Article

SM+S
social media + society

Social Media + Society
April-June 2018: 1–14
© The Author(s) 2018
Reprints and permissions:
sagepub.co.uk/journalsPermissions.nav
DOI: 10.1177/2056305118767134
journals.sagepub.com/home/sms
SAGE

Privacy in Mediated and Nonmediated Interpersonal Communication: How Subjective Concepts and Situational Perceptions Influence Behaviors

Doris Teutsch, Philipp K. Masur, and Sabine Trepte

Abstract

New communication media such as social networking sites (SNSs) and instant messengers (IMs) challenge users' privacy perceptions. Technical infrastructures and the flow of digital information lead to novel privacy risks that individuals are often not acquainted with. Users' subjective perceptions of privacy may thus be flawed and lead to irrational behavior. In this work, we investigated a concept that has been addressed only implicitly in academic research on privacy: the user's subjective perception of a given level of privacy. We examined the literature on how privacy perceptions have been conceptualized in traditional theories of privacy and how these conceptualizations are challenged in social media communication. We first qualitatively explored laypeople's privacy concepts and investigated their subjective perceptions of privacy levels and subsequent private disclosures in different mediated and nonmediated communication settings. Interviews with $N = 33$ Germans revealed that, similar to academic privacy theories, they tend to conceptualize privacy as control over social, physical, and psychological boundaries. However, trust and other-dependent privacy emerged as important novel aspects for understanding privacy regulation in online communication. We further found that individuals consistently perceived a high level of privacy in face-to-face situations and a low level of privacy in public communication on SNSs. With regard to IMs, however, their answers were mixed: Uncertainty regarding digital communication properties and audiences as well as limited control over the communication setting prevented a reliable and shared perception of the privacy level. With regard to privacy behavior and private disclosures, we found that people tend to adapt their sharing of private information to the perceived level of privacy.

Keywords

privacy, self-disclosure, qualitative interviews, face-to-face communication, computer-mediated communication, social network sites, instant messenger, social media

Social media such as social networking sites (SNSs) and instant messengers (IMs) have been largely integrated into everyday communication repertoires. Facebook, the most popular SNS, reported more than 1 billion daily active users for September 2017 (Facebook, 2017), and 1 billion people worldwide use the mobile IM WhatsApp every day (WhatsApp, 2017). Every second U.S. American is a daily Facebook user, and around 29% of smartphone users in the United States use IM apps (Pew Research Center, 2016). In Germany, 21% of the population log in to Facebook on a daily basis, and 55% use WhatsApp every day to stay in contact with family and friends (Koch & Frees, 2017; Media Impact, 2017). Communication on social media complements face-to-face conversations and other mediated forms of communication and may even reinforce communication in other channels (Dienlin, Masur, & Trepte, 2017). The properties of digital communication and in particular networked publics, however, involve privacy risks users might not be fully aware of. Hence, the level of privacy a social media user subjectively perceives when sharing private information may diverge from the actual level of privacy.

The regulation of privacy by controlling the flow of private information—as conceptualized in privacy theories by

University of Hohenheim, Germany

Corresponding Author:
Doris Teutsch, Department of Media Psychology (540F), School of Communication, University of Hohenheim, Wollgrasweg 23, 70593 Stuttgart, Germany.
Email: doris.teutsch@uni-hohenheim.de

scholars such as Westin (1967), Altman (1974), Burgoon (1982), and Petronio (2002)[1]—is challenging in social media as an appropriate perception and evaluation of the achieved level of privacy is necessary to choose behavior that leads to the desired level of privacy. Although scholars have extensively investigated individuals' self-disclosure and privacy regulation in social media, the question of how users perceive privacy levels in online communication settings and how this perception affects their behavior has remained widely unconsidered. We define a *privacy perception* as an individual's situational experience and assessment of the given privacy level (Altman, 1975; Dienlin, 2014; Masur, 2018). Contrary to privacy concerns (which have often been investigated in prior research), a privacy perception does not refer to stable negative attitudes concerning privacy in social media (cf. Dienlin & Trepte, 2015) but to a situational evaluation of a certain communication setting. Recently, Masur (2018) argued that communication research should put less emphasis on identifying differences between persons and identify the varying environmental factors that may be more influential in shaping privacy and self-disclosure processes instead.

To better understand which privacy concepts users' perceptions are built upon, we further considered *individual privacy concepts*. We define these as an individual's subjective understanding of the term *privacy*. Individual privacy concepts are rather stable cognitive representations, and as such, they are independent of specific situations. In a last step, we investigated social media users' *privacy behavior*. We were particularly interested in how subjective privacy perceptions and privacy concepts foster private disclosures in different communication settings. We therefore let our interview partners define what they considered to be private disclosures and analyzed how these were linked to privacy perceptions.

Hence, our overall research aim was to further the understanding of how individuals subjectively perceive the privacy level in different mediated and nonmediated communication settings, how these are based on subjective privacy concepts, and how both influence privacy behaviors and private disclosures. To follow up on this research aim, we investigated the everyday privacy concepts and experiences of German social media users (and nonusers) in qualitative interviews.

Privacy as a Theoretical Concept in Communication

Communication scholars most often refer to Westin's (1967) and Altman's (1975) theories as most important for laying the groundwork for the current understanding of privacy (for an overview, see Margulis, 2011). Westin (1967) defined privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about themselves is communicated to others" (p. 5). People achieve this by voluntarily and temporarily withdrawing from social interactions. In modern societies, privacy is necessary for the individual to maintain personal autonomy, emotional release, and self-evaluation, as well as limited and protected communication. According to Westin, these functions can be performed in four states of privacy: solitude, intimacy, anonymity, and reserve. The individual desire for privacy competes with other social and psychological needs and is shaped by the social and physical environment. As it changes constantly, an individual may perceive the given level of privacy as too much or too little. Although Westin does not explicitly discuss privacy perceptions, his work nonetheless suggests that the subjective perception of a given level of privacy must be regarded as a requirement for the personal adjustment process aimed at achieving a sufficient level of privacy.

Whereas Westin regarded privacy as resulting from withdrawal, Altman (1975) defined privacy as "selective control of access to the self" (p. 18). He used privacy synonymously with interpersonal boundary control through which individuals or larger social units aim to achieve a temporarily desired level of interpersonal contact. He emphasized the dialectical nature of the process that involves the regulation of input and output. Thus, Altman's concept of privacy is not only a process of withdrawing or a state of limited access. Privacy is rather an interplay of opposing forces, also including the desire to be accessible to others. One of Altman's major claims was that individuals compare their desired with their achieved level of privacy. He also called the two levels the *ideal* and the *outcome*, respectively (Altman, 1975). The ideal level of privacy is defined by the desired level of openness or closeness in a situation. Similar to Westin, Altman suggested that a boundary regulation process takes place whenever the achieved level of privacy is perceived as failing to match the desired level of privacy. Although Altman likewise did not explicitly refer to privacy perceptions as a prerequisite for privacy regulation processes, his concept implicitly necessitates that individuals subjectively assess the given level of privacy in any situation to evaluate it against their desired level of privacy.

Burgoon (1982) built on Westin's (1967) and Altman's (1975) work to answer the question of whether there are "different kinds of dimensions of privacy that have implications for communication" (p. 206). She suggested four interrelated dimensions of privacy: the ability to control physical, interactional, psychological, and informational access to oneself or to one's group. On the physical dimension, individuals regulate the degree of surveillance as well as physical access to their personal space. The interactional dimension of privacy encompasses autonomous engagement in or withdrawal from social encounters. The psychological dimension involves individuals' ability to prevent intrusions upon their cognitions and feelings. Finally, informational privacy is the ability to control the gathering and disseminating of information about the self (Burgoon et al., 1989). Burgoon (1982) emphasized the subjective nature of privacy and the role of an individual privacy perception as she stated that the "degree of privacy in any given situation is therefore dependent on each individual's interpretation of the situation" (p. 211).

With her communication privacy management (CPM) theory, Petronio (2002) further refined Altman's (1975) privacy concept of selective control. CPM offers a rule-based conceptualization of the mental calculus underlying the decision to hide or release private information. Central to the CPM is the ownership principle, which postulates that individuals see themselves as the owners of their private information from which they derive a right to control the flow of it. The sharing of private information is based on privacy rules that are driven by expected benefits and costs. Once an individual grants others access to private information, they become co-owners. Collective privacy rules, which are mutually agreed upon by the original owner and the co-owners, regulate how they further share or keep the disclosed information. According to Petronio, co-owning individuals manage privacy boundaries by applying *permeability rules*, which determine how much is shared; *linkage rules*, which determine who gets to know the information; and *ownership rules*, which determine how much control co-owners have over the private information. If co-owners fail to coordinate the privacy rules, CPM theory predicts *boundary turbulence* (i.e., privacy violations), which requires a recalibration of the established rules. Privacy perceptions, although not explicitly referred to as such, are relevant for privacy rule development. The perception of the physical setting and the social environment as safe and trustworthy are relevant criteria for rules of boundary regulation (Petronio, 2002).

Inherent to all the theoretical privacy concepts discussed here is the idea that individuals or larger social units achieve privacy by controlling access to information. Depending on the perceived level of privacy, individuals apply rules or choose behaviors in order to achieve and maintain their desired level of privacy. Although only Burgoon (1982) explicitly included the perception of the level of privacy in her concept, subjectively perceiving privacy and reacting accordingly must be regarded as the fundamental mechanisms of all privacy concepts.

Social media challenge this privacy mechanism in two ways. On one hand, unknown and invisible privacy risks impede a valid perception of the actual (or achieved) privacy level in communication settings. On the other hand, the infrastructure and properties of digital media limit individuals' capabilities to control the flow of personal information efficiently. In social media, the behaviors used to implement a desired level of privacy are somewhat limited. The changes that new communication media have brought for privacy management in everyday life demand a theoretical examination of privacy that takes these altered circumstances into consideration (Papathanassopoulos, 2015).

Theoretical Approaches to Privacy in a Social Media Era

Since social media's popularity has boomed, the means for interpersonal communication and privacy and data protection have re-emerged as topics of interest. Various applications collect, store, and process a variety of data about users, often without their awareness or the opportunity to opt out. Consequently, communication scholars have investigated how individuals manage their privacy in social media (boyd, 2008a; boyd & Hargittai, 2010; Gross & Acquisti, 2005; Joinson & Paine, 2007; Masur, 2018; Papacharissi, 2010; Trepte, Dienlin, & Reinecke, 2014; Trepte & Reinecke, 2011; Tufekci, 2008). Such research has given first insights into how the digital environment, social constellations, and individual needs challenge privacy perceptions and privacy regulation in social media.

On the basis of these previous studies, we found three aspects that most crucially influence and complement privacy theories. First, in social media, the *concept of audience* is different than in face-to-face communication. Social media audiences are potentially large and unknown and cannot be physically perceived (Litt, 2012). Beyond other users, the audiences include service providers, surveillance agencies, and other third parties that typically do not exist in nonmediated communication settings. In most privacy theories, communication partners are usually referred to as *others*. Altman (1975) summarized that privacy involves "individuals, families, mixed and homogeneous sex groups, and so on" (p. 11). Similarly, in Westin's (1967) and Petronio's (2002) privacy theories, it is assumed that individuals have a general idea of who *the others* are and that one can communicate with them. While communicating in social media, potentially unknown audiences may impede an accurate evaluation of the given level of privacy.

Second, digital data are *persistent, replicable, searchable*, and *scalable*, and information addressing a defined circle of recipients might spread further than expected or intended (boyd, 2011; Palen & Dourish, 2003). Most of the privacy theories consider the transfer of information: Petronio (2002), for example, argued that information transfer is negotiated between co-owners. The properties of social media undermine the rules established in negotiations because users sometimes unintentionally spread co-owned information beyond the agreed-upon boundaries. Social media are designed to potentiate information sharing. Thus, a heightened scalability has to be taken into account. Yet, not every user is aware of these characteristics or the fact that he or she might come along with privacy risks. Thus, users may have an inaccurate perception of the actual level of privacy in social media.

Third, multiple physical contexts with distinct behavioral norms that used to be separated by temporal, spatial, and social boundaries converge in social media. This *collapsing of contexts* causes privacy tensions, especially in one-to-many communication (Binder, Howes, & Sutcliffe, 2009; boyd, 2008b, 2011; Palen & Dourish, 2003). This is a fundamental challenge for privacy management in social media for which the traditional theories of privacy provide an adequate theoretical framework only in part.

In sum, the properties of social media require privacy regulations that are vastly different from offline settings in terms of audiences, access, and boundary control. Marwick and boyd (2014) found that social media users need to establish collective practices in order to safeguard their privacy. On the basis of these observations, they proposed "a model of privacy that is networked" (p. 12). This model requires an understanding of the technological and social peculiarities of social media contexts as well as shared social norms over information sharing. Although we agree that a contemporary understanding has to regard privacy as a collective endeavor, we suggest that a better understanding of how it is established in concrete situations is needed. As supposed by Altman (1974), Westin (1967), Burgoon (1982), and Petronio (2002), the properties of digital communication and online audiences challenge users' ability to properly perceive privacy levels and effectively control the flow of private information. Thus, there is a need to adapt the conceptualization so that privacy perceptions and behavior can be investigated adequately in a digitalized world.

Gaining a refined understanding of laypeople's *privacy concepts* is a prerequisite for investigating their *subjective perception of privacy* levels in different communication settings. Knowing what privacy means to them allows us to develop a refined understanding of the cues and conditions that determine the perception of a given level of privacy. Hence, we explored individual privacy concepts in qualitative interviews and asked the following research question:

RQ1. How do individuals conceptualize privacy today?

How Individuals Perceive Privacy in Mediated and Nonmediated Settings

So far, scholars have investigated people's privacy concerns, attitudes, and behaviors (e.g., Barnes, 2006; Taddicken, 2014), but there is hardly any research on how people perceive different levels of privacy in mediated and nonmediated communication settings. To distinguish privacy perceptions from related concepts such as privacy concerns, we define privacy perceptions as individuals' situational experiences with and assessments of their given privacy level. This implies that privacy perceptions can differ greatly among individuals (Dienlin, 2014). The perception of the given level of privacy is necessary in order to decide whether it needs to be adjusted or whether it is already optimal (Altman, 1975; Burgoon, 1982).

In order to determine how people experience and assess privacy perceptions, we are interested in the situational cues and conditions that determine privacy perceptions in various mediated and nonmediated communication settings. Burgoon (1982) suggested several factors for distinguishing privacy perceptions. According to her, the perception of physical privacy depends on the extent to which an individual can control access to the surrounding space and on the freedom of surveillance and the number of sensory channels through which access to the self is possible. A space is perceived as more private when it allows for seclusion and when the probability of intrusion is low. Factors determining perceptions of interactional privacy include the degree of control over communication partners and the frequency, length, and content of interactions. The perception of psychological privacy depends on the perceived freedom from the influence of others on cognitions and emotions and the ability to conceal thoughts and feelings. When both are low, one does not perceive a high level of privacy. Finally, the perception of informational privacy depends on the degree of control over the initial release of information and its subsequent distribution and use. Additional factors refer to the amount of information known by others and the number of people who have access to it. As Burgoon had defined privacy perception two decades before social media emerged, her theory does not yet include factors that might explain differences between the perception of privacy in mediated and nonmediated communication settings. Nonetheless, her abstract systematization of situational cues that might lead to a higher or lower perceived level of privacy may still be useful in understanding the potential of social media properties for shaping users' privacy perceptions.

Although the term privacy perception has sometimes been used interchangeably with privacy concerns or privacy attitudes in the literature, we want to emphasize that we consider them to be different concepts. The focus of this work is on privacy perceptions in terms of a situational experience and the assessment of privacy in mediated and nonmediated communication settings. Thus, we do not focus on overall attitudes or concerns. Moreover, no systematic comparison of privacy perceptions in mediated and nonmediated communication exists so far. We therefore asked the following research question:

RQ2. What do people perceive the level of privacy to be in mediated and nonmediated communication settings?

How Individual Privacy Perceptions Influence Self-Disclosure

Privacy perceptions as defined in the preceding section are important for assessing whether the given external conditions allow for the disclosure of private information (Masur, 2018). Self-disclosure has generally been defined as sharing information about the self with other humans (Cozby, 1973; Wheeless & Grotz, 1976). An individual's decision to disclose depends on the perception that one is in control of the kind of information that is shared and with whom. If an individual perceives that a communication setting is not private enough for sharing personal information, people will regulate their privacy by not divulging personal details (Derlega, Metts, Petronio, & Margulis, 1993). Early evidence was provided by Fidler and Kleinknecht (1977), who interviewed female college students on stigmatizing information. They found that they received more responses to the most sensitive questions when the interview technique guaranteed a high level of privacy.

The emergence of computer-mediated communication in chatrooms and online discussion forums has stimulated research on online self-disclosure patterns. A major finding was that study participants who perceived privacy in an anonymous setting disclosed significantly more sensitive information than they did in similar offline interactions (Joinson, 2001; Tidwell & Walther, 2002).

When social media, especially SNSs, replaced anonymous means of online communication, scholars focused on the influence of privacy concerns—a concept related to privacy perceptions—on self-disclosure (Dienlin & Trepte, 2015; Krasnova, Spiekermann, Koroleva, & Hildebrand, 2010; Taddei & Contena, 2013; Taddicken, 2014; Tufekci, 2008). Masur and Scharkow (2016) found that users tended to refrain from sharing information they subjectively perceived as private. Accordingly, posting particularly intimate information publicly was evaluated as inappropriate, a finding that was confirmed by a content analysis of status updates on SNSs (Bazarova, 2012). Studies have found that sensitive information tends to be shared in communication settings that are perceived as allowing a higher level of privacy, for example, email or instant messaging (Bazarova & Choi, 2014; Burkell, Fortier, Wong, & Simpson, 2014; McLaughlin & Vitak, 2012; Utz, 2015). Based on an experience sampling study with $N=164$ smartphone users who engaged in $N=1{,}104$ disclosure events, Masur (2018) showed that the environmental circumstances within a communication application allow for the prediction of the depth of self-disclosure. More specifically, the findings revealed that the depth of self-disclosure increased in situations in which the audience size was small (e.g., IM conversations) and potential respondents were considered as trustworthy and psychologically close. Similarly, Frye and Dornisch (2010) measured perceived privacy in terms of the perception of not being overheard or read by unintended audiences and the willingness to self-disclose on 32 topics across 10 communication settings. The results again showed that participants were more willing to self-disclose information when using a communication tool that was perceived to provide a high level of privacy.

So far, we have gained insight into how people adjust communication content with respect to public and private means of communicating on SNSs, and there is convincing evidence that privacy perceptions and self-disclosure are positively correlated for various communication settings. For our study, we followed up on Frye and Dornisch's (2010) systematic approach and explored how privacy perceptions in different mediated and nonmediated communication settings influence the disclosure of private information. We specifically focused on disclosures that the individual refers to as *private*. As privacy attributions for topics or types of information vary considerably between individuals (Masur & Scharkow, 2016), we did not classify information as private a priori but left it open to our participants to come up with an experience involving private disclosures. Thus, we sought to understand how privacy perceptions impact the kind of private information users disclose and how they communicate about it.

> *RQ3*. How do privacy perceptions in different mediated and nonmediated settings influence private disclosures?

Method

Procedure and Participants

We used qualitative interviews to obtain a fine-grained understanding of people's subjective privacy concepts and a contextualized understanding of privacy perceptions and private disclosures across different communication settings. To do so, we recruited a convenience sample of 33 German participants. We invited them via university mailing lists and postings in public buildings on campus and in surrounding residential areas. In addition, we contacted the principal of a comprehensive school to arrange the participation of 12 ninth graders who had all obtained their parents' informed consent. The participants were between 14 and 78 years old (16 females, 17 males). Table 1 (in the Supplementary Material) presents more information on occupations and media use.

Interview Procedure and Data Analysis

The critical incidents technique (Flanagan, 1954), which was developed to gather facts about behavior in predefined situations, was used to design the interview questions. After a warm-up question, we asked participants to remember and describe a recent situation involving a private disclosure. Our aim was to let the participants decide for themselves what they considered private disclosure. The participants' initial description of this situation was followed by questions concerning their perception of privacy and of their own and their conversation partners' behavior. Depending on the initial description, we further asked whether the participants could also remember a situation in which they shared private information with the same person via social media or in a non–social media setting, respectively. For the first 21 participants, we left it up to them whether they began by describing a mediated or nonmediated conversation. As the majority first described face-to-face conversations and had trouble remembering a recent social media interaction with the very same person, we directly asked the remaining 12 participants to describe a social media conversation and then moved on to a non–social media setting with the very same person. After the description of both situations, we prompted them to compare their behaviors and privacy perceptions in the two situations. Finally, we asked them about their social media use and their subjective definition of privacy. Three trained interviewers conducted the interviews from March to May 2014 in person in a room on campus. The interviews lasted between 10 and 63 min. Each participant received an incentive of 10 Euro cash after the interview.

The interviews were digitally recorded and transcribed. Using the qualitative data analysis software MAXQDA, we performed deductive and inductive qualitative data analyses. In a first step, we created a coding scheme with categories derived from our initial research questions. In a second step, we refined the coding scheme as we read the interviews for the first time by augmenting and subdividing the categories according to aspects mentioned in our interviewees' descriptions. We then used the refined coding scheme to code all interview data in a third step. Finally, we aggregated the statements extracted for each category across participants in order to identify patterns, similarities, and differences.

Results

Subjective Concepts of Privacy

In the following, we first present the results for RQ1 and refer to our interviewees' *subjective concepts of privacy*. The findings we report are mainly based on the responses to the interview question: How would you define privacy? These responses were further complemented by insights from the critical incidents of private disclosures.

A first finding was that people conceptualized privacy as having two semantic levels. On one hand, participants presented privacy as a property of topics and territories. On the other hand, they described privacy as a boundary or state that allows certain behaviors.

Private Topics and Territories. Most topics that interviewees considered private can be classified as information about the self, including feelings, thoughts, opinions, family affairs and romantic relationships, problems of any kind, professional and private aspirations, personal achievements and experiences, health conditions, one's financial situation, and sexual orientation. The participants considered loved ones such as family members, friends, or romantic partners to be private aspects of their lives. Moreover, holding hands and tattling on someone are behaviors that were labeled as private. Some of our interviewees offered only abstract ideas about private topics, whereas others identified them precisely. Isabelle (29)[2] described privacy as "everything that is hidden, [. . .]. What you can't see at first sight." Accordingly, she stated that nothing is more private than her thoughts, whereas anything that can be witnessed, for example, her job, is not private. Alisa (15) described privacy as "that not everyone knows my name, where I live, what I do and who my friends are," and Simon (23) defined privacy as "things or information that affect me or others, which should not or must not be known by anyone."

Participants also considered certain territories (places people claim as property) as private. For example, the home, a teenager's room, and a student's dorm room were perceived to be very private as they reveal a lot about their inhabitants. Furthermore, teenagers in particular referred to their cell phone and the messages they exchange on it as private.

Privacy as a Social Boundary. A dominant aspect of our interviewees' privacy concepts was the existence of boundaries for sharing personal information. Participants used terms such as frame, sphere, or circle to circumscribe privacy. These terms convey the idea of a closed unit and the possibility that it could include or exclude people, thus resembling Altman's (1975) and Petronio's (2002) concept of privacy as boundary control.

The most important criterion of these boundaries was identified as the people who are included or excluded. Some participants claimed that they felt they had their privacy only when this boundary included no one but themselves. For example, Erna (78) described privacy as keeping information to herself and not sharing it at all: "To me, privacy basically is, well everything that is really of my concern only [. . .] and there is a lot in everyday life that I want to keep to myself." By contrast, Mona's (22) concept included others with whom she shares everything:

> Well, for me, privacy is, on the one hand, that I'm either alone, well, that there are things for me only that I want to keep to myself, or privacy for me is as well that there are persons with whom I share everything, from whom I don't keep any secrets when we are together—that's also a kind of privacy for me.

Similar to Mona, most of the participants defined privacy as a bounded sphere that is limited by the persons with whom they intend to share information. The concepts of privacy as keeping information to oneself or sharing it with intimate others resembled two of Westin's (1967) states of privacy: reserve and intimacy.

The people who were included in the boundaries of privacy depended on relational closeness. Friends, especially close and best friends; spouses; life partners; and family members were generally considered appropriate for sharing private matters with. These trusted persons were identified as central to people's subjective privacy concepts. However, whether or not a person would be included within the boundaries of privacy was also described as depending on context. Two participants pointed out that they felt fine about sharing private information with the interviewer because they trusted in the scientific purpose of the interview. Yet, the quality of privacy would be different with a person they knew very well.

Privacy as a Physical Boundary. As mentioned earlier, some of our interviewees stated that they regard their family's home or a room with a door as private spheres. They explained that these spaces provide physical seclusion and allow them to enjoy the intimacy of their family or being by themselves. Fabian (23) stated that the physical privacy provided by his room permits him to withdraw from social interactions:

> . . . privacy is, for example, my home. I have a small room anyway, and I used to have many guests. I'm in touch with so many people, with the club, that's why I'm happy to have that room, and I'm able to withdraw.

Christina (24) emphasized the freedom from surveillance provided by physical boundaries: "Yes, to me privacy is when I can decide what I'm doing without having someone look over my shoulder somehow or restrain me from what I'm doing or knowing what I'm doing." However, participants stated that a space does not have to be owned or have concrete physical barriers (e.g., walls and doors) to function as a private sphere: They stated that it was crucial that others could not overhear a conversation, particularly not those who should not gain knowledge about personal details or those who were the subject of the conversation.

Privacy as Access Regulation. The management of boundaries was another aspect that was inherent to most of the subjective definitions of privacy. Although only one participant actually used the word *control*, most of them expressed the need to restrict access to information and the transfer of personal information. This finding is consistent with a recent study by Sarikakis and Winter (2017), who found that social media users' concepts of privacy revolved around the notion of control and constraint. One aspect of information control is the need to determine what becomes known about oneself to whom, which was expressed in Daniel's (27) privacy definition:

> Privacy to me means that I can decide what someone learns or knows about me, that it is my decision to whom I give what information, or that I know that this information is given to that person, that I can judge who knows what and how.

This idea is in line with Petronio's (2002) concept of privacy management: People seem to believe that they own information about themselves and should hence be able to decide who is allowed to know about it. In relation to this, several interviewees also mentioned that they do not want others to actively seek information about them when they want to keep such information private. This has also been referred to as spying on someone. In sum, the answers showed that regulating access to the self is an important part of privacy.

Privacy as a Form of Self-Determination. Another aspect raised by the interviewees referred to informational self-determination. They expressed the need to prevent the emergence of an unfavorable impression of oneself and to determine how one is seen and evaluated by others. This can be achieved only by maintaining control over the flow of information. Elena (30), for example, pointed out that she does not want someone who holds a different view than her to retell her opinion without giving her the opportunity to justify herself.

Privacy Through Trust. Most participants admitted being aware that they lose control the moment they share personal information with one or several others. This might explain why they did not use the term control but defined privacy as a state of *being certain* that information that had been shared with particular people was not transmitted to anyone else. Alexander (27) formulated this certainty: "Well, privacy to me is actually one's own certainty that particular information or actions simply stays within the circle of people whom one thinks should know about it—that it is not passed to third parties." One way to gain this certainty is to deliberately choose with whom to share personal information. For this decision, it is crucial to know whether the person can be *trusted*. Terms such as trust, to entrust, and trusted were frequently used to describe the nature of relationships that provide certainty for privacy. As Johann (77) put it, "Well, privacy is absolute trust between conversational partners and . . . absolute, absolute certainty that the subject of conversation will stay within this sphere." The importance of interpersonal trust that became apparent in the interviews has not been incorporated in seminal theories of privacy so far.

Subjective Perceptions of Privacy and Subsequent Disclosures

To answer RQ2 and RQ3, we analyzed participants' descriptions of critical incidents involving private disclosures to first identify perceptions of privacy (RQ2) and then how these are related to private disclosures (RQ3). As a first result, for RQ2, we identified five communication settings in which private matters are discussed. These differed in terms of perceived privacy: (a) face-to-face communication in dyads or small groups; (b) phone calls or video chats in dyads; (c) face-to-face communication in large or heterogeneous groups; (d) online messages such as email, Facebook messenger, or messenger apps such as WhatsApp; and (e) semipublic or public online interactions such as status updates on SNSs or comments on online discussion boards.

In the following paragraphs, we first answer RQ2 by showing how the privacy perceptions in these five settings differed and by elaborating on characteristics that determined participants' perceptions of privacy. We point out the significance of interpersonal trust, which emerged as a crucial requirement for achieving privacy. The results for RQ3 are presented in the same manner by referring to each setting to demonstrate how a certain perception of privacy (RQ2) is related to subsequent private disclosures (RQ3).

Face-to-Face Communication in Dyads or Small Groups. Participants stated that they prefer the face-to-face setting for private communication as the audience usually ranges from one to a few deliberately chosen and trusted individuals, and the physical presence of all participants allows them to effectively implement strategies to achieve and maintain an optimal level of privacy. However, they also explained that they tend to manage physical and social boundaries in face-to-face communication by excluding unintended audiences. They explained that they can achieve this by meeting in protected spaces such as in a bedroom. However, they noted that privacy can also be found in the anonymity of a crowded city center, in a quiet corner of a café, or during a walk in the park.

Participants stated that—better than any other communication setting—face-to-face conversations allow for empathy and emotional support expressed through verbal, paraverbal, and nonverbal communication. Thus, they explained that they openly discuss private topics in dyads and small groups, and they appreciate the opportunity to give and receive immediate feedback on private disclosures. Participants agreed that conversations typically involve the disclosure of emotions and problems with family, friends, relationships, school, or job, and that they share feelings and thoughts, personal experiences, and moral and religious beliefs in face-to-face conversations.

Phone Calls or Video Chats—For Example, via Skype. Participants tended to agree that they perceive conversations on either media channel as private as long as communication partners are alone on each side. They explained that they establish this protected sphere by assuring each other that no one else is listening. However, as one cannot be entirely sure that nobody can overhear the conversation at the other end of the phone, participants identified trust in the communication partner as vital for perceiving the situation as private. Moreover, they explained that when receiving a call on a mobile phone, they might be caught in a situation in which they are surrounded by known or unknown others. In such a situation, they did not perceive privacy as guaranteed, and they would have to manage social or physical boundaries by seeking seclusion or postponing the conversation. The perception of privacy was also based on the fact that these technologies allow for paraverbal, and in the case of video chats, even nonverbal, communication that is considered central for private disclosures as it enables people to express and perceive participation, empathy, and mutual understanding.

They explained that the perceived high privacy level of phone calls and video chats entails pleasant and comprehensive private conversations. Hence, participants admitted that they would discuss private matters here as openly and extensively as they would in dyadic face-to-face conversations.

Face-to-Face Communication With a Vast or Heterogeneous Group. Participants explained that they do not perceive face-to-face communication with a group as guaranteeing privacy or as adequate for private disclosures. They stated that this perception is invoked by audience size and composition, particularly when others who should not know about a private issue are present. However, they further explained that individuals are able to visually perceive the audience and that, even though it takes more effort compared with small groups, people can engage in boundary management (e.g., by seeking seclusion with selected members of the group).

Participants admitted that, as a consequence of the perceived lack of privacy, they tend to avoid personal disclosures when surrounded by a large and heterogeneous group. They explained that this particularly applies to very private issues such as sexual orientation or opinions about a controversial topic.

Instant Messenger Communication. Participants revealed that they perceive and assess privacy differently in this setting. Whereas some evaluated it as adequate for private disclosures, others expressed ambivalent perceptions, and some participants even stated that there is no privacy at all. Although most of the participants reflected on the risks and limitations of written digital communication, this awareness did not impact their privacy perceptions equally. In messenger communication, the perception of privacy was based on the properties of digital communication and on the social and physical communication settings. Most users admitted to being aware that the information they share via email or messenger apps may be recorded and may persist for an immeasurable period of time. Consequently, they expressed that the potential digital audience is elusive as it might include unintended users, the online service provider, or commercial and governmental institutions. Some users stated that they find social boundary management impossible and perceive privacy as insufficient as they cannot know and control who has access to the information they share digitally. Although they expressed that they generally trust the intended receiver of a private message, they stated that they could never be sure whether a third party will have access to the digitally recorded conversation. Here, the awareness of the risks emerging from digital communication exceeded interpersonal trust.

Nevertheless, some participants explained that they perceive privacy as adequate in messenger communication despite their awareness of surveillance practices and the replicability of digital data. These users expressed confidence that their messages were being read by the intended receiver only. This is why Alexander (27) stated that he feels fine about private disclosures when sending Facebook messages to a friend: "We just write personal messages. And you don't think any further that someone could intercept them. For us it is like: The message is sent to him, and the response comes back to me."

A substantial reason given for the perception of low privacy, however, was the limited range of forms of expression in written digital communication. Participants explained that the lack of paraverbal and nonverbal communication and immediate feedback impairs privacy decisively. Most bewailed the impersonality of written online communication and agreed that this communication setting is always inferior to face-to-face conversations or phone calls. Christina (24) stated, "Although the content is the same as when I talk to her face-to-face, somehow, I don't know, the feeling is still different when I'm texting."

Moreover, our participants also stated that they take into account the social and physical settings surrounding individuals while writing messages. Those who viewed privacy as insufficient pointed out that they could never be sure whether their communication partner was alone. Compared with phone calls, an undesired third party's access to the conversation was identified as even more difficult to perceive. Only those with a great deal of trust in their conversation partners perceived a high level of privacy in messenger communication.

In sum, whereas some of our interviewees stated that they experience a loss of control when disclosing private information via email, Facebook messenger, or WhatsApp, others expressed that they perceive these settings as adequate for private disclosures. This minority of unconcerned users stated that they discuss private matters via messengers as they would in face-to-face meetings. We found that an ambiguous perception of privacy when communicating via online messages could lead to rather superficial communication or to the initiation of phone calls or personal meetings. Mona said that she provides her mother with information on vegetarianism via email, but they discuss Mona's decision to become a vegetarian on the phone or face-to-face only. An additional consequence of an ambiguous perception of privacy is that vulnerable information is excluded from email and messenger communication, whereas one's current state of mind, relationship problems, or career decisions seem appropriate. The ambiguity of privacy perceptions can also be rooted in an inconsistency between the general awareness of privacy risks and an adequate privacy perception in the specific communication situation. As the latter seems crucial for the decision to share private information, participants sometimes admitted to forgetting about their concerns and disclosing private matters without hesitation. Like several participants, Julia (19) reflected on this inconsistent behavior in the interview: "You write private stuff, although you know that it's not actually right. But I don't have a feeling of being spied on in that moment. Actually, I do feel safe." We found that the willingness to disclose private information instead depended on a user's need for disclosure, trust in the communication partner, and the availability of alternative communication channels. Sometimes participants admitted to discussing private matters even when they did not perceive the level of privacy as adequate because either a private issue was introduced by the communication partner (e.g., in the situation Thomas [23] described, an acquaintance disclosed the death of his grandfather while they were chatting on Facebook) or the need to share private information was so strong that the perceived lack of privacy was secondary.

Reflecting on their disclosure behavior, participants stated that they use messengers to check what others are up to, share enjoyable media content, arrange face-to-face meetings, and coordinate tasks or activities. They explained that they feel that truly private conversations are the exception rather than the rule.

Public Interactions on SNSs or Discussion Boards. Most participants perceived SNSs and discussion boards as public. None of our interviewees viewed these media settings as adequate for private disclosures, thus confirming previous findings (Bazarova, 2012; Bazarova & Choi, 2014; Masur & Scharkow, 2016). They stated that the audience does not seem trustworthy, and they cannot effectively manage the social boundaries of privacy. Consequently, they explained that they would never use status updates and comments for private disclosures. They evaluated the act of publicly sharing feelings and other private information as inappropriate.

Participants reported that they perceive all reported instances of private disclosure in these social media settings as privacy violations. Emanuel (16), for example, was embarrassed by a family picture his mother tagged him in on Facebook, and Greta (16) felt bullied by a classmate's status updates. In these two cases, private information had become accessible to a vast audience before the affected person could prevent the privacy violation. The effort that was necessary to restore social boundaries varied. Although Emanuel had failed to ask his mother not to upload the photo to Facebook, he could at least untag himself and end the connection between his profile and the picture. Greta had to talk to her teacher and her classmates to stop the bullying on Facebook, and she successfully asked her adversary to delete all the mean posts. These instances of disclosure in semipublic online settings show that effective privacy management is almost impossible, and it can take some effort to restore one's privacy after a violation.

Participants said they rarely write status updates or posts in public groups and only if they intend to share information with their entire network. Among our participants older than 30 years, only Monika (58) stated that she occasionally shares links to special online content with her private virtual network, and Uwe (57) sometimes uploads landscape photos he took. Pupils and young adults admitted that they sometimes post achievements such as having passed their driving test or links to interesting and funny online content on Facebook, which they do not consider private.

The comparison of privacy perceptions in different communication settings illustrates the significance of trust for the experience of privacy. Although trust is a quality of the relationship between communication partners, its function for the achievement of privacy is prevalent in mediated communication settings where individuals are not fully in control. When sharing private information via messenger apps, the sender can never be entirely sure that the addressee is alone or will hide a message from unintended readers. Interviewees reported lowering this risk by explicitly asking their confidants not to share the information with anybody. This alludes to CPM theory, which suggests that people imply linkage rules, which determine who is allowed to know about private information. However, trust emerged as a central element of subjective privacy concepts relevant for the perception of privacy levels and resulting behaviors. Its increased importance in mediated communication suggests that trust should be the core of an updated academic privacy concept for the digitalized world.

Discussion

With the work presented in this article, we pursued the aim of increasing the understanding of *privacy perceptions*, a concept that is implicitly part of all academic privacy theories but has not received much attention in research on online privacy. A central finding of our study is that people's privacy perceptions in social media are still determined by the same *types* of cues that Burgoon (1982), for example, had already systematized much earlier but that the accessibility of cues has changed tremendously. For example, whereas access to private information is protected by walls and doors in face-to-face situations, it is now protected by privacy settings or even the infrastructure of the respective online environment. Physical barriers are easy to perceive and can thus be evaluated with regard to their potential to provide privacy. By contrast, digital barriers cannot be perceived in the same way. Individuals have to possess a certain amount of knowledge and access this knowledge in relevant communication situations in order to adequately evaluate the given level of privacy. Recent work on the role of online privacy literacy provides further evidence for such a claim (Masur, Teutsch, & Trepte, 2017; Park, 2013). It is hence not surprising that our study revealed that trust is a central factor for both, the individual perception of privacy levels in different mediated and nonmediated communication settings and for laypeople's subjective privacy concepts. Trust becomes a "risk mitigator" in environments in which the actual evaluation of its specific properties becomes challenging. Hence, we suggest that trust should be at the heart of a renewed privacy concept that accounts for the achievement of privacy in social media communication.

On the basis of the interviews, we further identified five communication settings in which private information is generally shared but that differs greatly regarding the perceived level of privacy: (a) face-to-face communication in dyads or small groups, (b) phone calls or video chats in dyads, (c) face-to-face communication in large or heterogeneous groups, (d) online messages such as email or IMs, and (e) semipublic or public online interactions on SNSs or online discussion boards. We found that the perceived level of privacy in these communication settings depended on a number of criteria that refer to social boundaries (audience size, interpersonal trust), physical boundaries (the existence of environmental artifacts for the protection of privacy), and the nature of communication (nonverbal, paraverbal, immediacy). Although subjective privacy perceptions varied from person to person, it is remarkable that participants nonetheless expressed consistent privacy perceptions across four of the communication settings. We found disagreement only with regard to the perception of the privacy level in IM communication.

As a main finding of our study, we hence suggest that privacy perceptions in small-group face-to-face encounters, phone calls and video chats, as well as encounters in large heterogeneous groups and public communication in social media (i.e., the four settings in which we found consistency) have undergone a process of *norming*. We believe people have developed and now share common norms that guide and regulate an appropriate flow of information in these settings. The first two communication settings are commonly perceived as private, resulting in the expectation that private matters can be openly discussed. The latter two communication settings are not perceived as private, and private disclosures are consequently avoided. The norming of privacy perceptions in these settings may have evolved from typical experiences, from similar socialization processes, and, in the case of public communication on SNSs, from mass media's consistent framing of SNSs as a risk for security and informational self-determination (Teutsch & Niemann, 2016).

However, with respect to messenger communication, privacy perceptions were divergent: Some of our interviewees perceived this communication setting as private, some did not see it as suitable for private communication, and others reported ambivalence. This divergence also held true for the behavior shown in these settings: Not all people who perceived messenger communication as ambiguous or as not private avoided sharing private matters. Hence, privacy perceptions in messenger communication do not yet conform to commonly shared norms. We argue that they are still in a phase of *storming*. Communicating via IMs is still relatively new, yet for many people, it offers a convenient and exciting way to interact with others. Users are exploring this new realm of online communication and have not yet formed a set of privacy rules. This may be due to the nature of messenger communication. On one hand, most people perceive the usually dyadic or small-group conversations as private and protected. The audience size seems manageable, and social boundaries of privacy seem to be under control. On the other hand, users are aware of the risks evoked by the persistence and replicability of digital communication and the surveillance practices of service providers. In addition, privacy and data protection practices of the most popular messenger app WhatsApp change frequently. For example, the originally independent company WhatsApp, Inc., was acquired by Facebook in 2014. Although all WhatsApp conversations are end-to-end encrypted, in August 2016, WhatsApp announced that it would start to connect the service with Facebook and share account information. Consequently, users are uncertain about whether their communication will be protected and secure. As the massive use of messenger apps is a relatively new communication habit, we assume that over time, users will have many experiences and negotiations. Hence, privacy perceptions will also undergo a process of norming.

The challenge and uncertainty of forming a reliable perception of the level of privacy in mediated communication were also reflected in our participants' subjective privacy concepts. On one hand, they referred to aspects of privacy that have been described in academic privacy theories—namely, self-determination, access regulation, and the management of social and physical boundaries—but on the other hand, they added new aspects to these privacy concepts that are crucially influenced by social media use. With regard to subjective concepts consistent with academic approaches, participants often claimed that they wanted to determine for themselves how other people see them or think about them—resembling Westin's (1967) concept of privacy. They further expressed that privacy is about managing access to the self within certain social and physical boundaries. This idea of privacy as access control was clearly reflected in Altman's (1975) theory of privacy and in Petronio's (2002) CPM. Physical and social boundaries were outlined by Burgoon (1982) and later Petronio (2002) with an emphasis on how these boundaries are negotiated and managed. A crucial enhancement of our academic understanding of privacy in the digital age is interpersonal trust, which our interviewees repeatedly referred to as an important requirement for perceived privacy. In the age of social media, when controlling the flow of information is not feasible, trust seems to have gained enormous importance. The seminal theories of privacy have not yet explicitly incorporated the concept of trust. However, more current conceptualizations, and especially empirical studies on online privacy, refer to trust as an important variable (Krasnova et al., 2010; Masur, 2018; Miltgen & Smith, 2015; Taddei & Contena, 2013). In this sense, interpersonal perceptions of trustworthiness determine the level of privacy that is experienced. In support of this, Masur's (2018) analysis of varying disclosure situations showed that depth of self-disclosure was indeed positively correlated to interpersonal assessments including interpersonal trust and psychological closeness. Despite such interpersonal evaluations, however, the risk that even trusted people might divulge what they should have kept to themselves remains. This risk seems to be particularly problematic if private communication is mediated. By sharing private information via messenger apps, the senders can never be entirely sure that the addressees are alone or that they are hiding their messages from unintended readers.

In sum, trust—a concept that was widely overlooked in early privacy research but is being considered more often in current studies—becomes more and more important for the definition of privacy. It is best understood as a boundary condition of privacy: Only if I trust the recipients of my disclosures will I experience privacy. For a novel privacy concept, not only is the interpersonal trust that was emphasized by our participants crucial but so is trust in online service providers and in the security of digital communication applications. As individual access regulation and control over personal data are hindered in social media, opting for trustworthy communication channels is a meaningful way to achieve and maintain privacy. Analogous to the above framed boundary condition, people experience privacy only if they consider a communication setting to be trustworthy, which involves trust in technology and service providers in social media communication. However, trust is not always well informed but may rely on heuristic information processing (Joeckel, Dogruel, & Bowman, 2016). It is thus inextricably linked with privacy perceptions and privacy behavior, and should always be considered a theoretical component of privacy.

Limitations

As the insights of our study were based on 33 qualitative interviews, they might not be exhaustive. Although the aim of our qualitative study was not generalization but theory development, a larger sample could yield additional privacy concepts and more diverse privacy perceptions and behaviors.

Furthermore, privacy concepts, perceptions, and behavior are culture sensitive (Altman, 1977). Previous research has shown that in social media, privacy attitudes and behaviors differ significantly across nations and cultures (Cho, Rivera-Sanchez, & Lim, 2009; Trepte et al., 2017). Although this previous research did not explicitly compare the intercultural differences between privacy perceptions and concepts, we can nonetheless assume that these are also a consequence of cultural socialization and thus differ across nations. Hence, qualitative research in different cultures may reveal further aspects relevant to a contemporary concept of privacy.

In addition, the social situation of the interview impacts the authenticity and honesty of participants' responses. This is particularly relevant for the question of whether they have private conversations in social media, as they may perceive that the social norm says not to do it and might adjust their responses to this norm. However, quantitative surveys underpin our results, as they found that German users refrain from disclosing private information publicly on SNSs (Trepte & Masur, 2017; Utz, 2015). Self-reported behavior, as in our interviews, is nevertheless always inferior to behavioral data and should be interpreted accordingly.

Conclusion and Future Perspectives

In this article, we explored the subjective perception of different communication settings. As the perception of privacy in a given situation depends on the subjective understanding of privacy, we also investigated laypeople's privacy concepts and compared these concepts with the most prominent academic approaches to privacy in communication research. Our results suggest that subjective perceptions adapt to new communication environments. Right now, people have already developed a (more or less) common perception of privacy on SNSs. Privacy perceptions with regard to IMs, by contrast, are still mixed. We framed them as being in a storming phase. People are still searching for common perceptions and evaluations that can then form the basis of the collective norms and rules that regulate communication and privacy management on these devices.

Although we found that our participants mentioned many aspects of academic theories of privacy, they also added new aspects that seem to have evolved from recent developments in communication and information technology. In an environment where perceived control over personal information is not feasible, individuals must rely on others for their own privacy protection. Interpersonal assessments and, in particular, evaluations of trustworthiness become central to effective privacy management. Today, trust has become a boundary condition of privacy. Consequently, we suggest that future research should focus on trust as a pivotal factor for determining when people experience privacy and how they behave as a consequence. In sum, this study demonstrates the importance of investigating laypeople's perceptions and concepts of privacy as their views may contribute tremendously to redefining and advancing the theoretical understanding of privacy.

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) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This research was funded by the German Federal Ministry of Education and Research (BMBF, Funding Number: 16KIS0094), awarded to Sabine Trepte.

Supplementary Material

Supplementary material for this article is available online.

Notes

1. We focus on theoretical approaches dedicated to individual privacy management, as these are the most prevalent underpinnings of research on privacy in online communication. Hence, our literature review omits certain concepts, such as the framework of contextual integrity by Helen Nissenbaum (2010) or the public–private distinction relevant to political, sociological, and legal discourse on privacy (e.g., Thompson, 2011).
2. The names used here are not the participants' real names.

References

Altman, I. (1974). Privacy: A conceptual analysis. In D. H. Carson (Series Ed.) & S. T. Margulis (Vol. Ed.), *Man-environment interactions: Evaluations and applications; the state of the art in environmental design research. Privacy* (pp. 3-28). Stroudsburg, PA: Dowden, Hutchinson & Ross.

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

Altman, I. (1977). Privacy regulation: Culturally universal or culturally specific. *Journal of Social Issues*, *33*, 67-83. doi:10.1111/j.1540-4560.1977.tb01883.x

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*, *11*(9). doi:10.5210/fm.v11i9.1394. Retrieved from: http://firstmonday.org/article/view/1394/1312

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

Binder, J., Howes, A., & Sutcliffe, A. (2009). The problem of conflicting social spheres: Effects of network structure on experienced tension in social network sites. In D. R. Olsen, R. Arthur, K. Hinckley, M. Ringel Morris, S. Hudson, & S. Greenberg (Eds.), *The SIGCHI conference* (pp. 965-974). New York, NY: Association for Computing Machinery. doi:10.1145/1518701.1518849

boyd, d. (2008a). Facebook's privacy trainwreck: Exposure, invasion, and social convergence. *Convergence: The International Journal of Research Into New Media Technologies*, *14*, 13-20. doi:10.1177/1354856507084416

boyd, d. (2008b). *Taken out of context: American teen sociality in networked publics* (Doctoral dissertation). University of California, Berkeley.

boyd, d. (2011). Social network sites as networked publics: Affordances, dynamics, and implications. In Z. Papacharissi (Ed.), *A networked self: Identity, community, and culture on social network sites* (pp. 39-58). New York, NY: Routledge.

boyd, d., & Hargittai, E. (2010). Facebook privacy settings: Who cares? *First Monday*, 15(8). Retrieved from: http://firstmonday.org/article/view/3086/2589

Burgoon, J. K. (1982). Privacy and communication. In M. Burgoon (Ed.), *Communication yearbook 6* (pp. 206-249). Beverly Hills, CA: SAGE.

Burgoon, J. K., Parrott, R., Le Poire, B. A., Kelley, D. L., Walther, J. B., & Perry, D. (1989). Maintaining and restoring privacy through communication in different types of relationships. *Journal of Social and Personal Relationships*, *6*, 131-158.

Burkell, J., Fortier, A., Wong, L. Y. C., & Simpson, J. L. (2014). Facebook: Public space, or private space? *Information,* *Communication & Society*, *17*, 974-985. doi:10.1080/1369118X.2013.870591

Cho, H., Rivera-Sanchez, M., & Lim, S. S. (2009). A multinational study on online privacy: Global concerns and local responses. *New Media & Society*, *11*, 395-416. doi:10.1177/1461444808101618

Cozby, P. C. (1973). Self-disclosure: A literature review. *Psychological Bulletin*, *79*, 73-91. doi:10.1037/h0033950

Derlega, V. J., Metts, S., Petronio, S., & Margulis, S. T. (1993). *SAGE series on close relationships. Self-disclosure*. Newbury Park, CA: SAGE.

Dienlin, T. (2014). The privacy process model. In S. Garnett, S. Halft, M. Herz, & J. M. Mönig (Eds.), *Medien und Privatheit* (pp. 105-122). Passau, Germany: Karl Stutz.

Dienlin, T., Masur, P. K., & Trepte, S. (2017). Reinforcement or displacement? The reciprocity of FtF, IM, and SNS communication and their effects on loneliness and life satisfaction. *Journal of Computer-Mediated Communication*, *22*, 71-87. doi:10.1111/jcc4.12183

Dienlin, T., & Trepte, S. (2015). 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*, 285-297. doi:10.1002/ejsp.2049

Facebook. (2017). Company info. Retrieved from: https://newsroom.fb.com/company-info/

Fidler, D. S., & Kleinknecht, R. E. (1977). Randomized response versus direct questioning: Two data-collection methods for sensitive information. *Psychological Bulletin*, *84*, 1045-1049. doi:10.1037/0033-2909.84.5.1045

Flanagan, J. C. (1954). The critical incidents technique. *Psychological Bulletin*, *51*, 327-358. doi:10.1037/h0061470

Frye, N. E., & Dornisch, M. M. (2010). When is trust not enough? The role of perceived privacy of communication tools in comfort with self-disclosure. *Computers in Human Behavior*, *26*, 1120-1127. doi:10.1016/j.chb.2010.03.016

Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. In V. Atluri, S. C. Di Vimercati, & R. Dingledine (Eds.), *The 2005 ACM workshop* (pp. 71-80). New York, NY: Association for Computing Machinery. doi:10.1145/1102199.1102214

Joeckel, S., Dogruel, L., & Bowman, N. D. (2016). The reliance on recognition and majority vote heuristics over privacy concerns when selecting smartphone apps among German and US consumers. *Information, Communication & Society*, *20*, 621-636. doi:10.1080/1369118X.2016.1202299

Joinson, A. N. (2001). Self-disclosure in computer-mediated communication: The role of self-awareness and visual anonymity. *European Journal of Social Psychology*, *31*, 177-192. doi:10.1002/ejsp.36

Joinson, A. N., & Paine, C. P. (2007). Self-disclosure, privacy and the internet. In A. Joinson, K. McKenna, T. Postmes, & U. D. Reips (Eds.), *The Oxford handbook of internet psychology* (pp. 237-252). Oxford, UK: Oxford University Press.

Koch, W., & Frees, B. (2017). ARD/ZDF-Onlinestudie 2017: Neun von zehn Deutschen online: Ergebnisse aus der Studienreihe „Medien und ihr Publikum" (MiP) [ARD/ZDF online study 2017: Nine out of ten Germans online. Results from the study series "Media and their audiences" (MiP)]. *Media Perspektiven*, (2017) *9*, 434-446.

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

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

Margulis, S. T. (2011). Three theories of privacy: An overview. In S. Trepte & L. Reinecke (Eds.), *Privacy online: Perspectives on privacy and self-disclosure in the social web* (pp. 9-17). Berlin, Germany: Springer.

Marwick, A. E., & boyd, d. (2014). Networked privacy: How teenagers negotiate context in social media. *New Media & Society*, *16*, 1051-1067. doi:10.1177/1461444814543995

Masur, P. K. (2018). *Situational privacy and self-disclosure: Communication processes in online environments*. New York, NY: Springer.

Masur, P. K., & Scharkow, M. (2016). Disclosure management on social network sites: Individual privacy perceptions and user-directed privacy strategies. *Social Media + Society*, *2*(1), 1-13. doi:10.1177/2056305116634368

Masur, P. K., Teutsch, D., & Trepte, S. (2017). Entwicklung und Validierung der Online-Privatheitskompetenzskala (OPLIS) [Development and validation of the online privacy literacy scale (OPLIS)]. *Diagnostica*, *63*, 256-268. doi:10.1026/0012-1924/a000179

McLaughlin, C., & Vitak, J. (2012). Norm evolution and violation on Facebook. *New Media & Society*, *14*, 299-315. doi:10.1177/1461444811412712

MediaImpact. (2017). *Studie zur digitalen Familienkommunikation—Key Findings* [Study on digital family communication—Key findings]. Retrieved from https://www.google.de/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwiNrcXSq-HXAhUIshQKHQcSCXUQFggmMAA&url=http%3A%2F%2Fdocs.dpaq.de%2F12836-techbook_digitale_familienkommunikation_key_findings_dpa.pdf&usg=AOvVaw1uDzQQhbYHl2LLVb2yPiKy

Miltgen, C. L., & Smith, H. J. (2015). Exploring information privacy regulation, risks, trust, and behavior. *Information & Management*, *52*, 741-759. doi:10.1016/j.im.2015.06.006

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Palo Alto, CA: Stanford University Press.

Palen, L., & Dourish, P. (2003). Unpacking "privacy" for a networked world. In *Proceedings of the ACM conference on human factors in computing systems* (pp. 129-136). New York, NY: Association for Computing Machinery.

Papacharissi, Z. (2010). *A private sphere: Democracy in a digital age*. Hoboken, NJ: John Wiley.

Papathanassopoulos, S. (2015). Privacy 2.0. *Social Media + Society*, *1*(1), 1-2. doi:10.1177/2056305115578141

Park, Y. J. (2013). Digital literacy and privacy behavior online. *Communication Research*, *40*, 215-236. doi:10.1177/0093650211418338

Petronio, S. (2002). *Boundaries of privacy*. Albany, NY: State University of New York Press.

Pew Research Center. (2016). *Social media update 2016: Facebook usage and engagement is on the rise, while adoption of other platforms holds steady*. Retrieved from http://www.pewinternet.org/2016/11/11/social-media-update-2016/

Sarikakis, K., & Winter, L. (2017). Social media users' legal consciousness about privacy. *Social Media + Society*, *3*(1), 1-14. doi:10.1177/2056305117695325

Taddei, S., & Contena, B. (2013). Privacy, trust and control: Which relationships with online self-disclosure? *Computers in Human Behavior*, *29*, 821-826. doi:10.1016/j.chb.2012.11.022

Taddicken, M. (2014). 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. *Journal of Computer-Mediated Communication*, *19*, 248-273. doi:10.1111/jcc4.12052

Teutsch, D., & Niemann, J. (2016). Social network sites as a threat to users' self-determination and security: A framing analysis of German newspapers. *Journal of International Communication*, *22*, 22-41. doi:10.1080/13216597.2015.1111841

Thompson, J. B. (2011). Shifting boundaries of public and private life. *Theory, Culture & Society*, *28*, 49-70. doi:10.1177/0263276411408446

Tidwell, L. S., & Walther, J. B. (2002). Computer-mediated communication effects on disclosure, impressions, and interpersonal evaluations: Getting to know one another a bit at a time. *Human Communication Research*, *28*, 317-348. doi:10.1111/j.1468-2958.2002.tb00811.x

Trepte, S., Dienlin, T., & Reinecke, L. (2014). Risky behaviors. How online experiences influence privacy behaviors. In B. Stark, O. Quiring, & N. Jackob (Eds.), *Schriftenreihe der Deutschen Gesellschaft für Publizistik- und Kommunikationswissenschaft: Vol. 41. Von der Gutenberg-Galaxis zur Google-Galaxis: Alte und neue Grenzvermessungen nach 50 Jahren DGPuK* (pp. 225-244). Konstanz, Germany: UVK.

Trepte, S., & Masur, P. K. (2017). *Privacy attitudes, perceptions, and behaviors of the German population: Research report of a representative survey study*. Retrieved from https://www.forum-privatheit.de/forum-privatheit-de/publikationen-und-downloads/veroeffentlichungen-des-forums.php

Trepte, S., & Reinecke, L. (Eds.). (2011). *Privacy online: Perspectives on privacy and self-disclosure in the social web*. Berlin, Germany: Springer.

Trepte, S., Reinecke, L., Ellison, N. B., Quiring, O., Yao, M. Z., & Ziegele, M. (2017). A cross-cultural perspective on the privacy calculus. *Social Media + Society*, *3*(1), 1-13. doi:10.1177/2056305116688035

Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society*, *28*, 20-36. doi:10.1177/0270467607311484

Utz, S. (2015). The function of self-disclosure on social network sites: Not only intimate, but also positive and entertaining self-disclosures increase the feeling of connection. *Computers in Human Behavior*, *45*, 1-10. doi:10.1016/j.chb.2014.11.076

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

WhatsApp. (2017). Connecting one billion users every day. Retrieved from https://blog.whatsapp.com/10000631/Connecting-One-Billion-Users-Every-Day?l=en

Wheeless, L. R., & Grotz, J. (1976). Conceptualization and measurement of reported self-disclosure. *Human Communication Research*, *2*, 338-346. doi:10.1111/j.1468-2958.1976.tb00494.x

Author Biographies

Doris Teutsch, MSc, is a researcher at the School of Communication, Department of Media Psychology, University of Hohenheim, Germany. Her research interests include online privacy and self-disclosure, social influence on news perception, and media literacy.

Philipp K. Masur, MA, is a researcher at the School of Communication, Department of Media Psychology, University of Hohenheim, Germany. His research interests include social media communication with a special focus on privacy and self-disclosure processes as well as media literacy.

Sabine Trepte, PhD, is a professor of media psychology at the School of Communication, Department of Media Psychology, University of Hohenheim, Germany. Her research interests include privacy and self-disclosure in the social web.