute of Journalism and Communication Research, University of Hamburg, Grindelberg 7, 20144, Hamburg, Germany

Given the diffusion of the Social Web and increased disclosure of personal information online, the 'privacy paradox' suggests that while Internet users are concerned about privacy, their behaviors do not mirror those concerns. This study investigates the potential influence of privacy concerns, psychological traits, attitudes to the Social Web and age on self-disclosure. Using an online survey of a representative sample of German Internet users (n = 2, 739), the variety and quality of self-disclosure as well as access were measured. The findings indicate that privacy concerns hardly impact self-disclosure, but different variables moderate this relation. Perceived social relevance and the number of applications used proved important. Users' general willingness to disclose is most important when providing sensitive information.

Key words: Social Web, privacy, self-disclosure, path analysis, online survey

doi:10.1111/jcc4.12052

Introduction

The 'Social Web' has gained a great deal of popularity in recent years. The term refers to a number of different Internet applications, such as social networking sites (SNS), blogs, wikis, as well as picture and video sharing platforms. It is argued that these applications can be labeled the Social Web because their common objective is frequently social interaction (e.g. Ellison et al., 2007; Stefanone & Jang, 2008). The user-generated Social Web content prevalently consists of the users' opinions, experiences, and knowledge, but often also includes personal information such as names, contact information, and private photos. The online disclosed information is digitally stored and therefore persistent, replicable, scalable and searchable (Boyd, 2008) as well as shareable (Papacharissi & Gibson, 2011). By participating in the Social Web, users face the challenge of managing their online identity, while compromising their online privacy.

Previous research has shown that users are indeed concerned about their privacy within the Social Web, but do not apply these concerns to their usage behavior correspondingly (e.g. Acquisti & Gross, 2006; Boyd & Hargittai, 2010; Debatin et al., 2009; Tufekci, 2008; Yao et al., 2007; Youn & Hall, 2008). This is known as the 'privacy paradox' (Barnes, 2006). So far, however, this paradox has not been fully explained. A lack of problem or risk awareness as well as the users' lack of awareness of possibilities to

*Accepted by previous editor Maria Bakardjieva

protect their privacy is assumed to be a major reason (Acquisti & Gross, 2006; Boyd & Hargittai, 2010; Debatin et al., 2009; Tufekci, 2008). It is also supposed that users tend to underestimate the privacy dangers of self-disclosure.

Furthermore, individual differences among users typically impact privacy-related behavior, including online self-disclosure. Different aspects have been analyzed so far, such as gender (Cho, 2007; Fogel & Nehmad, 2009; Lewis et al., 2008; Thelwall, 2008; Tufekci, 2008; Yao et al., 2007; Yao & Zhang, 2008; Youn & Hall, 2008), cultural background (Bellman et al., 2004; Cong, 2007), level of activity (Lewis et al., 2008) and Internet experiences (Bellman et al., 2004; Yao et al., 2007; Yao & Zhang, 2008). However, much less is known about the impact of personality and one's perceived relevance of the Social Web. The sociability of Social Web applications has been highlighted as their main characteristic. Thus, it will be argued that the importance of the Social Web in the users' social contexts should be an influential factor for self-disclosure online.

The aim of this paper is to examine how much and what kind of personal information users disclose in the Social Web and which factors predict their levels of self-disclosure. Consequently, privacy concerns, the dispositional personal aspect of general willingness to self-disclose, and the perceived social importance of the Social Web are taken into account. In addition, the role of age, gender and the number of Social Web applications regularly used is examined. It is argued that it is necessary to differentiate between different forms of self-disclosure that are affected differently by various impact factors.

Self-Disclosure in the Social Web

Providing personal information in the Social Web can be considered self-disclosure, which includes "any message about the self that a person communicates to another" (Wheeless & Grotz, 1976, p. 338). Self-disclosure regularly occurs in a communication process concerning specific individuals (Cozby, 1973; Petronio, 2002; Wheeless, 1976). In general, self-disclosure is a precondition for any social relationship (Altman & Taylor, 1973; Laurenceau et al., 1998). The transmission of information about oneself or one's own thoughts and feelings is needed to produce social ties and is, at the same time, an element of almost any communication. As such, self-disclosure can vary in scope; in degree of intimacy or depth and value; of sincerity or precision; in tone; and in the degree of awareness (Altman & Taylor, 1973; Cozby, 1973; Jourard, 1971; Wheeless & Grotz, 1976). Self-disclosure is ordinarily the result of the consideration of risks and utility (Petronio, 2002). There is often tension between the desire to self-disclose on the one hand and the desire to protect privacy on the other.

Privacy can be defined as the right to self-determine which information is made accessible to whom and when (Westin, 1967) or as "selective control of access to the self" (Altman, 1975 p. 18). The degree of privacy that is pursued incorporates various aspects, which, from a psychological perspective, should be understood as protection against external influence on personal thoughts and attitudes. Among interactional viewpoints, the desire to control who collects and distributes information about the self is important. From this perspective, privacy should not be perceived as the maximum boundary to personal information for others, but rather as a dynamic process of negotiation between retreat and disclosure. An ideal degree of privacy is reached when the individual need for social interaction and self-disclosure is brought in line with the need for privacy. Therefore, the desired degree of privacy is in agreement with what has actually been achieved (Altman, 1975).

In offline contexts, the results of this negotiation process between self-disclosure and privacy depend on the specific communicative situation. On the Internet, by contrast, the basic conditions differ. The potential availability of the self-disclosed information over space and time is, in comparison with other

modes of communication, significantly greater on the Internet. The range of the content increases, and it potentially becomes available to a large number of scattered users. It is also available for a long time, given that Internet content – unlike verbal communication – is persistent and therefore permanently searchable. Additionally, the content is available in digital form, which enables and simplifies the combination of different information from various applications. Self-disclosed information on the Internet is therefore persistent, replicable, scalable, searchable and shareable (Boyd, 2008; Papacharissi & Gibson, 2011).

This leads to a problem of the *recontextualization of self-disclosure*. Self-disclosure on the Social Web frequently occurs to a heterogeneous audience consisting of different social relationships, for example, friends, family, and colleagues. This phenomenon is known as 'context collapse' (Marwick & Boyd, 2011). Additionally, for the self-discloser, it is often unclear who and how many persons are included among the audience due to spatial and temporal separation. The audience that is assumed or intended by the self-discloser may differ from the audience that is actually reached. Serious problems for the users might be the consequence: What was introduced in the context of close friends, for example, party pictures or opinions about sensitive topics, can become a problem in communication settings with other reference groups such as parents or employers. Moreover, it is possible for third parties to pass on personal information and, in doing so, transfer it into other contexts (e.g. by the operators of platforms for advertising purposes or by other users who copy and distribute the content). In this respect, self-disclosing behavior can produce unwanted consequences for Social Web users.

However, to put this problem into perspective, it is useful to know the actual extent of self-disclosure in the Social Web. Various research has been conducted so far; however, it primarily refers to particular applications, mostly to SNS. Most studies focus on the extent of self-disclosure as well as its accessibility. In doing so, the extent is generally operationalized through profile information queried in SNS. Thus, for instance, Acquisti and Gross (2006) indicate that 84% of their questioned Facebook users truthfully disclose their birthday, 75% their instant messenger name, whereas only 24% divulge their postal address. In Fogel and Nehmad's (2009) survey of Facebook and MySpace users, a total of 81.8% reported that they supply their real name, and 35.2% present their e-mail address. However, Fogel and Nehmad's respondents are more cautious with their postal address: Only 9.4% reveal this information. The percentage of instant messenger names is also considerably lower and accounts to 49.1%. Tufekci (2008) again reports other data, based on a survey of Facebook and MySpace users. Here, it becomes apparent that 94.9% of Facebook users include their real name in their profile, whereas only 62.7% of MySpace users do so Hence, different studies indicate different percentages of disclosure. This also applies to the question of accessibility of a profile. According to Fogel and Nehmad (2009), 73.6% of profiles are freely accessible to all other users. Tufekci (2008), however, distinguishes between Facebook users, 42.2% of whom have a freely accessible profile, and MySpace users, 59.0% of whom grant unrestricted access to their profile.

In addition to these studies on SNS, research has been conducted on self-disclosure in blogs. It indicates that personal experiences and private information make up the majority of blog content (Lenhart & Fox, 2006; Qian & Scott, 2007; Viegas, 2005). Altogether, a high willingness of blog authors to self-disclose is assumed (Harper & Harper, 2006; Herring et al., 2005).

Overall, the study findings reported above cannot be generalized to all self-disclosing behavior on the Social Web because of the different foci and wide variance of results. Moreover, student or convenience samples are used in many cases. For that reason, it is necessary to explore the users' self-disclosure in the Social Web on a more general level. Regarding the argument that all Social Web applications are based on the same principles of user-generated content and social interaction, it seems useful not to differentiate between every single Social Web application, like other studies have done.

Moreover, the different Social Web applications have converged. Many SNS, for example, offer not only the uploading of pictures, but also the possibility to write a blog and discuss with other users in chat boxes. Therefore, it is more helpful to differentiate between different forms of self-disclosure than between different Social Web applications.

The concept of self-disclosure is comprised of different levels and forms of revealing personal and sensitive information concerning conceptualizing self-disclosure. When discussing the Social Web, one has to differentiate between two distinct dimensions of self-disclosure: first, the quality of self-disclosed information or, as Jourard (1959) states, the depth and value of the revealed details. Information that can easily be found or that might be obvious, such as one's gender, age or hobbies, must not be treated the same as more intimate information such as private photos or one's feelings. However, how sensitive information is perceived is a highly subjective assessment and varies from person to person. Second, self-disclosure can happen with access to the public and consequently to unknown users or with access to only specific individuals who are friends or family. Especially in a SNS, this is a common distinction for users. Privacy settings often enable users to decide whether only befriended users, friends of friends or everyone can access the divulged information. Other Social Web applications also offer such a differentiation concerning the audience, although not as sophisticated, for example, by protecting one's uploaded pictures with a password or by providing one's blog address only to specific people by restricting the search via external search engines. In the current study, four different forms of self-disclosure were assessed along the two dimensions of quality and access: self-disclosure of personal facts, self-disclosure of sensitive information, self-disclosure with access to the public, and self-disclosure with access to specific groups.

Therefore, the first research aim is to describe the extent of self-disclosure in the entire Social Web regarding variety, quality, and access:

> RQ1: How much and what kind of personal information do users disclose to the public on the Social Web?

Self-Disclosure and Privacy Concerns

Since the concepts of privacy and self-disclosure are theoretically related (Altman, 1975; Petronio, 2002; Westin, 1967), it is to assume that users who are concerned about their online privacy will present no or only a few personal information on the Social Web. Previous empirical research confirms that Social Web users generally consider protection of their privacy to be important (Barnes, 2006; Debatin et al., 2009; Tufekci, 2008). Nonetheless, users rarely allow their privacy concerns to affect their online behavior (Acquisti & Gross, 2006; Boyd & Hargittai, 2010; Debatin et al., 2009; Tufekci, 2008; Yao et al., 2007; Yao & Zhang, 2008; Youn & Hall, 2008). Concern for the security of one's private information on the Web is not necessarily accompanied by a corresponding behavior, such as revealing less information (Debatin et al., 2009) or changing the privacy settings on a Social Web profile (Acquisti & Gross, 2006; Boyd & Hargittai, 2010; Tufekci, 2008). Different explanations for this are provided: a lack of problem or risk awareness (Boyd & Hargittai, 2010; Debatin et al., 2009) as well as a lack of knowledge about protection possibilities, such as changing the privacy settings (Debatin et al., 2009), or a lack of knowledge about what happens to the published information, given that data protection guidelines are often accepted without being read (Milne & Culnan, 2004).

From these findings, it has to be deduced that privacy concerns do not directly affect users' overall self-disclosing behavior. However, different forms of self-disclosure might be more affected by online privacy concerns than others. Users might not be concerned about privacy invasions when disclosing only within specific user groups such as friends. Therefore, it can be assumed that the level of personal

information that is revealed to the public without restrictions is more affected than the self-disclosure within specific peer groups.

H1: Online privacy concerns are negatively related to public self-disclosure on the Social Web.

Moreover, it can be presumed that one's privacy concerns affect one's self-disclosure through other factors, which refer to the social context and the usage itself.

Importance of Social Relevance

Self-disclosure is a common form of communicative behavior. The level of personal information one is disclosing depends on the communication partners as well as the specific communication situation. Therefore, a social-situational perspective on self-disclosure has to be taken into account. Lewis et al. (2008) analyzed various influences on privacy settings (SNS profile public or not) and deduced that they are influenced by, among other factors, friends' privacy settings. Jourard (1959) highlighted very early on the relevance of sociality for self-disclosing behavior by finding a so-called 'dyadic effect.' He suggested that people are more attracted to revealing personalities and have the tendency to match each other in exchanging discourses: "The dyadic effect suggests that disclosure proceeds on a quid pro quo basis – 'you tell me and I tell you'" (Jourard, 1971, p. 25f). In the context of the Social Web, Barak and Gluck-Ofri (2007) discovered that the reciprocity of self-disclosure was evident in discussion forums, yielding positive correlations between the measures of self-disclosure in messages and responses to them. Another study, using the explorative method of focus groups, indicates that individuals experience social pressure to participate in the Social Web when their social environment is using it, so that they do not feel socially excluded (Taddicken, 2012). Thus, one can assume that the social pressure to self-disclose is also applicable to the usage of the Social Web. Consequently, the assessment of the social environment appears to be particularly relevant for users. Hence, it can be assumed that Social Web users whose social environment assesses a specific Social Web application as important are also more likely to use and disclose within this. However, this perceived social relevance might become more important, the more users are concerned about their online privacy. Users with high online privacy concerns might prefer using and disclosing only within those Social Web applications that their friends and acquaintances use, whereas less concerned users do not rely heavily on the image an application has in the social context.

H2: Online privacy concerns are positively related to the importance of the social relevance of the Social Web.

In light of this, it can be further assumed that the more important the social relevance of the applications is, the more one will self-disclose. Thus, the perceived relevance of the Social Web in one's social environment has considerable influence on one's level of self-disclosure.

H3a: Importance of the social relevance of the Social Web is positively related to self-disclosure on the Social Web.

However, the perceived social relevance is assumed to be more important for the self-disclosure of sensitive information, such as thoughts and feelings, which are more intimate, than for the disclosure of factual information like names. Users who rely more on the assessment of their social environment

by using the Social Web might self-disclose more intimate information because they feel more socially bound to the Social Web. Therefore, the subjective importance of social relevance is expected to be more highly related to the self-disclosure of sensitive information than of personal facts.

H3b: Importance of the social relevance of the Social Web is more positively related to the self-disclosure of sensitive than factual information on the Social Web.

For the same reason, it can be assumed that users who perceive the social relevance of Social Web applications they are using disclose more information with open access than with restricted access. This might be especially true for the disclosure of factual information. Users who perceive the Social Web applications they are using as socially relevant are expected to be more willing to disclose personal facts to all other users of these applications.

H3c: Importance of the social relevance of the Social Web is more positively related to the self-disclosure of personal facts with open access than with restricted access on the Social Web.

Number of Social Web Applications Used

It has been argued that online privacy concerns might indirectly affect users' self-disclosure on the Social Web. The use of Social Web applications might be such a mediator. It can be presumed that users with high online privacy concerns use only selected Social Web applications, whereas users who are less concerned use and thus disclose personal data in a variety of Social Web applications. Less concerned users may think less carefully about using an application, since they are not as concerned about privacy invasions.

H4: Online privacy concerns are negatively related to the number of Social Web applications used.

Concerning self-disclosure, it can be assumed that the number of Social Web applications used is related to the amount of personal information disclosed. The variety of different applications asks for a variety of personal information. Users generally disclose other personal data in SNS than in discussion forums or blogs. Therefore, the level of self-disclosure can be expected to be higher the more different Social Web applications are used.

H5a: The number of Social Web applications used is positively related to self-disclosure on the Social Web.

That a variety of different applications asks for a variety of personal information is especially true for factual information. Therefore, it can be assumed that individuals using different forms of Social Web applications disclose particularly more factual information than users who concentrate on specific applications.

H5b: The number of Social Web applications used is more positively related to the self-disclosure of factual than sensitive information on the Social Web.

Moreover, it can be assumed that individuals using many different Social Web applications do this more often with restricted access because of their experience with different forms.

H5c: The number of Social Web application used is more positively related to self-disclosure with restricted access than open access on the Social Web.

General Willingness to Self-Disclose

Individual differences in general self-disclosure have often been assessed since Lewin (1948) started speculating about the differences in initial openness with strangers and intimacy between friends. A large number of studies have attempted to catalog individual and personality differences associated with high or intimate self-disclosures, such as age, race, and religion as well as mental health, impulsivity, and the need for approval (for an overview, see Archer, 1979). Findings of personality research on self-disclosure are inconsistent and present what Archer names an "incomplete portrait" (Archer, 1979, p. 37). Buss (2001) attempted to add to this field by developing a privacy questionnaire that includes the general willingness to self-disclose. The general willingness to let other people know something about oneself can be seen as a dispositional personal characteristic. Some people like others to know things about themselves, whereas others maintain a sharp psychological boundary between themselves and others and prefer to be self-contained. The general willingness to self-disclose can be considered a dispositional personality trait. Thus, one can assume that an individual's general willingness to self-disclose is one of the main predictors for his/her self-disclosure on the Social Web.

H6a: General willingness to self-disclose is positively related to self-disclosure on the Social Web.

Regarding the different forms of self-disclosure, one can assume that a higher general willingness to self-disclose has more of an impact on the disclosure of sensitive and intimate information.

H6b: General willingness to self-disclose is more positively related to the self-disclosure of sensitive than factual information on the Social Web.

At the same time, it can be presumed that more willing users disclose personal information more often publicly and less often with restricted access.

H6c: General willingness to self-disclose is more positively related to self-disclosure with open access than restricted access on the Social Web.

In addition, the general willingness to self-disclose should not only be related to self-disclosure, but also to privacy concerns. According to Altman (1975), one perceives an ideal degree of privacy when the individually desired level of self-disclosure meets the desired degree of privacy. A generally higher willingness to self-disclose should therefore be related to a lower need for privacy, and hence, to lower privacy concerns such as being concerned that too much personal information can be found online.

H7: General willingness to self-disclose is negatively related to online privacy concerns.

Age

Debatin et al. (2009) found evidence that usage of Facebook has become a fixed and habitual part of students' lives. This kind of routinization is also assumed for other Social Web applications. For this

age group, participation in the Social Web has become a matter of course. Current studies verify that young people in particular use the Social Web very intensively (Rideout et al., 2010). One can therefore assume that age is linked to the number of applications one uses.

H8: Age is negatively related to the number of Social Web applications used.

Furthermore, it can be assumed that age and self-disclosure are directly linked. In general, self-disclosure behavior was found to differ between younger and older individuals (Parker & Parrott, 1995). Moreover, individuals who use the Social Web more intensively are to expect to reveal more personal information. Regarding young and adolescent users, self-disclosure on the Social Web additionally enables the practice of self and social examination, which are important adolescent development exercises. Peter and Valkenburg (2011) argue that the Social Web offers young users excellent possibilities to achieve development goals and pertinent skills, such as learning how to adjust their self-presentation according to the responses of others. Therefore, the Social Web is an ideal environment for building and managing identity processes. Thus, adolescents seem to be even more attracted to self-disclosure in the Social Web than adults. It is suspected that primarily young users show a high degree of self-disclosure on the Social Web, which might be especially true for the self-disclosure of sensitive information.

H9a: Age is negatively related to self-disclosure on the Social Web.

H9b: Age is more negatively related to the self-disclosure of sensitive information than factual information on the Social Web.

Furthermore, it is often argued that young users in particular disclose more incautiously because they are used to the process of revealing personal information (Hinduja & Patchin, 2008; Lenhart et al., 2007; Peter & Valkenburg, 2011; Rideout et al., 2010).

H9c: Age is more negatively related to self-disclosure with open access than restricted access on the Social Web.

Finally, age and privacy concerns can be assumed to be related. Livingstone (2008) has shown that teenage SNS users are not at all unconcerned about privacy risks online; rather, they have a different notion of privacy. Adolescent SNS users do not consider standard SNS information such as age, relationship status, or sexual orientation to be private information. This seems to contradict the notion of older users. Therefore, it can be expected that younger users may also vary in what they consider a violation of their privacy (Peter & Valkenburg, 2011), especially in an online environment (Yao et al., 2007).

H10: Age is negatively related to online privacy concerns.

Gender

In self-disclosure research, women were found to be generally more willing to reveal personal information and more often than men (Parker & Parrott, 1995). This is particularly true for self-disclosures concerning known persons (Dindia & Allen, 1992) as well as information regarding intimate information such as feelings (Derlega et al., 1981; Morgan, 1976). For the Social Web

context, Tufekci (2008) found gender differences in terms of self-disclosure in SNS profiles. Women were shown to be more likely to disclose their favorite books, favorite music and their religion, but rarely their phone number. Furthermore, women were found to more often have a private SNS profile (Lewis et al., 2008; Thelwall, 2008). They also seem to be more cautious about to whom they grant access to their profile information (Fogel & Nehmad, 2009). Moreover, it was found that women are more sensible about privacy issues than men (Cho & Hung, 2011). Females seem to be more self-regulated to protect personal information privacy and privacy risk-averse (Jianakoplos & Bernasek, 1998). Conversely, Barak and Gluck-Ofri (2007) found only minor gender differences in discussion forums. Cho (2007) did not even find any significant differences in self-disclosure concerning gender in online chats. It remains unclear whether gender differences exist regarding the relationships between privacy concerns and self-disclosing behavior on the Social Web. Thus, the following research question is investigated:

RQ2: To what extent do the proposed hypotheses hold for male and female users?

Model

To test the proposed hypotheses, path models that simultaneously consider self-disclosure, privacy concerns, general willingness, importance of social relevance as well as the number of different applications used, and age will be calculated. Using the analysis of a path model, it is possible to compare the relative importance of each predictor to the dependent variable, self-disclosure. Although privacy concerns and self-disclosure are assumed to be unrelated, the path will be tested to enlighten possible changes regarding different forms of self-disclosure. Figure 1 presents the structural model to be tested in this study.[2] To consider the different forms of self-disclosure, four additional path models using different indices along the two dimensions of quality and access are calculated.

Method

Participants

In order to assess the value of the proposed model, a Web survey was implemented through an online access panel. To obtain a representative Internet sample, the participants were recruited based on age, gender, and German state (see Table 1). Altogether, a survey with n = 3, 030 was conducted. A total of 9.6% of the respondents (291 cases) did not use any Social Web applications and were therefore excluded from the data analysis, so that the final sample size was n = 2, 739.

Measures[3]

Self-Disclosure on the Social Web

First, Social Web use was assessed via six different applications: blogs, SNS, wikis, discussion forums, and picture and video sharing platforms. Thereafter, the participants were asked what kind of personal information they have disclosed within these applications. Following Barak and Gluck-Ofri (2007), self-disclosure is divided into factual personal information, thoughts, and feelings. The factual information category is divided into different information typically provided when participating in the Social Web (first and last name, birth date, profession, email and mailing address as well as photos). Two additional categories were inductively integrated based on previously implemented exploratory focus groups:

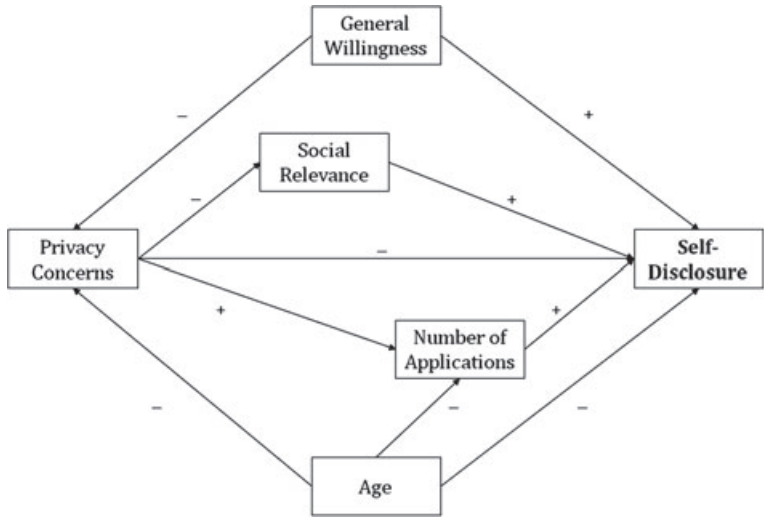

Figure 1 Proposed path model predicting user's self-disclosure on the Social Web

Table 1 Description of the Sample

	Survey	German Internet Users*
Gender		
Male	54.2%	54.5%
Female	45.8%	45.5%
Age Group		
13–19 years	10.2%	12.0%
20–29 years	20.5%	19.3%
30–39 years	20.3%	20.2%
40–49 years	23.2%	22.8%
50–59 years	14.8%	14.5%
60 years and older	11.1%	11.1%
Education		
No certificate or certificate of secondary education	12.9%	32.4%
Intermediate-level education	32.5%	38.5%
University entrance level	48.7%	29.1%

*According to AGOF (2008). Internet facts – Berichtsband zur Internet facts 2008-IV. [Internet facts – report of internet facts 2008-IV]. http://www.agof.de/internetfacts (June 6th, 2011).

The category 'description of personal experience' was added because it was reported as particularly important for Social Web use. Also added was the category 'disclosure of concerns and fears' for the specification of the feelings category, since it indicates a particularly high level of vulnerability for users. Regarding the question of accessibility of information, participants were asked for each information item provided, whether they made it available for general access and/or accessible only to specific groups.

Table 2 Statistical Values of Measures

	N	M	SD	Min.	Max.	Skew	Reliability*	No. of Items
Self-disclosure	2739	7.37	2.61	0	11	−.56	.82	11
General willingness to self-disclose	2699	2.77	.64	1	5	.15	.66	6
Online privacy concerns	2739	3.37	.72	1	5	.16	.92	17
Importance of social relevance	2721	3.25	.87	1	5	−.14	.60	2
Number of Social Web applications used	2739	2.93	1.97	0	6	−.09	–	–
Age	2739	38.10	14.45	13	83	.31	–	–

*Calculated with Cronbach's alpha.

General Willingness to Self-Disclose

To measure the participants' general willingness to self-disclose, a scale developed by Buss (2001) was used in this study. This scale consists of items that center on not divulging information about oneself. People who endorse these items prefer to be self-contained and to protect both their private and public self. For the German survey, the English language scale was translated into German by two translators, who worked independently from another.

Online Privacy Concerns

To determine privacy concerns in the Internet, the attitude dimension of the ''Adapted Scale for Online Privacy Concern and Protection'' (APCP) by Taddicken (2010) was used. This scale is based on the ''Online Privacy Concern and Protection'' (PCP) scale created by Buchanan et al. (2007). It has been developed for online use and consists of attitudinal items about online privacy. It is not used to measure the separate indices or factors of all theoretically delineated aspects of privacy, but rather to indicate the general concept of privacy concerns (Westin, 1967). The scale includes items of being concerned that others can find too much personal information online as well as concerns about identity problems that may arise online.

Importance of Social Relevance

In order to analyze the social relevance of the Social Web, two ad-hoc items were formulated. They determine how important it is for users that a Social Web application is publicly known and recommended by friends and acquaintances. Hence, they measure the importance users place on the relevance of their social environment of the Social Web.

Number of Social Web Applications Used

Participants were asked whether and how often they use six different Social Web applications (1-never to 7-a few times a day). For the number of Social Web applications one uses, it was counted how many different Social Web applications were used at least 'a few times per month.' Hence, applications that were once tried but not further used were excluded.

All scales were summed to single scores. The statistical values of the measured scales are displayed in Table 2.

Table 3 Self-Disclosure Factor Loadings

	Factor 1: Sensitive information	Factor 2: Factual information
Last Name		.80
Birth Date		.77
Profession		.52
Postal Address		.64
Photos	.57	
Experiences	.81	
Thoughts	.83	
Feelings	.85	
Concerns and Fears	.79	

Eigenvalue > 1, unrotated; Total variance extracted = 65.3%; Factor loadings > .5 are shown.
Note: The instructions accompanying the scale were "Below, we would like to know what personal information you have, at least once, made available for using applications in the Social Web. Only correct information should be included (e.g. your correct first name, no nicknames). Please check which information you have 'Never,' 'Only Once,' or 'More Frequently' revealed." Participants responded using a 3-point scale for each item (*1* = "*never*", *2* = "*only once*", *3* = "*more frequently*").

Results

Extent of Self-Disclosure (RQ1)

First, in order to obtain an overview on how much and what kind of personal information the participants had disclosed in the Social Web, an exploratory factor analysis was calculated for the self-disclosure items (Table 3). For this procedure, the basic information of first name and e-mail address were omitted because these details are normally needed when registering for every Social Web application. Then, two factors were identified: Factor 1 reflects sensitive information (37.4% variance explained), and factor 2 identifies fact-based personal information (30.0% variance explained). Cronbach's alpha for both factors is adequate (f1: $\alpha = 0.86$, f2: $\alpha = 0.77$).

The percentage of users who have disclosed the basic information of first name and email address on the Social Web is very high. Only 7.0 to 11.9 percent have never disclosed these details on the Social Web. First names are frequently identified as generally accessible on the Social Web. E-mail addresses, by contrast, are only made freely accessible in the Internet by one in every five users (23.0%).

Factual information, including last name, birth date, profession, and mailing address, are, with the exception of mailing address, provided by three-quarters of the users. Last name, birth date, and profession are made freely accessible by almost one in four who have provided this information on the Social Web. The mailing address is considerably less frequently disclosed as a contact option. A total of 54.6% state that they have published this information on the Social Web at least once (more frequently: 20.5%). However, only approximately one in every ten has provided these details without additional access restrictions. Therefore, this amounts to a greater reservation than found with other personal information.

Content that may be considered highly private, specifically the categories of photos, personal experiences, thoughts, feelings, and fears and concerns, is considered sensitive information. This information is disclosed significantly less frequently. Nonetheless, a surprisingly high number of users have disclosed this very private information on the Social Web. 67.5% of users provide photos on

Table 4 Self-Disclosure on the Social Web

	Self-Disclosure on the Social Web*				Self-Disclosure on the Social Web by Accessibility†	
	N	More Frequently	Once	Never	N‡	Open Access§	Restricted Access§
Basic Information							
First Name	2739	72.0%	21.1%	7.0%	2548 (2739)	56.6% (52.6%)	46.4% (43.2%)
E-mail Address	2739	59.4%	28.7%	11.9%	2413 (2739)	23.0% (20.3%)	78.6% (69.3%)
Factual Information							
Last Name	2739	54.7%	30.0%	15.3%	2320 (2739)	38.5% (32.6%)	63.0% (53.4%)
Birth Date	2739	59.8%	28.9%	11.3%	2429 (2739)	37.8% (33.5%)	63.5% (56.3%)
Profession	2739	38.3%	38.3%	23.5%	2096 (2739)	37.8% (29.0%)	63.1% (48.3%)
Postal Address	2739	20.5%	31.4%	45.3%	1497 (2739)	9.7% (5.3%)	88.6% (48.4%)
Sensitive Information							
Photos	2739	31.7%	35.8%	32.5%	1848 (2739)	45.0% (30.4%)	58.5% (39.5%)
Experiences	2739	20.4%	32.0%	47.5%	1437 (2739)	32.8% (17.2%)	68.6% (36.0%)
Thoughts	2739	23.4%	31.3%	45.3%	1498 (2739)	32.6% (17.8%)	68.6% (37.5%)
Feelings	2739	17.8%	24.4%	57.8%	1155 (2739)	30.1% (12.7%)	70.1% (29.6%)
Concerns and Fears	2739	13.1%	21.3%	65.6%	942 (2739)	30.5% (10.5%)	69.3% (23.8%)

*"Below, we would like to know what personal information you have, at least once, made available for using applications in the Social Web. Only correct information should be included (e.g. your correct first name, no nicknames). Please check which information you have 'Never,' 'Only Once,' or 'More Frequently' revealed."

†"You have revealed the following personal information at least once on the Social Web. Was this generally accessible or only accessible to a certain group? (Multiple answers are possible.)" This question was only asked for information that has been revealed at least once.

‡The number of users who have revealed these different types of information at least once varies; therefore, the sample sizes for each information item differ.

§The percentages in brackets refer to the whole sample.

the Social Web, 45.0% without additional access restrictions. Approximately half of the users have described experiences on the Social Web (more frequently: 20.4%) or expressed their own thoughts (more frequently: 23.4%). Approximately every fourth user has described his or her feelings at least once, and one in every three has even described his or her concerns and fears on the Social Web (more frequently: 17.8% and 13.1%). It is particularly noteworthy that 30% of these expressions were disclosed on the Social Web without access restrictions. Among all Social Web users, every sixth has shared his/her experiences and thoughts, every eighth his/her feelings, and every tenth his/her concerns and fears with the public of Social Web users (for more information see Table 4).

Hypotheses H1 to H14

In order to test the hypotheses on the different forms of self-disclosure, the self-disclosure information was compiled into a single index value. Therefore, the categories were dichotomized (1 = disclosed, 0 = not disclosed). In this respect, the index 'SD in total' shows the number of different categories in which a user has disclosed information about him-/herself on the Social Web at least once. To consider the different forms of self-disclosure, additional indices along the two dimensions of quality

Table 5 Statistical Values of Self-Disclosure Indices

	N	M	SD	Min.	Max.	Skew	Reliability*	No. of Items
Self-disclosure of factual information with open access (SD facts open)	2739	1.00	1.21	.00	4.00	.88	.70	4
Self-disclosure of factual information with restricted access (SD facts restricted)	2739	2.06	1.40	.00	4.00	−.06	.66	4
Self-disclosure of sensitive information with open access (SD sensitive restricted)	2739	.89	1.46	.00	5.00	1.72	.84	5
Self-disclosure of sensitive information with restricted access (SD sensitive restricted)	2739	1.66	1.75	.00	5.00	.69	.81	5

*Calculated with Cronbach's alpha.

and access were calculated. It was counted how much factual and sensitive information was disclosed by users to the public (open access) and only to specific groups such as befriended users (restricted access). Four different indices were calculated: 'self-disclosure of factual information with open access (SD facts open),' 'self-disclosure of factual information with restricted access (SD facts restricted),' 'self-disclosure of sensitive information with open access (SD sensitive open)' and 'self-disclosure of sensitive information with restricted access (SD sensitive restricted).' The statistical values for these indices can be found in Table 5. It has to be noted that the distribution of 'SD sensitive open' has a strong positive skew: only a few users make sensitive personal information generally accessible ($M = 0.89$ of 5).

An examination of the correlations between self-disclosure indices (Table 6) reveals that the indices cover different dimensions. Hence, most notably, the disclosure of personal facts to the public ('SD facts open') is highly negatively correlated with its disclosure to specific groups of users ('SD facts restricted') ($r = -0.56$, $p = 0.000$). Users seem to disclose factual information either to everyone or to a restricted audience. This implies that users do not actually follow an elaborate system of self-disclosure of personal facts, such as disclosing information to the public in one application, for example, in a SNS, and only to a specific audience in other applications such as blogs or video platforms. The same applies for the disclosure of sensitive information, although the correlation is much lower ($r = -0.26$, $p = 0.000$). This underscores that users decide on a basic strategy for self-disclosure (generally accessible or not) rather than making some information generally accessible (e.g. general thoughts, innocuous experiences) and other content only accessible to certain groups (e.g. opinions related to specific topics, private pictures). Moreover, it is interesting that the indices 'SD facts open' and 'SD sensitive open' report a rather high positive correlation ($r = 0.31$, $p = 0.000$). Users who disclose many personal facts to the public also tend to disclose more sensitive personal information to the public.

The proposed path models were calculated using AMOS Graphics 17. All measures were implemented as sum scores. The global fit values indicate a good fit to each of the data sets (Table 7).

Table 6 Correlations Between Self-Disclosure Indices

	SD in total	SD facts open	SD facts restricted	SD sensitive open	SD sensitive restricted
SD in total	1				
SD facts open	.30***	1			
SD facts restricted	.31***	−.56***	1		
SD sensitive open	.39***	.31***	−.19***	1	
SD sensitive restricted	.59***	−.03***	.18***	−.26***	1

Calculation according to Pearson;
***p = .000; **p ≤ .01, *p ≤ .05

Table 7 Global Fit Measures of Path Models 1-5

Model No.	Dependent variables	Chi^2(df)	p	Chi^2/df	NFI	CFI	RMSEA
1	SD in total	5.070(5)	.407	1.014	.995	1.000	.002
2	SD facts open	5.106(5)	.403	1.021	.993	1.000	.003
3	SD facts restricted	5.162(5)	.396	1.032	.991	1.000	.003
4	SD sensitive open	5.100(5)	.404	1.020	.993	1.000	.003
5	SD sensitive restricted	5.104(5)	.403	1.021	.993	1.000	.003

Figure 2 depicts the path model with the calculated path coefficients for the total self-disclosure (path model No. 1). Standardized path coefficients for the self-disclosure indices in models 1 to 5 are presented in Table 8.

Privacy Concerns (H1)

Given that previous research has shown no direct effects of privacy concerns on self-disclosure online, it is expected that privacy concerns would have no direct effect on the user's overall level of self-disclosure. However, it was assumed that this might differ for self-disclosure to the public (H1). The calculated path coefficients of privacy concerns to the self-disclosure indices are very small and not significant. However, it can be presumed that one's privacy concerns affect one's self-disclosing behavior through other factors such as social relevance.

Importance of Social Relevance (H2, H3a-c)

It was argued that the more participants are concerned about online privacy, the more important is the social relevance of Social Web applications (H2). Furthermore, it was assumed that the more important the social relevance is perceived, the more personal information is disclosed on the Social Web (H3a). The results confirm both hypotheses. The coefficient of the path privacy concerns to social relevance ($\beta_{\text{sr-pc}} = 0.22$, $p = 0.000$), as well as the coefficient of the path social relevance to overall self-disclosure ($\beta_{\text{sdtotal-sr}} = 0.27$, $p = 0.000$), are both statistically significant.

Regarding the different forms of self-disclosure, it was assumed that the disclosure of sensitive information is generally more affected by the users' perceived importance of social relevance than of facts (H3b). This is only confirmed for the restricted disclosure, as the public publishing of sensitive

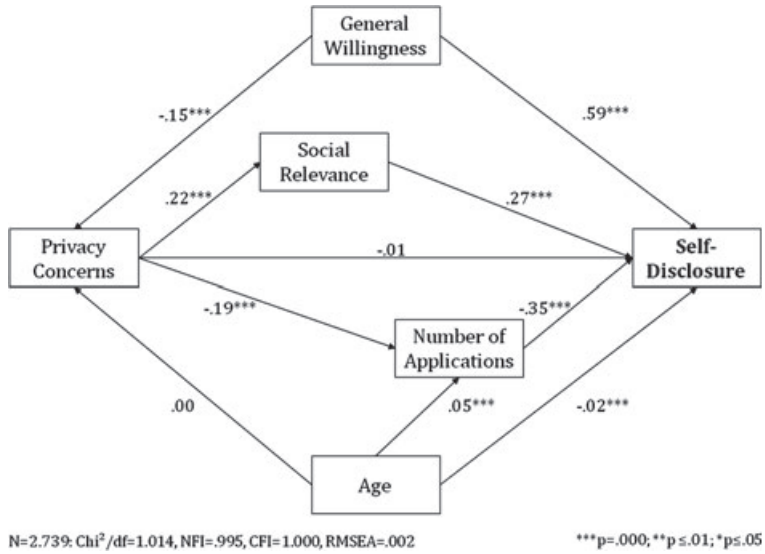

Figure 2 Calculated path model predicting user's overall self-disclosure

Table 8 Path Coefficients of Self-Disclosure Indices

Model No.	Dependent Variables	Independent Variables: Privacy Concerns	Social Relevance	Number of Apps	General Willingness	Age
1	SD in total	−.01	.27***	−.35***	.59***	−.02***
2	SD facts open	−.08	.09***	−.03**	.15***	−.02***
3	SD facts restricted	.04	.00	−.01	.05	.01***
4	SD sensitive open	−.02	−.00	−.14***	.13**	−.01**
5	SD sensitive restricted	.05	.16***	−.15***	.26***	−.01***

***p = .000; **p ≤ .01; *p ≤ .05

information is not related to the importance of social relevance. Thus, Social Web users tend to self-disclose more sensitive information when their friends and acquaintances also use it, but only within this group. This highlights the impact of the social environment on usage and self-disclosure behavior.

Hypothesis H3c, which assumes the perceived social relevance of the Social Web more important for disclosing personal facts publicly than with restricted access, is confirmed. Users who find the social relevance of the applications they are using important disclose personal facts more often with open access. They might expect it to be more beneficial to be found by other users within these applications because of their assumed high relevance within their peer group.

Number of Social Web Applications Used (H4, H5a-c)

Another indirect effect of privacy concerns was assumed through the number of different Social Web applications used regularly. The online privacy concerns were assumed to negatively affect this number

(H4), whereas the number of applications positively influences the level of self-disclosure (H5a). Concerning the relationship between privacy concerns and the number of applications, the hypothesis can be accepted. This path shows a significant negative coefficient ($\beta_{\text{na-pc}} = -0.19$, $p = 0.000$). People who are concerned about their online privacy tend to use fewer Social Web applications. However, regarding the hypothesized effect of the number of applications used on self-disclosure, the calculated path model shows a high negative path coefficient ($\beta_{\text{sdtotal-na}} = -0.35$, $p = 0.000$). This result is contrary to the proposed hypothesis (H5b rejected). Individuals who only use a few different Social Web applications tend to reveal more personal information. Users seem to focus on specific applications and stay within these.

Furthermore, this assumption is supported by the finding that the disclosure of sensitive information in particular – either restricted or open – is higher negatively related to the number of applications used than the disclosure of personal facts. People who use only a small number of different Social Web applications disclose a lot of sensitive information on the Social Web. Conversely, the disclosure of factual information is hardly related to the number of applications.

Hypothesis H5c must also be rejected. The path coefficients of self-disclosure with open and restricted access are similar. Thus, users seem to concentrate their self-disclosing behavior on specific Social Web applications. This might be explained with users' strong focus on communication with friends and family. It was found that e.g. SNS are more often used for maintaining social relationships than for finding new contacts (Boyd & Ellison, 2007; Ellison et al., 2007). If users wish to communicate and maintain contact with close friends and family, it is not necessary for them to use manyfold applications, particularly when users know that their comments will be addressed on a daily basis (Ellison et al., 2007, 2011; Haythornthwaite, 2005).

General Willingness to Self-Disclose (H6a-c, H7)

The results indicate a high and statistically significant positive correlation between one's general willingness to self-disclose and actual self-disclosure in the Social Web. The coefficients for these paths are among the highest in every model, and they indicate a strong positive effect of the dispositional personality trait of general willingness on self-disclosing behavior, independent of any privacy concerns ($\beta_{\text{sdtotal-gw}} = 0.59$, $p = 0.000$) (H6a confirmed).

However, the level of direct influence of the dispositional general willingness to self-disclose differs depending on the self-disclosure index. It was assumed that a higher willingness would lead to higher levels of self-disclosure of sensitive information (H6b) and with public access (H6c). It was found that the index 'SD sensitive restricted' is the highest positively correlated with general willingness ($\beta_{\text{sdsensrest-gw}} = 0.26$, $p = 0.000$), whereas 'SD facts restricted' and general willingness are not significantly correlated ($\beta_{\text{sdfactsrest-gw}} = 0.05$, $p = 0.255$) (H6b confirmed). The disclosure of personal facts to the public is more positively related to general willingness ($\beta_{\text{sdfactsopen-gw}} = 0.15$, $p = 0.000$). Users who do not want others to know things about them nevertheless disclose factual information such as last name and profession on the Social Web, but with restricted access. However, hypothesis H6c is not fully confirmed because the correlation of the disclosure of sensitive information with general willingness is higher for 'SD sensitive restricted' than for 'SD sensitive open' ($\beta_{\text{sdsensopen-gw}} = 0.13$, $p = 0.002$). Users who are generally more willing to let others know something about them nevertheless prefer restricted disclosure on the Social Web. From this, it can be deduced that even individuals who do not care very much about who knows what and how much about them prefer to reveal this information within a specific community.

Concerning the relationship between general willingness and online privacy concerns, a negative impact of general willingness was assumed (H7). This hypothesis is also accepted. The path coefficient

proves a negative correlation, but only on a small level ($\beta_{\text{pc-gw}} = -0.15$, $p = 0.000$). Social Web users who are generally more willing to self-disclose are slightly less concerned about their online privacy.

Age (H8, H9a-c, H10)

Age was hypothesized to have an impact on self-disclosure, both directly (H9a-c) and indirectly through the number of applications used (H8). However, all path coefficients of age are – although significant – only small. Thus, age has hardly any effect on self-disclosure. It is nevertheless interesting that age and number of applications used is positively correlated. Younger users do not use significantly more different Social Web applications, even though they have grown up with these. In addition, they only marginally disclose more personal information. It is often discussed whether young users are particularly affected by the risk of privacy abuses, since they might self-disclose the most. Findings here show that this is only marginally the case.

Regarding the impact of age on privacy concerns (H10), the result shows that age does not affect the level of online privacy concerns in a linear way.

Gender (RQ2)

To investigate research question RQ2 on gender differences, it is tested whether the models held for male and female users. A multiple-group analysis was performed for each model. For this, the full specified models 1–5 were used to check unconstrained models (all path coefficients are freely estimated) against metric measurement invariance, where all path coefficients were set as equal in the two submodels (male and female users). Table 9 reports the each of the model fit statistics for an unconstrained model as well as a model with imposed cross-group constraints. The Chi^2-difference test for nested models shows that the constraints led to a significant Chi^2-change (Chi^2_{change} $(10, n = 2,739) = 22.335$, $p = 0.013$) for self-disclosure in total (model 1), which means that the cross-gender constraints decreased the global fit. Further Chi^2-difference tests expose the main gender difference for the self-disclosure of sensitive information with open access (Chi^2_{change} $(10, n = 2,739) = 27.974$, $p = 0.002$). Separate analyses of each structural weight proved significant Chi^2-changes for constraining the following paths: privacy concerns, general willingness, social relevance, and age on self-disclosure of sensitive information with open access. This suggests gender differences regarding the impact of these variables. The path coefficients of the unconstrained model 4 show that the female users' self-disclosure is more affected by their online privacy concerns and their general willingness to self-disclose. The impact of social relevance and age – although significantly different between male and female users – was shown as only very minor overall (H5b,c and H9b,c were rejected). No gender differences were found regarding the self-disclosure of sensitive information with restricted access and of factual information, either with open or restricted access.

Discussion

The present study was conducted to examine how much personal information Social Web users disclose and how this is affected by privacy concerns, the dispositional personality trait of general willingness to self-disclose, social relevance, as well as by age and the number of applications used.

The first part of the findings regarding the extent of self-disclosure on the Social Web revealed that it is necessary to differentiate between different forms of personal information. It was found that a majority of users disclose personal facts. Factual information, such as names and profession, is obligatory in many Social Web applications. Based on this study, users tend to provide honest and valid information. Fewer users disclose factual information, which cannot be considered standard Social Web information, and if so, often with restricted access. Furthermore, it was found that sensitive information

Table 9 Multiple-Group Analyses Between Male and Female Users for Models 1-5

Model	Chi^2	df	p
1) SD in total			
unconstrained	14.009	10	.173
constrained	36.344	20	.014
Change	*22.335*	*10*	***.013***
2) SD facts open			
unconstrained	13.958	10	.175
constrained	22.631	20	.307
Change	*8.673*	*10*	***.563***
3) SD facts restricted			
unconstrained	13.956	10	.175
constrained	31.098	20	.054
Change	*17.142*	*10*	***.071***
4) SD sensitive open			
unconstrained	13.914	10	.177
constrained	41.888	20	.003
Change	*27.974*	*10*	***.002***
5) SD sensitive restricted			
unconstrained	14.027	10	.172
constrained	23.268	20	.276
Change	*9.241*	*10*	***.509***

is disclosed by considerably fewer users. Nevertheless, it has to be noted that approximately two-thirds of the participants distributed photos, which were publicly accessible. About half of them disclosed experiences, thoughts and feelings on the Social Web at least once. When taking into account that this was done with open access in every third case, these numbers can be considered proof of extensive self-disclosure on the Social Web.

However, this study did not assess whether the disclosed information was related to the users' real names or for what purposes they provided it. Therefore, it is not possible to assess the potential risk of privacy invasion or of the discussed recontextualization of the self-disclosed information.

The calculated path models allowed simultaneous analyses of the formulated hypotheses, also concerning different forms of self-disclosure. One of the relationships on which this study focuses is the impact of online privacy concerns on self-disclosing behavior. Many previous studies have failed to directly relate users' privacy concerns to their self-disclosure in the Social Web. That is why the notion of a 'privacy paradox' (Barnes, 2006) was invented. Several explanations were suggested for this paradox, mainly concerning a lack of awareness and literacy. In this paper, it was tested whether an effect of online privacy concerns could be found when differentiating self-disclosing behavior. Although no significant direct effect has been found, the results show that it might be useful for future studies to distinguish between public self-disclosure and self-disclosing behavior with clearly defined communities where users feel safe from privacy invasion. Furthermore, these different forms of self-disclosure could be related to the different dimensions of privacy concerns. For example, it could be interesting to

differentiate between the fear of identity theft or fraud and the fear of privacy invasion from known people, for example, the concern that a boss or colleague might see private information they should not.

However, in this paper, a moderating influence of other situational, social and interactional variables is confirmed. Taking into account the influence of peers and perceived social relevance, participants in this study rated the social relevance of social media. Here it was found that the higher the people rate the social relevance of the Social Web as important, and the more they focus on the use of specific Social Web applications, the more information they disclose. Social Web users tend to self-disclose more personal and sensitive information when their friends and acquaintances also use it. This highlights the impact of the social environment on usage and self-disclosure behavior in social media. This finding also confirms previous research that found the dyadic effect of reciprocity to be an important impetus to self-disclosure (Barak & Gluck-Ofri, 2007). A social norm or perceived pressure to reciprocate by revealing personal details within the Social Web seems to exist and to affect the users' self-disclosing behaviors, in particular in applications their social peer groups are also using. Additionally, users have been found trying to construct a certain popularity status within an application through the publishing of private information (Christofides et al., 2009). It is confirmed here that users tend to stay within only a few applications that are relevant for their social environment, and that within these Social Web applications, they disclose a variety of personal information.

This study revealed that the number of applications used and the level of self-disclosure are significantly negatively related. Users who utilize fewer applications disclose more personal information, especially more sensitive information. Against the background of a large body of research that has proven the usefulness of SNS for not only building, but also maintaining social relationships (Boyd & Ellison, 2007; Ellison et al., 2007), this finding leads to the assumption that not only SNS, but also other Social Web applications are particularly beneficial for bonding social capital.

In this paper, the personality trait of general willingness to self-disclose was expected to affect self-disclosing behavior the most. The results proved this assumption to be true. Users who are generally willing to disclose a lot of personal information disclose the most on the Social Web. Those who prefer to stay self-contained actually reveal less. This finding indicates that users resist the invitation of the Social Web to disclose a lot of personal information if they are not generally willing to share personal and sensitive information. Regarding the public disclosure of personal facts, the impact of general willingness is hardly existent. Users who do not want others to know things about them nevertheless disclose factual information such as last name and profession on the Social Web, but they do not reveal this information to the public.

Furthermore, the results showed only a minor influence of general willingness on privacy concerns. From a theoretical viewpoint, it can be argued that these concepts are closely related. But the measurement of direct linear effects neglects situational, social and interactional variables. One has to assume that this correlation is much more complex.

Findings on age can be highlighted, since a representative sample of Internet users with an age range of between 13 and 83 years was used, unlike in various other studies in which a sample of college students was employed. Here, age was hardly found to have an impact on the level of self-disclosure. This is interesting, since younger users are often suspected to be more generous with their personal information and less concerned about their privacy. However, this study found no impact of age on online privacy concerns. Other age effects concerning the number of applications used and the level of self-disclosure are only very minor. These

Finally, gender was proven to influence the relation of privacy concerns and general willingness to self-disclose, with higher correlations for female users. However, these gender differences only exist regarding the disclosure of sensitive information with access to the public.

One of the main limitations of this study is the recruitment via an online access panel. Members of online access panels participate more often in Web surveys than other Internet users and thus might be more skilled Internet users. In addition, they may be more willing to reveal personal information than other individuals. However, there is no persuasively obvious reason for a differing structure of attitudes or behavioral tendencies between this and other groups of participants.

The reliability of self-reported information is another important limitation of this study. The effects of social desirability may have affected the measurement of online privacy concerns and of self-disclosure. Then again, unlike prior research, the current study examined previous disclosure and not intended disclosure behavior (Joinson et al., 2010).

For future research, it seems worthwhile to analyze the influence of other mediating factors of the users' social environment. It has been shown that the importance of social relevance, as well as the number of Social Web applications one regularly uses, are important influencing factors and moderators in the negotiation process of privacy and self-disclosure. Moreover, social factors have been highlighted as important.

Furthermore, it was shown that it is necessary to distinguish between different forms of self-disclosure. In this paper, the dimensions of quality and access were taken into account. The next step could be to consider the degree of intimacy, the sincerity and the accuracy in each disclosure category. Finally, it would be interesting to research the level of awareness, since the interactional perspective has proven to be an important factor for online self-disclosure. This may indicate that self-disclosure on the Social Web is less the result of conscious impression management, and more the consequence of social interaction processes that have moved online.

For regulators, it is important to understand that the usage of social media is socially driven. Although the personality of users proved to be important for their self-disclosing behavior, even fewer outgoing people tend to disclose factual information online. Users seem to feel safe within socially relevant applications. Much information was disclosed with restricted access. However, the thread of possible recontextualization of the disclosed information is existent, even when individuals are communicating 'only' with befriended users. First, it is important for users to know exactly who their audience is. In a SNS, for example, this might be implemented quite easily. Second, it is necessary to highlight that even if personal details are revealed online 'only' to known people, it is still possible for the information to be passed on and then transferred into other contexts.

Finally, it should be taken into account that adolescents and younger users are not the only ones who face privacy risks by self-disclosing personal information on the Social Web. Older users who have not grown up with the Internet revealed a similar level of self-disclosure online and should therefore also be informed and educated about online privacy in social media.

Notes

1 This research was supported by the German Research Foundation (Deutsche ForschungsGemeinschaft, DFG) and conducted at the University of Hohenheim, Germany, Professor Michael Schenk.

2 The path analyses are calculated with single index values of the measured scales. Variables are therefore represented as observed variables in the graphics.

3 Items can be found here. The original German wording of the items can be provided by the author on request.

References

Acquisti, A., & Gross, R. (2006, June). *Awareness, information sharing, and privacy on the Facebook*. Paper presented at the 6th "Privacy Enhancing Technologies," workshop Cambridge, England.

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

Altman, I., & Taylor, D. A. (1973). *Social penetration: The development of interpersonal relationships*. New York: Holt, Rinehart, & Winston.

Archer, R. L. (1979). Role of personality and the social situation. In G. J. Chelune (Ed.), *Origins, patterns and implications of openness in interpersonal relationships* (pp. 28–58). San Francisco: Jossey-Bass.

Barak, A., & Gluck-Ofri, O. (2007). Degree and reciprocity of self-disclosure in online forums. *CyberPsychology & Behavior*, 10(3), 407–417.

Barnes, S. (2006). A privacy paradox: Social networking in the United States. *First Monday*, 11 (9). http://firstmonday.org/issues/issue11_9/barnes/index.html (June 6th, 2011).

Bellman, S., Johnson, E. J., & Kobrin, S. J. (2004). International differences in information privacy concerns: A global survey of consumers. *Information Society*, 20(5), 313–324.

Boyd, D. (2008). *Taken out of context. American teen sociality in networked publics*. Ph.D. Dissertation, University of California, Berkeley. http://www.danah.org/papers/TakenOutOfContext.pdf (June 6th, 2011).

Boyd, D., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, 13(1), 210–230.

Boyd, D., & Hargittai, E. (2010). Facebook privacy settings: Who cares? *First Monday*, 15(8). http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3086/2589 (June 6th, 2011).

Buchanan, T., Paine, C., Joinson, A. N., & Reips, U.-D. (2007). Development of measures of online privacy concern and protection for use on the internet. *Journal of the American Society for Information Science and Technology*, 58(2), 157–165.

Buss, A. (2001). *Psychological dimensions of the self*. Thousand Oaks, CA: Sage.

Cho, S. H. (2007). Effects of motivations and gender on adolescents' self-disclosure in online chatting. *CyberPsychology & Behavior*, 10(3), 339–345.

Cho, V., & Hung, H. (2011). The effectiveness of Short Message Service for communication with concerns of privacy protection and conflict avoidance. *Journal of Computer-Mediated Communication*, 16(2), 250–270.

Christofides, E., Muise, A., & Desmarais, S. (2009). Information disclosure and control on Facebook: Are they two sides of the same coin or two different processes? *CyberPsychology & Behavior*, 12(3), 341–345.

Cong, L. (2007). Online chatters' self-marketing in cyberspace. *CyperPsychology & Behavior*, 10(1), 131–132.

Cozby, P. C. (1973). Self-disclosure: A literature review. *Psychological Bulletin*, 79(2), 73–91.

Debatin, B., Lovejoy, J. P., Horn, A.-K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication*, 15(1), 83–108.

Derlega, V. J., Durham, B., Gockel, B., & S holis, D. (1981). Sex differences in self-disclosure: Effects of topic content, friendship, and partner's sex. *Sex Roles*, 7(4), 433–447.

Dindia, K., & Allen, M. (1992). Sex differences in self disclosure: A meta-analysis. *Psychological Bulletin*, 112(1), 106–124.

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.

Ellison, N. B., Steinfield, C., & Lampe, C. (2011). Connection strategies: Social capital implications of Facebook-enabled communication practices. *New Media & Society*, 13(6), 873–892.

Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior*, 25(1), 153–160.

Harper, V. B., & Harper, E. J. (2006). Understanding student self-disclosure typology through blogging. *The Qualitative Report*, 251–261.

Haythornthwaite, C. (2005). Social networks and Internet connectivity effects. *Information, Communication & Society*, 8(2), 125–147.

Herring, S. C., Scheidt, L. A., Wright, E., & Bonus, S. (2005). Weblogs as a bridging genre. *Information Technology & People*, 18(2), 142–171.

Hinduja, S., & Patchin, J. W. (2008). Personal information of adolescents on the Internet: A quantitative content analysis of MySpace. *Journal of Adolescence*, 31(1), 125–146.

Jianakoplos, N. A., & Bernasek, A. (1998). Are women more risk averse? *Economic Inquiry*, 36(6), 620–630.

Joinson, A., Reips, U.-D., Buchanan, T., & Paine Schofield, C. B. (2010). Privacy, trust and self-disclosure online. *Human Computer Interaction*, 25(1), 1–24.

Jourard, S. M. (1959). Self-disclosure and other-cathexis. *Journal of Abnormal and Social Psychology*, 59 (3), 428–431.

Jourard, S. M. (1971): *Self-disclosure: An experimental investigation of the transparent self*. New York: Wiley.

Laurenceau, J.-P., Feldman Barrett, L., & Pietromonaco, P. R. (1998). Intimacy as an interpersonal process: The importance of self-disclosure, partner disclosure, and perceived partner responsiveness in interpersonal exchanges. *Journal of Personality and Social Psychology*, 74(5), 1238–1251.

Lenhart, A., & Fox, S. (2006). *Bloggers: A portrait of the internet's new storytellers*. Washington, D.C.: Pew Internet & American Life Project.

Lenhart, A., Madden, M., Macgill, A. R., & Smith, A. (2007). Teens and social media. http://pewinternet.org/~/media//Files/Reports/2007/PIP_Teens_Social_Media_Final.pdf.pdf (November 29th, 2011).

Lewin, K. (1948). *Resolving social conflicts*. New York: Harper.

Lewis, K., Kaufman, J., & Christakis, N. (2008). The taste for privacy: An analysis of college student privacy settings in an online social network. *Journal of Computer-Mediated Communication*, 14(1), 79–100.

Livingstone, S. (2008). Taking risky opportunities in youthful content creation: Teenagers' use of social networking sites for intimacy, privacy and self-expression. *New Media & Society*, 10(3), 393–411.

Marwick, A. E., & boyd, d. (2011). I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media & Society*, 13(1), 114–133.

Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing*, 18, 15–29.

Morgan, B. S . (1976). Intimacy of disclosure topics and sex differences in self-disclosure. *Sex Roles*, 2(2), 161–166.

Papacharissi, Z., & Gibson, P. L. (2011). 15 minutes of privacy: Privacy, sociality, and publicity on social network sites. In S. Trepte, & L. Reinecke (Eds.): *Privacy online: Perspectives on privacy and self-disclosure in the social web* (pp. 75–89). Heidelberg and New York: Springer.

Parker, R., & Parrott, R. (1995). Patterns of self-disclosure across social support networks: Elderly, middle-aged, and young adults. *The International Journal of Aging & Human Development*, 41, 281–297.
Peter, J., & Valkenburg, P. M. (2011). Adolescents' online privacy: Toward a developmental perspective. In S. Trepte, & L. Reinecke (Eds.): *Privacy online: Perspectives on privacy and self-disclosure in the social web* (pp. 221–234). Heidelberg and New York: Springer.
Petronio, S. (2002): *Boundaries of privacy. Dialectics of disclosure*. Albany, NY: SUNY Press.
Rideout, V. J., Foehr, U. G., & Roberts, D. F. (2010). *Generation M2: Media in the lives of 8- to 18-year-olds*. Menlo Park, CA: Kaiser Family Foundation. http://www.kff.org/entmedia/upload/8010.pdf (November 29th, 2011).
Qian, H., & Scott, C. R. (2007). Anonymity and self-disclosure on weblogs. *Journal of Computer-Mediated Communication*, 12 (4), 1428–1451.
Stefanone, M. A., & Jang, C.-Y. (2008). Writing for friends and family: The interpersonal nature of blogs. *Journal of Computer-Mediated Communication*, 13(1), 123–140.
Taddicken, M. (2010). *Measuring Online Privacy Concern and Protection in the (Social) Web: Development of the APCP and APCP-18 Scale*. Paper presented at the 60th Annual Conference of the International Communication Association, Singapore.
Taddicken, M. (2012). Privacy, surveillance, and self-disclosure in the social web: Exploring the user's perspective via focus groups In C. Fuchs, K. Boersma, A. Albrechtslund & M. Sandoval (Eds.), *Internet and surveillance: The challenges of web 2.0 and social media*. New York: Routledge
Thelwall, M. (2008). Social networks, gender, and friending: An analysis of MySpace member profiles. *Journal of the American Society for Information Science and Technology*, 59(8), 1321–1330.
Tufekci, Z. (2008). *Can you see me now?* Audience and disclosure regulation in online social network sites. *Bulletin of Science*, Technology & Society, 20–36.
Viegas, F. B. (2005). Bloggers' expectations of privacy and accountability: An initial survey. *Journal of Computer-Mediated Communication*, 10(3), article 12.
Westin, A. F. (1967). *Privacy and freedom*. New York: Atheneum.
Wheeless, L. R. (1976): Self-disclosure and interpersonal solidarity: Measurement, validation, and relationships. *Human Communication Research*, 3(1), 47–61.
Wheeless, L. R., & Grotz, J. (1976). Conceptualization and measurement of reported self-disclosure. *Human Communication Research*, 2(4), 338–346.
Yao, M. Z., Rice, R. E., & Wallis, K. (2007). Predicting user concerns about online privacy. *Journal of the American Society for Information Science and Technology*, 58(5), 710–722.
Yao, M. Z., & Zhang, J. (2008). Predicting user concerns about online privacy in Hongkong. *CyberPsychology & Behavior*, 11(6), 779–781.
Youn, S., & Hall, K. (2008). Gender and online privacy among teens: Risk perception, privacy concerns, and protection behaviors. *CyberPsychology & Behavior*, 11(6), 763–765.

About the Author

Monika Taddicken is a postdoctoral researcher at the Institute of Journalism and Communication Research at the University of Hamburg, Germany. Her research fields are computer-mediated communication, reception studies, and methodology.
Address: University of Hamburg, Grindelberg 7, 20144 Hamburg, Germany.

Annex

Information via hyperlinks:

General Willingness for Self-Disclosure	
sd1	It is difficult for me to talk about myself. (reversed)
sd2	I prefer that people know only a little bit about me. (reversed)
sd3	If I kept a diary, I would never show it to anyone. (reversed)
sd4	I sometimes find myself telling casual acquaintances things about myself.
sd5	There are many things about myself that I would rather not talk about with other people. (reversed)
sd6	I will not talk about personal matters unless someone else does so first. (reversed)

Note: The instructions accompanying the scale were "To what extent do the following statements apply to you?" Participants responded using a 5-point scale for each item (*does not apply at all* to *applies very much*).

Adapted Scale for Online Privacy Concern and Protection for Use on the Internet (APCP) (attitude)	
pc1	In general, how concerned are you about your privacy while using the Internet?
pc2	Are you concerned about online organizations not being who they claim they are?
pc3	Are you concerned that you are asked for too much personal information when you register or make online purchases?
pc4	Are you concerned about online identity theft?
pc5	Are you concerned about people online not being who they say they are?
pc6	Are you concerned about people you do not know obtaining personal information about you from your online activities?
pc7	Are you concerned that personal content that you store securely in the Internet (e.g. photos) can be viewed by others?
pc8	Are you concerned that information about you could be found on an old computer?
pc9	Are you concerned about who might access your medical records electronically?
pc10	Are you concerned that an email you send may be read by someone other than the person to whom you sent it?
pc11	Are you concerned that an email you send someone may be inappropriately forwarded to others?
pc12	Are you concerned that an email you send someone may be printed out in a place where others can see it?
pc13	Are you concerned that a computer virus could send out emails in your name?
pc14	Are you concerned about emails you receive not being from whom they claim to be?
pc15	Are you concerned that an email containing a seemingly legitimate address may be fraudulent?

Continued	
pc16	Are you concerned that if you use your credit card to buy something on the Internet, your credit card number will be obtained/intercepted by someone else?
pc17	Are you concerned that if you use your credit card to buy something on the Internet, your card will be mischarged?

Note: The instructions accompanying the scale were "We will now ask you to answer some questions about privacy and security. Please answer every question using the full scale provided." Participants responded using a 5-point scale for each item (*not at all* to *very much*).

Importance of Social Relevance	
sr1	That the application was recommended by friends and acquaintances.
sr2	That the application is known by the public.

Note: The instructions accompanying the scale were "If you sign up for one of the aforementioned Internet applications, how important are the following?" Participants responded using a 5-point scale for each item (*not at all* to *very much*).