Disclosure Management on Social Network Sites: Individual Privacy Perceptions and User-Directed Privacy Strategies

Philipp K. Masur and Michael Scharkow

Abstract
The social web and specifically social network sites (SNS) have offered new opportunities for interaction and communication, but have also increased the risk of privacy violations. In this study, we investigated how far users imply different disclosure management strategies in status updates and chat conversations. We hypothesized that users perceive specific information as differently private depending on their personal privacy preference, but generally show the same disclosure management pattern: the higher the perceived privacy level of an information, the less frequently it will be shared. We tested the hypothesis using an online survey with 316 German SNS users. The findings suggest that respondents engaged in disclosure management taking both communication channel and type of information into account. We further found that trust toward SNS contacts and use of privacy settings significantly influenced disclosure management in one-to-many (status updates) but not in one-to-one communications situations (chat conversations). The results complement existing research by showing the pivotal role of individual privacy perceptions in explaining users’ privacy management in the social web.

Keywords
privacy, self-disclosure, disclosure management, social network sites

As most Internet services require users to provide personal information in order to function (Joinson, Houghton, Vasalou, & Marder, 2011), people willingly disclose personal information and oftentimes even intimate details of their lives (European Commission, 2011; Madden et al., 2013; Taddicken, 2013). And the more users disclose of themselves, the more they may find gratifications and benefits these systems have to offer (Walther, 2011). As the infrastructure of the social web is based on both technical and social convergence (Papacharissi, 2010), it connects people, applications, and businesses. Hence, a new flow of information across media platforms takes places, subsequently creating manifold opportunities for users to interact both as consumers and as producers (Papacharissi, 2012), but also expanding potential threats to individuals’ privacy. Current debates about Internet privacy have consequently proclaimed that we are witnessing an irreversible transformation of how we conceptualize and perceive privacy in general (acatech, 2013). In a nutshell, the Internet and in particular the social web are altering the concept of privacy due to four interconnected properties which are typically not present in face-to-face situations: persistence of data, searchability of specific information, exact copyability, and invisible audiences meaning people or third parties who have access to the information without the user’s knowledge (boyd, 2007, p. 2).

In this study, we focus on privacy management on social network sites (SNS) and specifically on disclosure management as a strategy of data parsimony. Initial research on privacy in online environments has found that people share intimate details of their lives despite pronounced privacy concerns and generally show little privacy protection behaviors (Gross & Acquisti, 2006; Taddei & Contena, 2013; Taddicken, 2013; Tufekci, 2008). Yet, other studies found contrary results and did not support the privacy paradox (e.g. Debatin, Lovejoy, Horn, & Hughes, 2009; Krasnova, Spiekermann, Koroleva, & Hildebrand, 2010; Stutzman, Vitak, Ellison, Gray, & Lampe, 2012). A recent study even suggests that the seeming paradoxical behavior of SNS users...
is illusory as refined measurement and operationalization of the relevant concepts make the paradox disappear (Dienlin & Trepte, 2014). In line with these findings, we believe that people do engage in many different privacy strategies in order to achieve their ideal level of privacy. Some recent studies have shown that many users do use different privacy settings to imply specific privacy boundaries and they also monitor their disclosures (e.g., boyd & Hargittai, 2010; boyd & Marwick, 2011; Christofides, Muise, & Desmarais, 2011; Litt, 2013). We extend this line of research by arguing that the management of disclosures is pivotal in the process of achieving an optimal level of privacy. Conclusions in previous studies were often based on the premise that the more SNS users disclose, the more privacy they lose. Yet, the mere sharing of information itself might not be perceived as privacy endangering by the individual. We argue that people are only concerned about privacy violations if the shared information is actually perceived as private. In view of that, we hypothesize that people attribute different levels of privacy to different types of information depending on their individual privacy preferences. They further disclose information perceived as private less often than non-sensitive information. This disclosure management should be more pronounced in public or semi-public communication situations (e.g., status updates) where users communicate with multiple audiences.

Within the following paragraphs, we will first elaborate on the theoretical background of privacy and self-disclosure. Second, we will review current literature on privacy management on SNS arguing that the incorporation of individual privacy perceptions is necessary when investigating disclosure behavior on SNS. In the subsequent section, we will present theoretical arguments supporting the concept of disclosure management as a specific form of privacy management. We will test the hypotheses based on data from an online survey among German users of the SNS Facebook.

**Privacy as Selective Boundary Control**

From the individual’s point of view, privacy corresponds to private sphere—a situation, room, or space in which a high level of privacy is given. People need a privacy from time to time as it facilitates personal autonomy, emotional release, self-evaluation, and limited or protected communication (Westin, 1967). From a psychological perspective, however, achieving a desired level of privacy encompasses a complex and dynamic process of limiting access of others to the self. According to Altman (1975), privacy involves “the selective control of access to the self” (p. 18). He argues that privacy regulation is “like the shifting permeability of a cell membrane” (Altman, 1975, p. 10). Achieving an optimal level of privacy thus affords a dynamic process of interpersonal boundary control. Depending on the situation, people desire a certain level of privacy which constitutes their ideal level of interaction with others. Achieved privacy, in contrast, is the actually perceived level of privacy in a situation. Thus, individuals engage in a constant optimizing process to achieve an ideal balance between desired and actual privacy (Altman, 1975). The individual’s goal is hence not always a maximum of privacy. Depending on situational factors and needs, an optimal level can range anywhere between no privacy to high privacy.

Extending these approaches, communication privacy management (CPM) theory by Petronio (2002) seems to be the most useful concept for understanding privacy in computer-mediated communication (Margulis, 2003, 2011). In congruence with Altman’s theory, CPM theory posits that privacy can range from complete closeness to complete openness (Petronio, 2002). A crucial aspect of CPM theory, however, is the proposition that people regulate this dialectic process in terms of ownership and linkage rules (Petronio, 2002). In line with this reasoning, private information is defined by individuals as information that belongs to them. Because of this ownership, they claim the right to control the distribution. Based on individual importance criteria, they manage the flow of this information. Once this information becomes shared, the nature of this information changes as it becomes co-owned by others. This co-ownership is ideally negotiated as a collective privacy boundary based on permeability rules (how much are other people allowed to know), ownership rules (how much control about the information have co-owners), and linkage rules (who else can become co-owner) (Petronio, 2002; Petronio & Reierson, 2009). If these rules are violated, privacy turbulences occur and people try to update, correct, or recalibrate the adequate functioning of privacy rules (Child & Petronio, 2011; Child & Westermann, 2013). Privacy management hence includes processes of concealing and revealing.

In sum, the theories discussed here posit that people engage in various regulative behaviors in order to obtain an appropriate level of privacy, thereby taking into account both risks and benefits that derive from disclosing information (Child & Petronio, 2011). Privacy management can thus be referred to as a selective boundary control which is enacted in multiple behavioral mechanisms and strategies. In the following section, we will categorize typical privacy management strategies in the context of social media usage.

**Privacy Management in the Social Web**

Many scholars have investigated what practices users imply in order to protect different aspects of their online privacy. However, a universally accepted categorization is not available. Nonetheless, it is fruitful to distinguish privacy management practices on different levels. Whereas social web users generally try to protect their personal information against misuse and unwanted forwarding through other users, they also want to ensure data protection against massive data mining and surveillance by providers, companies, and institutions. Raynes-Goldie (2010) calls the first social
privacy and the latter institutional privacy. She found that users mostly worry more about inappropriate friend requests or threats from multiple audiences than privacy threats from institutional data-handling practices (Raynes-Goldie, 2010). These social privacy concerns might be more pronounced because in the social web, users are mainly confronted with people they are connected to in their daily life. Interpersonal boundary turbulences might hence cause real consequences in their lives, whereas data mining of companies or institutions has mostly no visible or sensible consequences.

Privacy strategies can further be differentiated into individual and collaborative, as well as preventive and corrective measures (Lampinen, Lehtinen, Lehmuskallio, & Tamminen, 2011). In recent years, many privacy-related studies in the context of SNS have focused on individuals’ use of pseudonymization strategies including using fake names (e.g., Debatin et al., 2009; Dienlin & Trepte, 2014; Tufekci, 2008), the use of privacy settings such as using friend lists (e.g., Litt, 2013; Vitak, 2012), not befriending persons (e.g., Christofides, Muise, & Desmarais, 2009), or restricting visibility of the profile or different parts of the profile (e.g., Debatin et al., 2009; Dienlin & Trepte, 2014). But apart from these strategies, which serve to establish and regulate the context in which the user can feel private and disclose information, users also monitor and control their disclosures. In terms of CPM theory, all contacts become co-owners of any information users disclose to them (Child & Petronio, 2011; Petronio, 2002). Thus, individuals have to carefully decide what information they want to share. Privacy management strategies thus also include strategies relying on data parsimony. A first option is to opt-out and thus refrain from using a service or platform. But as social web applications and in particular SNS become a popular resource for people to connect with others, maintain relationships, consume user-generated content, distribute personal content about the self (Ellison, Steinfield, & Lampe, 2007; Ellison, Vitak, Steinfield, Gray, & Lampe, 2011), and also offer a variety of other gratifications (Papacharissi & Mendelsohn, 2011; Smock, Ellison, Lampe, & Woh, 2011), opting-out is not an attractive solution for most users. Recent qualitative research has shown that some users also perform a sort of “soft” opt-out as they deactivate their account every time they leave the site in order to make their profile unsearchable (boyd, 2010a). However, so far, no quantitative study has examined this technique in more detail. In a qualitative study with young Estonian social media users, the researchers found no indication that this advanced strategy was actually used (Oolo & Siibak, 2013).

Consequently, many—especially young—SNS users engage in more advanced privacy strategies which serve to reduce the risks associated with social media use while still benefiting from the social gratifications that sharing of private content has to offer. Social steganography (boyd, 2010b), for example, means that users limit access to the meaning of a publicly posted message, but do not limit the access itself. Although the message is communicated to multiple audience simultaneously, it is meaningless to the greater audience as the interpretation of such a multi-layered message requires recognizing references and cues (boyd & Marwick, 2011; Oolo & Siibak, 2013). In structured interviews with Estonian high school students, Siibak and Murumaa (2011) found that these cues can be song lyrics and quotes which target the posts to specific audiences who possess the interpretive lens to decode the message.

A second strategy can be described as “whitewalling” or “whitewashing.” In a qualitative study, boyd (2010a) found that young girls delete wall messages and status updates shortly after they have been read. These users indicated that they were interested in posting and keeping in contact with other people, but that these interactions should not be persistent (boyd, 2010a).

Apart from these elaborated strategies, most SNS users use a simple heuristic: They try to avoid posting overly private information in most and specifically in one-to-many communication situations. In the following, we will consequently define this disclosure management as a typical and commonly used strategy.

**Monitoring Self-Disclosure as an Implementation of Data Parsimony**

In social psychology, self-disclosure has been defined as the process of revealing information about oneself to another person (for an overview, cf. Cozby, 1973; Greene, Derlega, & Mathews, 2006; Pearce & Sharp, 1973). Altman and Taylor (1976) further argue that self-disclosure can be categorized into peripheral (e.g., biographic data), intermediate (attitudes, values, and opinions), and core layers (personal beliefs, needs, and fears). People might perceive these layers as differently private due to different privacy preferences. Prior studies have found pronounced differences in privacy preferences (e.g., Marshall, 1974; Pedersen & Frances, 1990). Our first hypothesis draws upon these findings; not only do people have different general privacy preferences resulting in different situational privacy needs, but they also perceive different types of information as differently private (H1).

Self-disclosure furthermore fulfills an important function: the revealing of private information is required in social relationship as it serves to strengthen ties and bonds in dyadic or group relationships (Joinson & Paine, 2007; Jourard, 1971). Thus, the individual decision process with regard to self-disclosure always reflects the balancing of contradictory needs. People generally seek to maximize social rewards and benefits, but at the same time, they try to minimize personal risks (Petronio, 2002). However, the traditional concept of self-disclosure does not necessarily transfer to all communication situations on SNS (Bazarova & Choi, 2014). Although dyadic disclosure is possible on SNS (e.g., private messaging), many users also communicate to their whole network of contacts (e.g., in status updates). Social media are typically...
characterized by one-to-many communication situations where users disclose information to large, socially diverse, and sometimes even unknown or invisible audiences (Vitak, 2012). Whereas disclosure in private messages is mostly directed toward a specific recipient, status updates are typically undirected or only directed toward an imagined audience (Litt, 2012). As Jourard argued already in 1971, dyadic interactions might be completely different from more public situations where people broadcast private information publicly. In these situations, users are confronted with different audience representations which might in turn affect self-disclosure goals and specific disclosure patterns (Bazarova & Choi, 2014; Rosenfeld & Kendrick, 1984). Again, to use CPM theory as a framework, any information broadcast in status updates becomes co-owned by other users who were allowed as members of the network. SNS users thus have to carefully decide which information to share. As a general assumption, SNS users’ disclosure frequency should hence differ depending on (a) the information and (b) the communication channel (H2). We further argue that these differences can be explained by individual privacy preferences. In the following section, we will propose the concept of disclosure management which suggests that SNS users show a specific disclosure pattern which helps them to maximize social reward and minimize privacy risks.

**Defining Disclosure Management**

The proposed concept of disclosure management can be classified as a privacy management strategy based on the principle of data parsimony. Apart from contextual privacy strategies, people constantly monitor and control their own disclosures, thereby adapting to changing situations. As such, it can be regarded as a sort of self-censorship. Scholars have found that only relatively few communication transactions involve high levels of private information disclosure (Jourard, 1967; Pearce & Sharp, 1973). People thus do not generally disclose private information. Many conclusions in previous research are nonetheless based on the premise that the more SNS users disclose (no matter if private or not), the more privacy they lose. From a psychological point of view, it seems more reasonable to assume that the individual only fears the risk of a privacy violation if the information being shared is actually perceived as private. As people attribute different levels of privacy to different information depending on their individual privacy preferences, they should consequently disclose information perceived as private less often than non-sensitive information. Our third hypothesis is therefore formulated as follows: There will be a negative relationship between individual privacy perceptions and disclosure frequency (H3a).

While we assume that this disclosure pattern should be recognizable in any communication situation, it should nevertheless be more pronounced in public than in private communication situations. Disclosure management is particularly needed when information is not protected by a dyadic, trusted relationship (Altman & Taylor, 1976; Bazarova & Choi, 2014). We assume that self-disclosure in one-to-many communication situations differs from self-disclosure in one-to-one interactions. A few carefully designed studies by Bazarova and colleagues have investigated differences between public and private communications. Using an experimental design, Bazarova (2012) found that disclosures in private messages on Facebook were perceived as more intimate and private as disclosures in status updates. In a second study, Bazarova and Choi (2014) used a novel design to assess differences in disclosure intimacy depending on the communication condition: participants were asked to copy and paste the six most recent status updates, wall posts, and private messages into a web survey. Using content analysis, the researchers investigated the intimacy of each message. The findings revealed that disclosures via private messages were indeed more intimate than disclosures via status updates or wall posts. The authors also found that these differences can be explained by different motives. Whereas social validation goals were more evident in status updates than in private messages, participants indicated that their motivation behind disclosures in private messages was mainly relational development. These findings also support assumptions of the lowest common denominator principle (Hogan, 2010). According to this concept, SNS users only reveal information in status updates that is appropriate for all members of the SNS network.

In line with this reasoning, we hypothesize that people disclose information which they perceive as private less frequently in status updates than in private messages. Our assumptions thus differ from the studies of Bazarova in one crucial aspect: disclosure management depends on the individual privacy perception of a specific information. This means that even if one person might consider a photo of himself as private and accordingly chooses not to disclose it in a status update, and another person might rate photos of himself as less private and consequently share them with other people more frequently, they both show the same pattern of disclosure management. The hypothesis can be formulated as follows: Disclosure management—operationalized as the negative relationships between individual privacy perception and disclosure frequency—will be higher in status updates than in private messages (H3b).

**Influences on Disclosure Management**

A number of different influences on privacy management in general and disclosure management in specific can be identified. The decision to disclose personal information may be dependent on distal (cultural criteria, social network characteristics, and individual differences in personality) and proximal factors (self, other[s], relationship-linked reasons), as well as the assessment of the situation (Greene et al., 2006). In this study, we investigate potential distal (need for privacy)
and proximal (trust) factors of disclosure management. As noted before, disclosure management is enacted individually and thus depends on individual privacy preferences. This implies that people differ with regard to privacy needs. As Child and Petronio (2011) denote, “higher control needs are manifested in regulating privacy boundaries by controlling the flow of information to others” (p. 30). We hence assume that SNS users with a high need for informational privacy will engage in more disclosure management in (a) chat conversations and (b) status updates (H4).

As disclosure always requires social interactions, trust seems to be a pivotal factor in the decision to disclose personal information (Wheelells & Gross, 1977). The privacy boundary may be open or closed depending on the level of trust that a person has toward the recipients of the information (Altman & Taylor, 1976; Roloff, 1981). Scholars found out that lower trust predicts general information control (Christofides et al., 2009). A number of studies also suggest that the influence of privacy concerns on self-disclosure was mediated by trust (Joinson, Reips, Buchanan, & Schofield, 2010; Malhotra, Kim, & Agarwal, 2004; Metzger, 2004). We can also assume that privacy boundaries and ownership rights—as defined by CPM theory—are mostly based on trust. People feel particularly able to disclose personal information if they perceive potential co-owners as trustworthy. Qualitative research presents anecdotal evidence that teenagers disclose specifically to an inner trusted circle (Marwick & boyd, 2014). As noted before, SNS users establish privacy boundaries through befriending other users who inevitably become co-owners of the information disclosed. Accordingly, in one-to-many communication situations, this boundary is also based on trust. We hence hypothesize that SNS users with higher trust toward their whole SNS network will engage in less disclosure management in both (a) chat conversations and (b) status updates (H5).

Another important question is how far preventive privacy management strategies, such as using friend lists, influence the disclosure management. CPM theory again suggests that privacy settings are used to establish privacy boundaries and circles of co-ownership. It seems possible that users who strongly restrict the visibility of their profile actually disclose more because they believe that the disclosed information remains in a trusted privacy boundary. However, it has been argued that social media flatten multiple audiences into one (Marwick & boyd, 2014) leading to a context collapse (Vitak, 2012). On Facebook, users are generally confronted with broad and unspecific audiences including people from different social contexts such as co-workers, family members, friends, and even strangers or mere acquaintances. The feature friend lists enables users in particular to distinguish audiences from different social contexts. Previous scholars have consequently argued that using friend lists leads to more disclosure of intimate information because they establish trusted privacy boundaries by segmenting their contacts into smaller and more manageable groups (Stutzman, Capra, & Thompson, 2011). In a larger model, Vitak (2012) investigated, among other relationships, how far the privacy settings (operationalized as the use of friend lists) influence the amount of actual and intended disclosures. But in contrast to the findings of Stutzman and colleagues (2011), and disconfirming her own hypothesis, there was no significant relationship between the use of friend lists and the actual amount of disclosures. We think it is plausible to assume that users who think more about potential privacy threats and consequently use specific privacy settings also consciously think about their potential audiences and additionally engage in passive data protection strategies. We hence argue that SNS users who use friend lists will also engage in more disclosure management in status updates (H6).

Methods

Participants and Procedure

To test the hypotheses, an online survey was conducted from December 2013 to January 2014. The study’s link was disseminated using a snowball sampling technique: 27 students with Facebook profiles posted the link in status updates to their Facebook networks, thereby inviting their Facebook friends to participate in the study and to further share the link with their contacts. This way, existing study subjects recruited future subjects among their acquaintances. This sampling technique was favored as the study focused specifically on Facebook users. In total, 379 Facebook users took part in the survey. Due to missing data, 63 participants had to be excluded. The following analyses are accordingly based on the remaining 316 participants.7 As university students served as the initial informants, the majority of participants were also students (66%). Their average age was 24.58 years (standard deviation [SD] = 5.48) and 199 (63%) of them were female. Most participants used Facebook several times a day (66%) or at least once a day (25%). Respondents furthermore indicated that on average, they spent 53.36 min per day on Facebook (SD = 60.27). Completion of the survey took around 13 min.

Measures

Individual Privacy Perceptions of Specific Information Types. To measure differences in privacy perceptions, we presented participants with a list of nine different types of information that are typically shared on SNS. We constructed the list by extending and adapting the Self-Disclosure Index by Miller, Berg, and Archer (1983). The list thus included supposedly private information such as “My deepest fears,” “My personal feelings,” “Details from relationships to other people,” “My political, ethical or religious views,” and “Things that I am proud of.” We further included information assuming less private such as “Changes in my life,” “What I like or enjoy,” “My hobbies or my work,” and “Photos of myself.” Respondents answered all items on
a 5-point Likert-type scale, ranging from 1 (Not at all private) to 5 (Very private).

**Disclosure Frequency of Specific Information Types.** We further measured how often people disclosed these information types in status updates and chat conversations. For each information type, participants indicated the disclosure frequency on a 6-point scale. The scale ranged from 1 (Never) to 6 (Very often). To assess the overall frequency of information disclosure, we computed the mean index for each communication situation. The mean for disclosure frequency in status updates was $M_{\text{status}} = 2.04$ ($SD_{\text{status}} = 0.88$). The internal consistency of the index was good (Cronbach’s $\alpha = .88$). Frequency of information disclosure in chat conversations was slightly higher ($M_{\text{chat}} = 3.20$; $SD_{\text{chat}} = 1.12$). Again, internal consistency of the index was good (Cronbach’s $\alpha = .91$).

**Need for Informational Privacy.** To assess the individual’s need for informational privacy, we used a 4-item scale which was specifically designed for this study. The items read as follows: “It does not bother me, if information about myself is publicly available” (reverse coded), “I prefer that little is known about myself,” “I don’t want my personal data to be visible for the public,” and “My identity should not be accessible for everyone.” Respondents had to answer on a 5-point Likert-type scale, ranging from 1 (Do not agree at all) to 5 (Totally Agree). The internal consistency of the scale was satisfactory (Cronbach’s $\alpha = .78$). The scale’s mean was $M = 3.88$ ($SD = 0.73$).

**Trust toward SNS Network.** In order to measure people’s trust toward their individual SNS network, we used a 3-item scale. An example item is “In general, people in my SNS network are trustworthy.” Again, respondents indicated agreement with the items on a 5-point Likert-type scale ranging from 1 (Do not agree at all) to 5 (Totally Agree). Internal consistency of the scale was satisfactory (Cronbach’s $\alpha = .72$). On average, participants rated their SNS network as rather trustworthy ($M = 3.56$; $SD = 0.64$).

**Use of Friend Lists.** So far, we have argued that status updates generally equal one-to-many communication situations and chat conversations correspond to one-to-one communication situations. Facebook, however, provides users with the possibility of segmenting their audience: by using friend lists, SNS users are able to limit the visibility of status updates to a specific, predefined group. We hence asked respondents the following question: “Do you use friend lists in order to divide your SNS network in different groups?” One-third of the participants reported that they used this feature.

**Variable Coding and Data Analysis**

As a key concept of this article, disclosure management is defined as a behavioral pattern: individuals disclose private information less often than non-sensitive information. Statistically, this implies a negative correlation between individually perceived privacy of different types of information and the frequency of disclosing them on social networks. The more consistent this behavior is, the closer this correlation should be to $r = -1.00$. Since both the perceived privacy of the information type and the disclosure frequency will vary across respondents, it is necessary to compute a within-subject correlation for every respondent. Hence, we measured the extent of individual disclosure management by computing the within-subject correlation between individual privacy perceptions and disclosure frequency for all nine information types mentioned above and separately for status updates and chat conversations. For easier interpretation, we reversed the sign of the correlation coefficient so that a consistent disclosure management would yield a (large) positive score, whereas the score would be zero when no relationship between privacy perceptions and posting frequency is observed.

In order to test Hypotheses 4–6, we estimated a multivariate regression model with two outcomes (disclosure management for status updates and chat conversations, respectively). Since some of the predictors are constructed as latent variables (e.g., need for privacy and trust toward SNS networks), we used structural equation modeling with (full information) maximum likelihood estimation. Frequency of disclosures in status updates and in private messages was included as control variables. All analyses were conducted using R and the lavaan package (Rosseel, 2012).

**Results**

In the first step, we analyzed what levels of privacy respondents attributed to different types of information, with the expectation that there would be a considerable amount of variation both across information types and between respondents. Figure 1 displays the means and 95% confidence intervals of these respondent ratings.

Our data support Hypothesis 1, as there were significant differences in the means for the various information types, as illustrated by the non-overlapping confidence intervals in Figure 1. Fears, concerns ($M = 4.5$, $SD = 0.7$), and personal feelings ($M = 4.3$, $SD = 0.7$) were almost universally considered very private, whereas favorite books ($M = 2.3$, $SD = 0.9$) or hobbies ($M = 2.2$, $SD = 0.8$) were perceived as less private information. In addition, there was considerable disagreement about the level of privacy of certain information types, as indicated by larger SDs. Respondents varied especially in their privacy perceptions concerning political or religious opinions ($M = 3.0$, $SD = 1.1$) and important events in life, such as births or marriages ($M = 2.8$, $SD = 0.9$).

Looking at the disclosure frequency of different types of information and information channels displayed in Figure 2, we see that our Hypothesis 2 was also supported: There were substantial and statistically significant differences between communication channels as well as between different types
Respondents shared all types of information significantly less often via status updates than via private chat messages. Moreover, information considered private by many respondents, such as personal feelings ($M=1.7, SD=1.0$), relationship details ($M=1.5, SD=0.9$), or fears and concerns ($M=1.2, SD=0.6$), were almost never disclosed in status updates. It is noteworthy that the rank order of disclosure frequency, aggregated across all respondents, was not simply the inverse of the privacy attributions.

Figure 2 also shows that the rank order for disclosure frequency in private message was not the same as for status updates so that we can assume that respondents clearly adapted their disclosure behavior by taking information and channel into account.

By computing the disclosure management score, that is, the within-subject correlation of individual privacy perceptions and disclosure frequency, we could test Hypothesis 3a that the more privately the information is perceived, the less often it is shared on SNS. Indeed, the average correlation coefficient was negative and significant for status updates (average $r=-.38, SD=.34$) and, to a lower degree, for chat messages (average $r=-.14, SD=.39$). A paired $t$-test confirmed H3b that disclosure management was less pronounced for private messages than for status updates, $t(263)=10.1$,
The disclosure management scores for both channels were moderately correlated ($r = .43$).

Since there were substantial inter-individual differences in disclosure management, we investigated potential predictors in the final step of our analysis. For this purpose, we estimated a multivariate regression model with latent variables, as depicted in Figure 3.

The structural equation model fit the data very well according to common criteria (Hu & Bentler, 1999), with a non-significant $\chi^2$ goodness-of-fit index. Although the regression model with five predictor variables only explained a small amount of variation in disclosure management, especially for chat messages, we nonetheless found that individual differences in privacy attitudes and SNS usage were related to disclosure management. However, need for informational privacy did not significantly predict disclosure management, neither for status updates nor private messages, disconfirming Hypothesis 4. In contrast, Hypothesis 5 was supported by the data, since stronger trust in their SNS network was related to less disclosure management in status updates ($\beta = -.17$) and privacy chat conversations ($\beta = -.17$). In line with Hypothesis 6, respondents who used friend lists as an active way of privacy management on SNS were also more likely to employ a consistent disclosure management ($\beta = .11$). In addition, we also found that respondents who posted status updates more often also engaged in more consistent disclosure management ($\beta = .27$), although the same effect could not be found for chat messages.

Summing up the empirical results, we can say that our data show strong evidence that disclosure management (a) could be observed, to a varying degree, among many respondents; (b) was far less pronounced for private messages than for status updates; and (c) was related to attitudes and behaviors concerning SNS in general and trust in one’s SNS network in particular.

**Discussion**

Older studies with regard to privacy management on SNS have often suggested that people behave illogically because they disclose a considerable amount of information and do not engage in privacy protection strategies, despite their often pronounced concerns about privacy violations (e.g., Acquisti & Gross, 2006; Taddicken, 2013; Tufekci, 2009). Yet, with the rationale presented in this article and in line with more recent studies on privacy management, we suggest that there is a need for a more specific differentiation between distinct privacy management strategies. We furthermore argue that it
is also necessary to investigate more closely when and under which circumstances people use these specific strategies. It is particularly important to differentiate to what or whom these protection strategies are directed. In order to exemplify this need, this study focused specifically on disclosure management as a strategy of data parsimony, which is directed against privacy violations that arouse from other SNS users. To our knowledge, apart from the qualitative studies mentioned above, no quantitative study has investigated the relationship between subjective privacy perceptions and self-disclosure. This study hence extends prior research by suggesting a more specific methodological approach toward measuring this specific privacy management strategy by accounting for individual differences in privacy preferences.

Our results show that SNS users manage their disclosures by sharing less to almost no information that they perceive as private. We were able to observe this behavioral pattern in a varying degree among all participants of the study. They consequently try to be parsimonious with information that they individually consider as private. In line with CPM theory, people hence seek to protect their individual privacy by concealing certain information from others and thus retaining a personal privacy boundary (Child & Petronio, 2011). This deliberate management is more pronounced in public than private communication situations. Facebook offers possibilities to communicate in chat conversations and to communicate with the whole network of contacts. Both communication channels have specific characteristics. Whereas private messages resemble typical face-to-face conversations, status updates address a broader audience in a larger privacy boundary. As our findings show, SNS users generally disclose less information in status updates, but they also consciously refrain from posting information that they individually consider as private for their Facebook contacts. This might be due to the perceived risk of privacy violations which is potentially higher in status updates because of the larger audience. This result is comparable to the findings of Bazarova and Choi (2014) who also found that disclosures in chat conversations are more intimate than disclosures in status updates.

A second aim of our study was to identify potential influences on disclosure management which can explain why SNS users differ with regard to the amount of disclosure management. First, we investigated to what extent the need for informational privacy affects the tendency to use a strategy of data parsimony. Yet, in contrast to our hypothesis, there was no significant relationship. However, as the need for informational privacy specifically measured a general discomfort to make personal identifying information available to the public, this finding is not too surprising: the amount of disclosure management indicates how far people refrain from posting information that they perceive as private, but not whether they generally refrain from making personal data available to a broader public. Although our initial hypothesis was not supported, this finding shows that different strategies are being used for different reasons. In contrast to active strategies, such as encryption or pseudonymization, disclosure management does not help against all data collection by institutions, organizations, or online providers, and might hence not be related to this general concept of need for informational privacy.

An important negative predictor of disclosure management is trust. Disclosure management was less pronounced if SNS users rated their SNS contacts as trustworthy. The higher the trust toward the recipients of an information, the more he or she believes that this person will not abuse the co-ownership that he or she transferred to him by disclosing the information. Disclosure management is hence specifically necessary if the possible audience is not trustworthy. By consciously constructing a limited privacy boundary (e.g., by adding only trusted friends or acquaintances), SNS users are able to create a room in which they are able to disclose personal information.

Using privacy settings such as friend lists, users should also be able to create limited and trusted privacy boundaries. However, based on previous findings, we hypothesized that people who use such privacy settings also disclose private information more carefully. Using friend lists was indeed a positive predictor of disclosure management replicating the findings of Vitak (2012). Using friend lists and managing disclosures might hence be consequences of the same psychological disposition. SNS users with strong concerns might implement as many strategies as possible in order to get an optimal protection of their private information.

On a general note, however, it seems important to ask how far online privacy literacy (cf. Trepte et al., 2015) influences practices of privacy protection. Trepte and colleagues (2015) argue that users with low levels of privacy literacy are not aware of potential threats, thus misjudging the risks of sharing information and hence do not employ sophisticated privacy strategies. Future studies should hence focus on the role of privacy literacy and its influence on the implementation of different privacy strategies. It might be possible that specifically users with low levels of online privacy literacy engage in disclosure management as deciding what information is too private to share requires lower skills than implementing sophisticated privacy tools or settings.

**Limitations**

In this study, we focused on disclosure management as a strategy of data parsimony. We therefore asked participants to rate the level of privacy of various types of information. Due to economic reasons while developing the questionnaire, we used only a small number of information types which are typically disclosed on SNS. In order to model the extent of disclosure management more comprehensively, it would be necessary to investigate all potential information that a user might disclose. Nonetheless, we do not believe that a more refined and broader questionnaire would yield
different results. Based on the rationale presented in the theoretical outline, we argue that it is more important to incorporate the individual privacy perception for each information. However, future studies investigating disclosure management should also focus on the way users disclose information. As recent qualitative studies suggest, people also change the mode of disclosing information depending on the context. For example, hiding information by changing the style of writing and including specific references or cues is another strategy that can be implemented within the more general disclosure management.

A number of methodological limitations have to be taken into account when interpreting the results of this study. The first limitation refers to the oftentimes observed discrepancy between self-reported data and actual data which can be observed with logging software. The instruments used in this study are based on self-reports. As findings of recent studies suggest, self-reports of behaviors are often not accurate (e.g., Junco, 2013; Scharkow, 2014). Self-reports require a reconstruction of attitudes, feelings, or behaviors from memory and can subsequently be biased. Future research should imply more objective measurement procedure such as tracking and logging of actual behavioral data. Second, as the data stem from a non-probability sample of Facebook users, the results cannot be generalized for all SNS users. As we used a snowball-technique, the sample was very homogeneous. Consequently, it remains unclear whether users of different platforms implement the same privacy strategies or whether there is a difference between younger and older SNS users. However, we do believe that the general assumptions of the proposed model can also be found in more heterogeneous and diverse sample. Specifically, disclosure management should also be identifiable in representative samples. Future studies should nonetheless extend and replicate the findings of this study with larger samples.

Conclusion and Implications

The popularity of social media applications and recent debates about their negative effects has led many parents, scholars, and politicians to believe that most people do not care about privacy while using Facebook, Twitter, or Instagram. However, based on our empirical findings, we believe that this is not the case. Nowadays, social media have become part of our daily routine and many people—especially young adolescents—show a deep engagement with specific applications and its functions. Social web applications offer manifold possibilities to satisfy needs, and to benefit from various gratifications. However, this does not imply that users do not care about privacy and thus generally refrain from implementing privacy management strategies. There are many distinct strategies an individual can apply to protect his personal data depending on potential risks and the potential receivers of the information. In this study, we found that many SNS users do evaluate whether an information is too private to be shared. Especially in public situations, they relinquish only non-sensitive information that they deem appropriate for all potential users. In summary, SNS users do manage their disclosures depending on the level of privacy of the information and the publicness of the communication channel.

That being said, this finding does not imply that users generally do everything to protect their personal data while surfing the Internet. It is important to keep in mind that disclosure management is only directed toward other users. Effective data protection against other privacy violations requires other (oftentimes more technical and difficult) strategies. Although people might generally be parsimonious in disclosing private information, they do abandon a lot of personal identifying information—in many cases without even noticing. Looking at the dynamics of the social web from a provider versus client perspective, privacy violations do not only originate from the disclosure of private information, but from any information provided in the web that can be linked to the user (e.g., meta-data). To protect themselves from massive data mining, profiling, and ubiquitous surveillance, users need to implement comprehensive, and oftentimes difficult, protection measures such as encryption or anonymization. Although observed privacy practices reveal how users deal with these new technical affordances, it seems questionable whether an overall effective self-protection can be achieved by the individual.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

Note

1. Note that the disclosure management score was reversed before estimating the model so that a negative path coefficient can be interpreted in a straightforward manner.
2. We uploaded the data and a documentation of the analyses in the following online repository: https://osf.io/8bzxd/.

References

Acatech. (2013). Internet privacy. Options for adequate realisation (acatech STUDY). Heidelberg: Springer.
Acquisti, A., & Gross, R. (2006, June). Imagined communities: Awareness, information sharing, and privacy on the Facebook. Paper presented at the 6th Workshop on privacy enhancing technologies, Cambridge, UK. Retrieved from http://people.cs.pitt.edu/~chang/265/proj10/zim/imaginedcom.pdf.
Altman, I. (1975). The environment and social behavior: Privacy, personal space, territory, crowding. Monterey, CA: Brooks/Cole.
Altman, I., & Taylor, D. (1976). Social penetration: The development of interpersonal relationships. New York, NY: Holt, Rinehart and Winston.
Bazarova, N. N. (2012). Public intimacy: Disclosure interpretation and social judgments on Facebook. Journal of Communication, 62, 815-832. doi:10.1111/j.1460-2466.2012.01664.x
Bazarova, N. N., & Choi, Y. H. (2014). Self-disclosure in social media: Extending the functional approach to disclosure motivations and characteristics on social network sites. Journal of Communication, 64, 635–657. doi:10.1111/jcom.12106
boyd, d. (2007). Why youth (heart) social network sites: The role of networked publics in teenage social life. In D. Buckingham (Ed.), Youth, identity, and digital media (pp. 119–142). Cambridge, MA: MIT Press.
boyd, d. (2010a). Risk reduction strategies on Facebook. Retrieved from http://www.zephoria.org/thoughts/archives/2010/11/08/risk-reduction-strategies-on-facebook.html
boyd, d. (2010b). Social steganography: Learning to hide in plain sight. Retrieved from http://www.zephoria.org/thoughts/archives/2010/08/23/social-steganography-learning-to-hide-in-plain-sight.html
boyd, d., & Hargittai, E. (2010). Facebook privacy settings: Who cares? First Monday, 15(8), 13-20. Retrieved from http://www.uic.edu/hubin/cgiwrap/bin/ojs/index.php/fm/article/view/3086/2589
boyd, d., & Marwick, A. (2011). Social steganography: Privacy in network publics. Paper presented at Annual Conference of the International Communication Association. Retrieved from http://www.danah.org/papers/2011/Steganography-ICAVersion.pdf
Child, J. T., & Petronio, S. (2011). Unpacking the paradoxes of privacy in CMC relationships: The challenges of blogging and relational communication on the internet. In K. Wright & L. Webb (Eds.), Computer mediated communication in personal relationships (pp. 21–40). Cresskill, NJ: Hampton Press.
Child, J. T., & Westermann, D. A. (2013). Let’s be Facebook friends: Exploring parental Facebook friend requests from a communication privacy management (CPM) perspective. Journal of Family Communication, 13, 46–59. doi:10.1080/15267431.2012.742089
Christofides, E., Muise, A., & Desmarais, S. (2009). Information disclosure and control on Facebook: Are they two sides of the same coin or different processes? Cyberpsychology & Behavior, 12(3), 341–345. doi:10.1089/cpb.2008.0226
Cozby, P. C. (1973). Self-disclosure: A literature review. Psychological Bulletin, 79, 73–91. doi:10.1037/h0033950
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, 83–108. doi:10.1111/j.1083-6101.2009.01494.x
Dienlin, T., & Trepte, S. (2014). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. European Journal of Social Psychology, 45(3), 285–297. doi:10.1002/ejsp.2049
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, 1143–1168. doi:10.1111/j.1083-6101.2007.00367.x
Ellison, N. B., Vitak, J., Steinfield, C., Gray, R., & Lampe, C. (2011). Negotiating privacy concerns and social capital needs in a social media environment. In S. Trepte & L. Reinecke (Eds.), Privacy online: Perspectives on privacy and self-disclosure in the social web (pp. 19–32). Berlin, Germany: Springer.
European Commission. (2011). Special Eurobarometer 359: Attitudes on data protection and electronic identity in the European Union. Retrieved from http://ec.europa.eu/public_opinion/archives/eb/eb359_en.pdf
Greene, K., Derlega, V. K., & Mathews, A. (2006). Self-disclosure in personal relationships. In A. L. Vangelisti & D. Perlman (Eds.), The Cambridge handbook of personal relationships (pp. 409–427). New York, NY: Cambridge University Press.
Hogan, B. (2010). The presentation of self in the age of social media: Distinguishing performances and exhibitions online. Bulletin of Science, Technology & Society, 30, 377–386. doi:10.1177/0270467610385893
Hu, L., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. Structural Equation Modeling: A Multidisciplinary Journal, 6, 1–55. doi:10.1080/10705519909540118
Joinson, A. N., Houghton, D. J., Vasalou, A., & Marder, B. L. (2011). Digital crowding: Privacy, self-disclosure, and technology. In S. Trepte & L. Reinecke (Eds.), Privacy online: Perspectives on privacy and self-disclosure in the social web (pp. 33–45). Berlin, Germany: Springer.
Joinson, A. N., & Paine, C. B. (2007). Self-disclosure, privacy and the internet. In A. N. Joinson, McKenna, K. Y. A., T. Postmes, & U.-D. Reips (Eds.), Oxford handbook of internet psychology (pp. 237–252). Oxford, UK: Oxford University Press.
Joinson, A. N., Reips, U.-D., Buchanan, T., & Schofield, C. B. P. (2010). Privacy, trust, and self-disclosure online. Human-Computer Interaction, 25(1), 1–24. doi:10.1080/0737002903586662
Jourard, S. M. (1967). To be or not to be: Existential-psychological perspectives on the self (University of Florida Monographs, Social Sciences, Vol. 34). Gainesville: University of Florida Press.
Jourard, S. M. (1971). The transparent self (rev. ed.). New York, NY: Van Nostrand Reinhold.
Junco, R. (2013). Comparing actual and self-reported measures of Facebook use. Computers in Human Behavior, 29, 626–631. doi:10.1016/j.chb.2012.11.007
Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. Journal of Information Technology, 25, 109–125. doi:10.1057/jit.2010.6
Lampinen, A., Lehtinen, V., Lehmuskallio, A., & Tamminen, S. (2011). We’re in it together: Interpersonal management of disclosure in social network services. Proceeding of the SIGCHI Conference on Human Factors in Computing Systems (pp. 3217–3226). New York, NY: ACM.
Litt, E. (2012). Knock, knock. Who’s there? The imagined audience. Journal of Broadcasting & Electronic Media, 56, 330–345. doi:10.1080/08838151.2012.705195
Litt, E. (2013). Understanding social network site users’ privacy tool use. Computers in Human Behavior, 29, 1649–1656. doi:10.1016/j.chb.2013.01.049
Walther, J. B. (2011). Introduction to privacy online. In S. Trepte & L. Reinecke (Eds.), Privacy online: Perspectives on privacy and self-disclosure in the social web (pp. 3–7). Berlin, Germany: Springer.

Westin, A. F. (1967). Privacy and freedom. New York, NY: Atheneum.

Wheeless, L. R., & Grotz, J. (1977). The measurement of trust and its relationship to self-disclosure. Human Communication Research, 3, 250-257. doi:10.1111/j.1468-2958.1977.tb00523.x

Author Biographies

Philipp K. Masur (MA, University of Mainz, 2012) is a Research Assistant at the University of Hohenheim in Stuttgart, Germany. His research interests include online communication, media use, privacy, and self-disclosure.

Michael Scharkow (PhD, Berlin University of the Arts, 2011) is a Research Associate at the University of Hohenheim in Stuttgart, Germany. His research interests include empirical research methods, online communication, and media use.