JOURNAL OF COMPUTER-MEDIATED COMMUNICATION

Journal of Computer-Mediated Communication

An Extended Privacy Calculus Model for SNSs: Analyzing Self-Disclosure and Self-Withdrawal in a Representative U.S. Sample

Tobias Dienlin

Department of Media Psychology (540 F), University of Hohenheim, 70599 Stuttgart, Germany

Miriam J. Metzger

Department of Communication, University of California, Santa Barbara, Ellison Hall, Santa Barbara, CA 93106-4020

The privacy calculus established that online self-disclosures are based on a cost-benefit tradeoff. For the context of SNSs, however, the privacy calculus still needs further support as most studies consist of small student samples and analyze self-disclosure only, excluding self-withdrawal (e.g., the deletion of posts), which is essential in SNS contexts. Thus, this study used a U.S. representative sample to test the privacy calculus' generalizability and extend its theoretical framework by including both self-withdrawal behaviors and privacy self-efficacy. Results confirmed the extended privacy calculus model. Moreover, both privacy concerns and privacy self-efficacy positively predicted use of self-withdrawal. With regard to predicting self-disclosure in SNSs, benefits outweighed privacy concerns; regarding self-withdrawal, privacy concerns outweighed both privacy self-efficacy and benefits.

Keywords: Privacy Calculus, Privacy Paradox, Self-Efficacy, Facebook, Structural Equation Modeling, Representative Sample.

doi:10.1111/jcc4.12163

Introduction

With literally billions of users today, social network sites (SNSs) play a central role in everyday life. This is because SNSs offer several benefits such as helping users initiate or maintain social relationships, share information, or provide entertainment (e.g., Choi & Bazarova, 2015). However, SNSs also pose risks; for example, users can become victims of cyberbullying, surveillance by government agencies and private companies, and information or identity theft by unintended audiences (e.g., Marwick & boyd, 2011). Most of the risks relate to aspects of privacy, which helps explain why a lot of people have strong concerns when it comes to having control over the information they provide online (e.g., Hong & Thong, 2013).

Editorial Record: First manuscript received on August 13, 2015. Revisions received on February 25, 2016 and April 21, 2016. Accepted by S. Shyam Sundar on May 28, 2016. Final manuscript received on June 2, 2016. First published online on August 4, 2016.

Nonetheless, understanding why, how, and to what effect people use SNSs despite the risks to privacy remains a major challenge for researchers. Given that SNSs introduced a completely new infrastructure of communication, changed interpersonal processes in a way that can be compared only to the effect of the telephone, and enticed people to provide personal information to private companies on a scale never before seen, it is crucial to further our understanding of SNS behavior. And Facebook, despite the fact that other SNSs such as Instagram or Snapchat are becoming increasingly popular, is an important center of focus when it comes to privacy issues with more than one billion users worldwide.

As shown by Krasnova, Spiekermann, Koroleva, and Hildebrand (2010), the best explanation of SNS use despite privacy fears is that of the "privacy calculus" theory, which states that people will self-disclose personal information when perceived benefits exceed perceived negative consequences. Although this makes intuitive sense, in practice using the privacy calculus to explain self-disclosure on SNSs has proved to be difficult. According to the privacy calculus, people should disclose information on SNSs only when they perceive the benefits of doing so outweigh the perceived costs. Yet, some studies found that people disclosed information in SNSs even when they felt the risks were high (e.g., Taddicken, 2014), which has been called the "privacy paradox." This sparked a great deal of research, which sometimes did find significant statistical relations between privacy concerns (or perceived risks) and self-disclosure behavior in SNSs (e.g., Dienlin & Trepte, 2015; Zlatolas, Welzer, Heričko, & Hölbl, 2015). Hence, our first aim is to replicate earlier findings of the privacy calculus suggesting that both perceived benefits and potential risks affect self-disclosure.

Though prior research has applied the privacy calculus to SNSs, the generalizability of this finding needs to be substantiated. Altogether, we found seven published studies that have analyzed the privacy calculus on SNSs, of which five focused on youth (e.g, Krasnova et al., 2010; Krasnova, Veltri, & Günther, 2012), five had small sample sizes ($N < 300$; e.g., Shibchurn & Yan, 2015; Xu, Michael, & Chen, 2013), and six used convenience samples (e.g., Sun, Wang, Shen, & Zhang, 2015). Moreover, even though SNSs initially came from the US, an extensive study on the privacy calculus using a large sample in the US is still missing — so far, large-scale studies have only been conducted in China (Cheung, Lee, & Chan, 2015) and Korea (Min & Kim, 2015), or have focused on similar but distinct notions such as the privacy paradox (e.g., Taddicken, 2014).[1] Even these studies yield conflicting findings, as some report no relationship between perceived privacy risks and self-disclosure (Cheung et al., 2015; Taddicken, 2014) and others a negative relationship (Min & Kim, 2015). Hence, the second aim is to improve the generalizability of the privacy calculus by analyzing it in a representative U.S. sample.

The third aim of this research is to elaborate the privacy calculus theory. One central finding of research that has not been addressed adequately in the theory is the concept of *self-withdrawal.* Unlike self-disclosure, which is the typical focus within this literature, self-withdrawal refers to the active retention of information (Altman, 1975). Park (2015) and others have demonstrated the importance of considering both self-disclosure *and* self-withdrawal in privacy research. And both aspects of privacy behavior are particularly salient for research on SNSs, as privacy behavior in SNSs is not limited to self-disclosure but also includes self-protection via withholding information. This is true for many reasons: For example, because of the collapse of formerly distinct social contexts into a single audience on SNSs (Marwick & boyd, 2011), users need to be able to make some information inaccessible to particular people.

Theoretical Background

Privacy Theory

Theorists disagree about how to define privacy as well as what it includes. According to Burgoon (1982), it is possible to distinguish *physical privacy* (freedom from surveillance and unwanted intrusions upon one's physical space), *interactional privacy* (control over social encounters), *psychological privacy* (protects from intrusions upon one's thoughts, feelings, attitudes, and values), and *informational privacy* (the ability to control the aggregation and dissemination of information). As privacy in SNSs is largely about the dissemination and retention of personal information, we hence focus on aspects of informational privacy.

According to Westin (1967), "privacy is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means" (p. 7). This definition is pivotal in the privacy literature and shows the two major components of privacy theory: Privacy is, first of all, a withdrawal from others (e.g., Westin, 1967) that, second, must happen voluntarily by people who are in control of their withdrawal (e.g., Altman, 1975). Withdrawal can be determined by physical aspects such as clothes, walls, or spatial distance; similarly, withdrawal can also be determined by immaterial aspects such as choosing not to disclose certain information (Westin, 1967). People withdraw from others for many reasons, for example, to make autonomous decisions, to foster intimate relationships, or to regulate emotions (Westin, 1967). Self-withdrawal is largely about trying to avoid negative outcomes of communication; which is why it can be considered a form of self-protection behavior (see Rogers, 1983).

On the other hand, people need to interact with one another to foster social relationships, and interacting with others always requires some form of self-disclosure—which in turn reduces privacy (Altman, 1975). Hence, people regulate their privacy most prominently by either self-withdrawing or self-disclosing (see also Petronio, 2012). But when do people withdraw from social interactions and when do they partake? Referring to the "calculus of behavior" (p. 35), Laufer and Wolfe (1977) were one of the first to analyze this question.

The Privacy Calculus

The answer provided by Laufer and Wolfe (1977) is that people weigh the potential risks and benefits in terms of the consequences for them in the future. Of course, people cannot know in advance what those risks and benefits might be, so they rely on past experience, intuition, or perception to assess them. Applying this perspective to SNSs, when users weigh perceived benefits more heavily than the risks to privacy—which are often nebulous and uncertain—disclosure is likely to occur. Indeed, some research suggests that disclosure behavior may be primarily motivated by the more proximate social benefits of SNS use rather than by the more distal risks to privacy (Krasnova et al., 2010).

The notion that expected risks and benefits influence peoples' behavior originally comes from economic literature (hence the term *homo economicus*), and stresses that human decision-making is often based on mathematical calculations. Later, social sciences adopted the calculus perspective in order to explain interpersonal behavior, often with a stronger focus on affect: Social exchange theory, for example, posits that when people expect to get more rewards than punishments they will engage in interpersonal interactions (Homans, 1974). Estimating the consequences of behaviors is difficult, as people cannot calculate the risks and benefits rationally, but rather have to perceive them psychologically (Rogers, 1983). Regarding the negative consequences of behavior, protection motivation theory hence argues that *subjective*, rather than objective, threat appraisals are the driving factor that determines behavior (Rogers, 1983). Empirical studies on SNSs support this theoretical reasoning; for example, Xu et al. (2013) found that the perceived privacy risk strongly predicted privacy concern in SNSs.

In an e-commerce setting, Culnan and Armstrong (1999) found that when people were not explicitly told that their personal data would be handled with care, people with greater privacy concerns were less willing to provide personal data. Culnan and Armstrong were the first to call this tradeoff the "privacy calculus" (p. 106). Building on behavior calculus theory (Laufer & Wolfe, 1977), the privacy calculus posits that people will disclose personal information when the perceived benefits exceed the potential costs. The privacy calculus has now been used to explain self-disclosure behaviors in various online contexts, but Krasnova et al. (2010) were the first to analyze the privacy calculus in the context of SNSs. The authors found that users who reported having higher perceived privacy risks had a less comprehensive Facebook profile and users who reported getting more benefits had a more comprehensive profile.

A New Privacy Calculus Model

Distinction of Self-Disclosure and Self-Withdrawal

As stated earlier, one objective of this study is to integrate important tenets of privacy theory in an extended privacy calculus model. This is because prior research on the privacy calculus arguably has missed to integrate an important finding. That is, to date, most studies involving the privacy calculus have focused on self-disclosure only (e.g., Cheung et al., 2015). However, using SNSs does not only involve the *dispersion* of information (i.e., self-disclosure), but also the active *retention* of information (i.e., self-withdrawal; for example, limiting the audience for one's posts). Although related, SNS self-disclosure and self-withdrawal are not simple mirror-images of one another, but rather are distinct concepts (see Christofides, Muise, & Desmarais, 2009). For example, high self-disclosure does not necessitate low self-withdrawal (e.g., it is possible to disclose extensively while talking to a small group of people). For this reason, both concepts should be considered in the privacy calculus.

The basic tenet of communication privacy management theory (CPM, Petronio, 2012) is that disclosure and withdrawal stand in dialectical tension with one another. This means that people feel competing simultaneous needs to be both social (by disclosing information) and private (by withholding information). CPM differs from other theories in its view that in order to understand how people navigate privacy disclosure must always be considered in relation to the desire to protect information. People handle these competing needs by making decisions about the extent of privacy and publicness they want to have in a given interaction (Petronio, 2012). People hence establish privacy rules for both information disclosure and information withholding (for example, not to reveal one's medical history to a stranger).

Although CPM theory was developed for interpersonal interactions, the notion of competing desires for disclosure and privacy is also relevant in SNSs. For example, while most attention has been directed toward disclosure, SNS users can and do enact rules about untagging themselves in particular photos, posting only certain types of content, or being selective about whom they "friend" as a means to protect their privacy. In accordance, Marwick and boyd (2011) posited that in order to leverage the benefits of SNSs, users have to make some information available to certain groups of users but not to others. We argue that such mechanisms can be considered *self-withdrawal behaviors* and are central facets of privacy-related behavior in SNSs. If self-disclosure is one side of the privacy coin, self-withdrawal is the other; and so far, whereas research on similar online phenomena has included this differentiation (Park, 2015), research on the privacy calculus has tended to focus on only one side.

Privacy Concerns as Costs

In privacy calculus research to date, "costs" of SNS use have been measured by either perceived privacy risks or privacy concerns. Privacy risks are "the expectation of losses associated with the release of personal information" (Xu, Luo, Carroll, & Rosson, 2011, p. 46), and privacy concerns are "the degree to which an Internet user is concerned about website practices related to the collection and use of his or her personal information" (Hong & Thong, 2013, p. 276). These definitions show that both privacy risks and privacy concerns involve fear concerning potential losses due to the disclosure of, or lack of control over, personal information. Protection motivation theory (Rogers, 1983) shows that fear is a strong driving factor in why people employ preventive measures, which may include self-withdrawal (i.e., withholding information) in SNS contexts. Most research on SNSs has operationalized costs as concerns (e.g., Min & Kim, 2013). Moreover, Xu et al. (2013) found that privacy risks predicted privacy concerns, which in turn determined self-disclosure. As a result, we focus on privacy concerns as a mitigating cost factor for self-disclosure and as a reinforcing factor for self-withdrawal.

Integrating Privacy Self-Efficacy

Establishing self-protective behaviors can be difficult in any context (Rogers, 1983), and this may be especially true in SNSs, as enacting behaviors to protect privacy requires knowledge of how to implement the multitude privacy settings that are available and that change over time (Marwick & boyd, 2011). Protection motivation theory suggests that if people want to establish self-protecting behaviors, experiencing fear or concern does not suffice to effectively change behavior, as people also need to have sufficient self-efficacy (Rogers, 1983). Self-efficacy refers to the belief in one's ability to execute certain behaviors. As a result, we suggest integrating privacy self-efficacy as third predictor of SNS behavior in our extended privacy calculus model. To date, no studies of the privacy calculus have included this factor.

Hypotheses

Benefits

The most important factors to explain self-disclosure on SNSs are the positive aspects of SNS use, for example, making new friends or learning about things that are important or useful. In the context of SNSs, research shows that people have manifold motives for using SNSs: for example, information exchange, relational development, or entertainment (e.g., Choi & Bazarova, 2015). Several studies have also found empirical evidence that these motives for using SNSs manifest in several specific benefits, such as increased social capital, leveraged social support, or enacted identity management (e.g., Trepte, Dienlin, & Reinecke, 2014). All seven empirical studies on the privacy calculus for SNSs showed that if users expected benefits from using SNSs they disclosed more personal information. Benefits explained between 5% (Krasnova et al., 2012) and 66% (Xu et al., 2013) of variance in self-disclosure, and thus demonstrated that expected benefits have good predictive power. Thus, we hypothesize:

> **H1:** The more people expect benefits by using Facebook, the more they will disclose information about themselves.

The question remains, though, whether the expected benefits of participating in SNSs also influence self-protective behaviors online. Referring to Christofides et al. (2009), we argued that self-disclosure and self-withdrawal behaviors are related but nonetheless distinct behaviors. For example, on SNSs it is possible to have few users as friends (high self-withdrawal) to whom one nevertheless reveals a lot of information (high self-disclosure). On the one hand, one could argue that if people expect benefits from using SNSs they should withdraw less in order to maximize their outcomes; on the other hand, protection motivation theory (Rogers, 1983) suggests that only negative threat appraisals (i.e., privacy concerns), rather than positive feelings (i.e., expected benefits), determine self-protective behaviors. Hence, as we are not aware of any studies that analyzed the relationship between expected benefits and self-withdrawal empirically, and because of conflicting theoretical considerations, we propose the following research question:

> **RQ1:** Do people who expect more benefits from using Facebook show more or less self-withdrawal behaviors?

Privacy Concerns

For the Internet in general, privacy concerns have been found to negatively predict self-disclosure (e.g., Metzger, 2004). Also, for SNSs in particular, privacy concerns have been shown to negatively relate to self-disclosure: For example, SNS users who were concerned about their privacy tended to have profiles that were less personal, and also tended to disclose less identifying information (Dienlin & Trepte, 2015). Six of the seven studies on the privacy calculus in SNSs showed significant negative effects of concerns or risks on self-disclosure—only the study by Cheung et al. (2013) and the U.S. subsample in the study by Krasnova et al. (2012) did not show significant results. Similarly, in a representative survey of German social media users, Taddicken (2014) examined privacy behavior in blogs, SNS, wikis, discussion forums, photo and video sharing sites and found that, across these platforms, disclosure varied depending on the sensitivity of the information to be disclosed. At the same time, no significant direct relation between privacy concern and self-disclosure was found, which shows that the relation between privacy concern and self-disclosure is still somewhat capricious. However, despite some inconsistency in the literature, a growing body of empirical studies has supported that concern about privacy and self-disclosure on SNSs are negatively associated with one another.

H2a: The more concerned people are regarding privacy, the less information they will disclose about themselves in Facebook.

We also predict that privacy concerns are related to the active retention of information. Several studies report that concepts relating to privacy concerns are related to self-withdrawal behaviors: For example, in a study with 340 Malaysian university students, privacy concerns were found to directly and significantly predict self-withdrawal measures on SNSs (Mohamed & Ahmad, 2012). Utz and Kramer (2009) similarly found that privacy concerns were associated with the use of privacy settings on Hyves, a SNS in the Netherlands. We therefore hypothesize that:

H2b: The more concerned people are regarding privacy, the more they will engage in acts of self-withdrawal in Facebook.

Self-Efficacy

The extant literature supports the notion that self-efficacy should predict implementing privacy-enhancing or self-withdrawal behaviors online. For example, users who reported having more technical Internet skills related to privacy (e.g., phishing, p3p, or cache) also report employing more privacy-enhancing behaviors (e.g., using fake names for SNSs, clearing browser history, or deletion of cookies; Park, 2013). Lee, LaRose, and Rifon (2008) found that users who reported more self-efficacy in using virus protection measures had a stronger intention to adopt virus protection behaviors. Similar results can be found for the context of SNSs: Both Cheung et al. (2013) and Zlatolas et al. (2015) evidenced that people who perceive to be in control of their privacy report less privacy concerns. Likewise, Mohamed and Ahmad (2012) found that both self-efficacy and response efficacy had a positive effect on the use of privacy measures.

H3: People with greater privacy self-efficacy will engage in more self-withdrawal behaviors.

Finally, the question remains whether privacy self-efficacy might also affect self-disclosure. Niemann and Schenk (2014) found that privacy self-efficacy influenced self-withdrawal but not self-disclosure behaviors in SNSs. Also, from a theoretical perspective it can be argued that because the entire infrastructure of SNSs is built for self-disclosure, self-disclosing on SNSs is easy and does not necessitate high levels of competence or perceived behavioral control. However, privacy self-efficacy is conceptually close to self-efficacy regarding self-presentation, which has been shown to increase information disclosure (Krämer & Winter, 2008). Indeed, people who feel better able to protect themselves by using available SNS privacy settings, for example, may be more willing to disclose. Thus, because of conflicting theoretical and empirical considerations, we pose the following research question:

RQ2: Do people with greater privacy self-efficacy show more or less self-disclosure?

The Extended Privacy Calculus Model

The predictions advanced in the four hypotheses combine to suggest a novel framework to analyze the privacy calculus that we call the extended privacy calculus model. In accordance with CPM theory (Petronio, 2012), the model has two dependent variables: self-disclosure and self-withdrawal. We reason that these two variables are explained by different factors: Self-disclosure is explained on the basis of expected benefits and privacy concern, whereas self-withdrawal is explained by privacy concern and privacy self-efficacy. Due to a lack of theoretical and empirical clarity, we ask in two research questions whether perceived benefits predict privacy behaviors and whether privacy self-efficacy predicts self-disclosure.

Method

Procedure and Participants

The data are representative of adult Facebook users ages 18 and over residing in the US and were collected by the research firm GFK (www.gfk.com) in October 2012 by means of an online questionnaire. GfK samples households from its KnowledgePanel, which is a probability-based web panel designed to be representative of the US. To qualify for the main survey, a panel member must have had a Facebook account, as determined by a screener question at the time of data collection. The median participation time was 20 minutes.

The resulting sample consisted of $N = 1{,}156$ respondents ranging in age from 18 to 86 ($M = 46.91$) years. 57.35% of the respondents were female. Regarding ethnicity, 77.5% of the respondents were *White, Non-Hispanic*, 6.8% *Black, Non-Hispanic*, 3.2% *Other, Non-Hispanic*, 8.5% *Hispanic*, and 4% *2+ Races, Non-Hispanic*. In relation to education, 6.1% indicated *less than high school*, 24.3% *high school*, 32.8% *some college*, and 36.8% *bachelor's degree or higher*. The median household income was *between $60,000 to $74,999 per year*. Regarding current residency, 18.9% of the respondents came from the Northeast, 22.6% from the Midwestern, 34.3% from the Southern, and 24.2% from the West of the US.

Measures

Based on established scales and additional items that we designed in order to fit the research question more closely, confirmatory factor analyses (CFA) were run for each variable to select items that formed a unidimensional structure. To assess the assumption of normality, Shapiro-Wilk normality tests were done. As the results showed violations of normality, we used the more robust Satorra-Bentler scaled test statistic. Items that did not sufficiently load on the latent factor were deleted. To assess reliability of the constructed and congeneric scales, the usual fit indices (χ^2, CFI, TLI, RMSEA, SRNR), McDonald's composite reliability omega, and Cronbach's alpha were calculated. All scales had adequate to good factorial validity and reliability. The variables and their psychometrics appear in Table 2; all questionnaire items, the data, item distributions, and the CFAs can be found in the online supplementary material.[2]

Facebook benefits

Facebook benefits measured how many positive aspects people attributed to Facebook use. Twelve items were initially developed based on an earlier focus group pilot study of users who discussed the benefits and risks that they experience as a result of using Facebook. Of the 12 items, 10 were used as determined by the data preparation analysis discussed above that included, for example, using Facebook for self-expression, learning new things, and making new personal or business contacts (see online supplementary material). Respondents answered all items on a 5-point scale ranging from 1 = *strongly disagree* to 5 = *strongly agree*.

Privacy concerns

Privacy concerns measured how strongly people worried about their privacy online. Four items were developed based on Malhotra et al. (2004), which all were used—for example, “I do not feel especially concerned about my privacy online.” Respondents answered both items on a 5-point scale ranging from 1 = *strongly disagree* to 5 = *strongly agree*. Several answers were reverse coded.

Facebook privacy self-efficacy

Facebook privacy self-efficacy measured if people felt confident and capable of adjusting their privacy options on Facebook. We adapted the perceived privacy control scale by Krasnova et al. (2010) in order to better represent self-efficacy, and used all 5 items. One example item is: “I feel confident in my ability to protect myself using Facebook’s privacy settings.” Answers ranged from 1 = *strongly disagree* to 5 = *strongly agree*.

Facebook self-disclosure

Facebook self-disclosure measured the extent to which people share personal information on Facebook. We extended the self-disclosure scale by Krasnova et al. (2010) using 5 of the 7 items, including “I have put a lot of information about myself in my Facebook profile.” Respondents answered all items on a 5-point scale ranging from 1 = *strongly disagree* to 5 = *strongly agree*.

Facebook self-withdrawal

This variable measured how many deliberate privacy-preserving behaviors people engaged in that helped to make their profiles more private. In line with Mohamed and Ahmad (2012), we asked respondents on a binary scale whether they have already implemented various privacy measures, such as the untagging of posts or photos, or making one’s profile unsearchable. Respondents answered each item with either 0 = *no* or 1 = *yes*. Ten items were developed, of which six items formed a unidimensional scale.

Data Analysis

All hypotheses were tested with a saturated structural equation model (SEM). Again, we used the robust Satorra-Bentler scaled test statistic. Because of the high number of items, which increases the complexity of the SEM, we used item parceling (Little, Cunningham, Shahar, & Widaman, 2002). Item-parcels average the information of several items into individual parcels. As a precondition, items that are parceled need to show unidimensionality, which was positive in our case (see Table 1). We used

Table 1 Psychometric Properties of Variables

	Recom. Crit.	FB benefits	Privacy concerns	FB privacy self-efficacy	FB self-disclosure	FB self-withdrawal
m		3.13	3.34	2.89	2.65	0.67
sd		0.91	0.97	0.95	1.04	0.41
skewness		−0.49	−0.17	−0.04	0.07	−1.03
kurtosis		0.09	−0.39	−0.49	−0.69	0.77
χ^2		158.50	6.06	12.14	25.34	30.47
df		35	2	5	5	9
p	>.05[a]	<.001	.050	.030	<.001	<.001
CFI	>.95[a]	0.96	0.99	1.00	0.99	0.96
TLI	>.95[a]	0.95	0.97	0.99	0.97	0.93
RMSEA	<.08[a]	0.06	0.04	0.04	0.06	0.05
SRMR	<.08[a]	0.03	0.02	0.01	0.02	0.06
α	>.70[a]	0.91	0.67	0.91	0.80	0.74
ω	>.60[a]	0.91	0.68	0.91	0.81	0.56
AVE	>.50[a]	0.77	0.55	0.83	0.71	0.32
MSV	<AVE[a]	0.37	0.15	0.08	0.37	0.15
ASV	<AVE[a]	0.09	0.06	0.05	0.10	0.04

Note. [a]Hair, Black, Babin & Anderson (2010); α = Cronbach's alpha; ω = composite reliability. AVE = average variance extracted, MSV = maximum shared variance, ASV = average shared variance (all measured in final SEM).

the item-to-construct balance approach and measured each variable with 2 parcels, and when possible as recommended with 3 parcels (Little et al., 2002).

Missing data were treated with listwise deletion. We tested Hypotheses with a two-tailed .05 significance level. Regarding effect sizes, coefficients with values exceeding $\beta = .1$ were considered small effects, $\beta = .3$ medium effects, and $\beta = .5$ large effects. We decided against including poststratification weights and demographic control variables[3]. The software R was used (version 3.1.2) for the analyses, supplemented by packages such as lavaan (version 0.5-17).

Results

Model Fit

The SEM showed adequate fit ($\chi^2 = 99.7$, $df = 44$, $p < .001$, CFI = 0.99, TLI = 0.98, RMSEA = 0.03, SRMS = 0.03). To assess convergent factorial validity, the average variance extracted (AVE) was calculated. Values above AVE = .5 indicate good convergent validity. Four of the five variables were above this threshold, and one was below (Facebook self-withdrawal, AVE = .32; see Table 1). Given that Facebook self-withdrawal was measured with binary items only, factorial validity can thus be considered acceptable. To assess discriminant validity, the AVE was compared to the maximum shared variance (MSV) and the average shared variance (ASV). Results showed that AVE values were above MSV and ASV values (see Table 1), which supports that the variables had sufficient discriminant validity.[4]

Hypotheses

Facebook benefits as predictor

Hypothesis 1 stated that the more benefits people expect from using Facebook, the more they would self-disclose. The data supported Hypothesis 1: Respondents who reported that they would get more social benefits on Facebook also posted more personal information ($b = 0.65$, 95% CI [0.57, 0.73], $\beta = .57$, $p \leq .001$, $SE = 0.04$). The standardized regression coefficient of $\beta = .57$ showed that the effect was strong.

Research question 1 asked whether Facebook benefits would predict Facebook self-withdrawal. Results indicated there was no significant effect of Facebook benefits on self-withdrawal ($b = 0.01$, 95% CI [-0.03, 0.04], $SE = 0.02$, $p = .713$, $\beta = .02$).

Privacy concerns as predictor

Hypothesis 2a predicted that the more concerned people are about privacy, the less information they would disclose. The data supported Hypothesis 2a: Respondents who reported higher levels of concern about their privacy also posted less personal information on Facebook ($b = -0.29$, 95% CI [-0.38, -0.20], $\beta = -.23$, $p \leq .001$, $SE = 0.05$). The standardized regression coefficient of $\beta = -.23$ indicated that the effect was small.

Hypothesis 2b stated that the more concerned people are regarding privacy, the more they would employ active self-withdrawal. The data supported Hypothesis 2b: Respondents who reported greater concern about their privacy also reported using more self-withdrawal mechanisms on Facebook ($b = 0.19$, 95% CI [0.15, 0.23], $\beta = .45$, $p \leq .001$, $SE = 0.02$). The standardized regression coefficient of $\beta = .45$ showed that the effect was of medium strength.

Bootstrap analyses with $N = 2000$ draws indicated that, taken together, privacy concerns explained 41.2% of variance in self-disclosure and self-withdrawal (95% CI [26.9%, 56.6%]).

Privacy self-efficacy as predictor

Hypothesis 3 anticipated that people with greater Facebook privacy self-efficacy would employ active self-withdrawal more than those with lower self-efficacy. The data supported Hypothesis 3: Respondents who reported higher self-efficacy in terms of managing their privacy also reported using more self-withdrawal mechanisms on Facebook ($b = 0.08$, 95% CI [0.05, 0.11], $\beta = .27$, $p \leq .001$, $SE = 0.01$). The standardized regression coefficient of = .27 indicated that this effect was small.

Research question 2 asked whether privacy self-efficacy would also predict Facebook self-disclosure. Results showed that there was no significant effect of Facebook privacy self-efficacy on self-disclosure ($b = 0.03$, 95% CI [-0.03, 0.09], $SE = 0.03$, $p = .308$, $\beta = .03$).

Comparison of effects

Regarding effects on Facebook self-disclosure, comparison of confidence intervals shows that the net effect of benefits exceeded that of privacy concerns, which in turn exceeded that of privacy self-efficacy. Taken together, all three variables explained 37.87% of Facebook self-disclosure. With regard to effects on Facebook self-withdrawal, comparison of the confidence intervals shows that the net effect of privacy concern exceeded that of privacy self-efficacy, which in turn exceeded that of Facebook benefits. Taken together, all three variables explained 27.58% of Facebook self-withdrawal.

In addition, we tested whether expected benefits or privacy concerns explained more variance of both dependent variables taken together (i.e., self-disclosure plus self-withdrawal behavior). Bootstrap

Table 2 Regression Coefficients

		95% CI				
	b	*LL*	*UL*	*SE*	*p*	*β*
Facebook self-disclosure						
Facebook benefits	0.65	0.57	0.73	0.04	<.001	.57
Facebook concerns	−0.29	−0.38	−0.20	0.05	<.001	-.23
Facebook privacy self-efficacy	0.03	−0.03	0.09	0.03	.308	.03
Facebook self-withdrawal						
Privacy benefits	0.01	−0.03	0.04	0.02	.713	.02
Facebook concerns	0.19	0.15	0.23	0.02	<.001	.45
Facebook privacy self-efficacy	0.08	0.05	0.11	0.01	<.001	.27

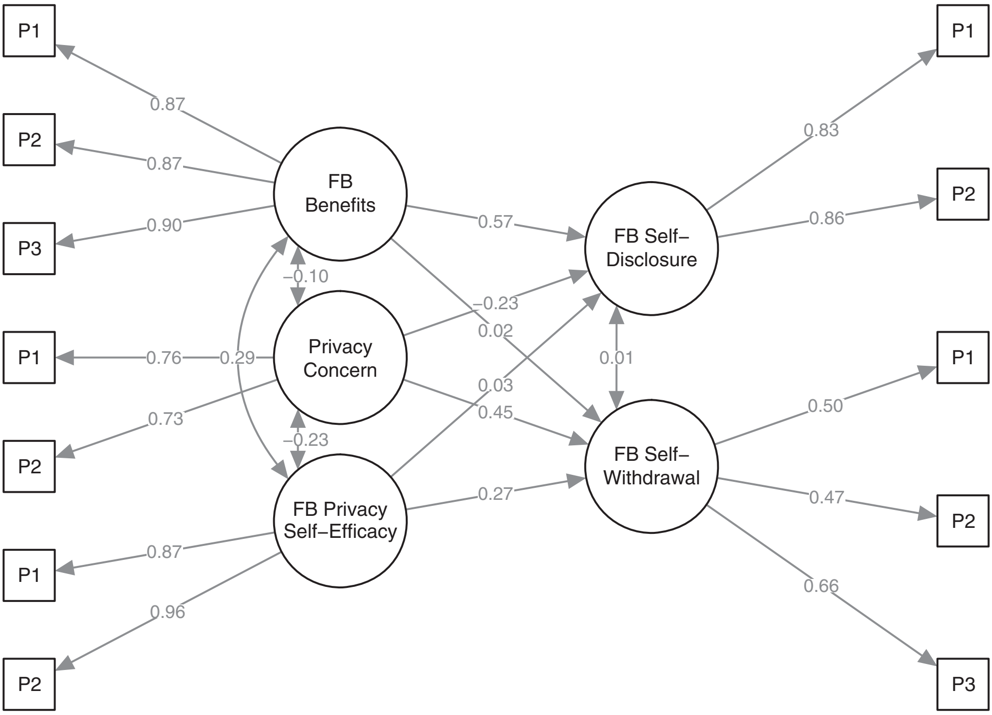

Figure 1 Results of the extended privacy calculus model. P1-P3 represent item parcels consisting of 2-4 items each. The effects are standardized.

analyses with $N = 2000$ draws showed that Facebook benefits altogether explained 32.9% of variance (95% CI [26.0%, 38.9%]) and that privacy concerns explained 41.2% of variance (95% CI [26.9%, 56.6%]). As the confidence intervals do not overlap, this shows that both variables did not differ significantly in their overall predictive power. For a list of all regression statistics see Table 2, and for a visual representation see Figure 1.

Discussion

Implications

This study set out to see if prior findings on the privacy calculus and its effect on self-disclosure in SNS could be replicated, to analyze the generalizability of the privacy calculus to a larger and representative U.S. sample, and to extend its theoretical framework.

The importance of replication in research has been discussed widely in recent years. Thus the first major finding of this study is that the privacy calculus findings of past work could be replicated. Specifically, this study finds that when people decide whether to self-disclose in SNSs, both concerns and benefits compete with one another. This is relevant as some research on the privacy paradox showed no, small, or complex relations between concerns and disclosure; Taddicken (2014), for example, found that perceived social relevance mediated the relation between privacy concerns and self-disclosure. The mixed findings could partly result from the fact that privacy concerns have often been operationalized differently and in specific contexts (e.g., ecommerce, SNSs); hence, results from any one study should not be overly generalized. Overall, by finding evidence for the privacy calculus, this study adds to a growing body of research that does not find evidence for the privacy paradox in the context of SNSs (e.g., Dienlin & Trepte, 2015). However when predicting Facebook self-disclosure, expected benefits still have more predictive power than privacy concerns. This replicates findings by Min and Kim (2015) and supports the idea that when partaking actively in SNSs, benefits loom larger than concerns.

The second major finding of this study is that, by means of a nationwide representative study, the data confirmed that the privacy calculus can be generalized to the U.S. adult Facebook population. Prior research on the privacy calculus has mainly been conducted with college-age samples only, whereas this study included people from across different generations and people from a much wider variety of educational and ethnical backgrounds. As a result, this study substantiates the empirical foundation for the privacy calculus laid by prior research and, by showing that it can be applied to Facebook users in an entire nation, adds to its robustness.

The third and perhaps most interesting finding is that this study makes several contributions to the privacy calculus's theoretical framework. In our extended privacy calculus model we included self-withdrawal behaviors as a new criterion and added privacy self-efficacy as a predictor. Although other studies have investigated the mechanisms underlying the privacy calculus by, for example, examining further predictors of self-disclosure (Min & Kim, 2015) or privacy risks (Krasnova et al., 2010), to our knowledge, this is the first study to show that both self-disclosure and self-withdrawal behaviors can be analyzed in a single model. This helps to show two things: First, the results further underscore the relevance of privacy concerns, as privacy concerns not only explained self-disclosure but also self-withdrawal. Hence, privacy concerns are more powerful as initially thought and play an important role in determining SNS behavior. Second, different factors help to explain variance in self-disclosure and in self-withdrawal. That is, whereas benefits predicted only self-disclosure, privacy concerns predicted both self-disclosure and self-withdrawal behaviors. A comparison of the combined effects even confirmed that benefits and concerns have equal predictive power for self-disclosure and self-withdrawal.

The results of the research questions shed further light on the role of both perceived benefits and privacy concerns in SNS, as well as self-efficacy. Prior to this study it was unclear whether perceived benefits, in addition to increasing self-disclosure, influence self-withdrawal in SNSs since no research had investigated this relationship. The data from this study support the suggestion from Protection Motivation Theory that only negative threat appraisals (e.g., privacy concerns) should impact self-protection behaviors (e.g., self-withdrawal in SNS contexts).

Finally, this study showed that privacy self-efficacy is not related to disclosure in SNSs. This relation has not been studied previously but could be supported by research on optimistic bias in that privacy self-efficacy might impart a sense of invulnerability to potential negative consequences of using SNSs. However, we found no evidence for this notion. This study also revealed that privacy self-efficacy significantly predicted self-withdrawal, which supports one of privacy theory's central tenets that in order to regulate privacy effectively, people also need to have sufficient control (Westin, 1965), including the psychological perception that they are able to enact such control.

Limitations and Future Research

A limitation of the privacy calculus theory, as well as the model advanced in this study, is that it explicitly focuses on the individual. Yet, within SNS contexts, privacy is both an individual *and* a social issue. Indeed, one of the most exciting recent developments in the privacy research literature is the notion of "networked audience" (Marwick & boyd, 2011), which refers to the fact that control of information disclosure in networked environments such as SNSs does not solely reside in the actions taken by an individual user — it is collectively affected by network ties. For example, one user's action (e.g., self-disclosure, "liking," tagging, etc.) can reveal information about other users in the network to unknown or unauthorized audiences.

The idea of networked privacy, or the fact that privacy is socially contextualized in networked environments, has not been studied extensively in the privacy calculus literature, and yet an individual's calculus of the costs and benefits of using SNSs is most certainly affected by their network linkages. Indeed, Cheung et al. (2015) showed that social influences can explain up to 16% of variance in self-disclosure. Social influences on the privacy calculus need to be examined in future research, and it would be valuable to integrate socially oriented theories to do so (e.g., the theory of planned behavior). That said, given that three variables can explain 38% of self-disclosure and 28% of self-withdrawal behavior, the extended privacy calculus offers a both parsimonious and effective approach for understanding privacy in SNSs.

Because the study used cross-sectional data, the postulated directions of effects have yet to be verified with a longitudinal design. In addition, the scales used in this study need to be further optimized, as some items could not be used due to lack of reliability or factorial validity.

The study presents the psychology and behaviors of Facebook users in 2012. Since then, the online world has changed significantly: New SNSs such as Instagram entered the market, new messengers such as Snapchat appeared, and new risky behaviors such as novel forms of sexting or taking extreme selfies manifested. As a result, it is important to find out whether the extended privacy calculus model also helps to explain these novel behaviors, or whether other aspects such as fear of missing out (FoMO) or sensation seeking become increasingly relevant. It is important for future research to examine if the extended privacy calculus model holds for newer SNS platforms. It is possible, for example, that SNSs that allow for ephemeral communication (e.g., Snapchat) may alter an individual's cost-benefit calculus of posting risky messages with impacts to their self-disclosure and self-withdrawal behaviors. That said, the results of this study likely remain valid for Facebook and platforms like it, as the core structures (news feed, timeline, groups, messenger) and the main ways people interact in it (post, like, share, message) did not change significantly since the time the data for this study were collected.

Conclusion

By using U.S. representative data, this study adds to a growing literature that confirms the privacy calculus in SNSs. The extended privacy calculus model is the first to integrate the theoretical tenets of both SNS self-disclosure *and* self-withdrawal into a single model. We believe that this novel integration is important. To illustrate consider the following figurative example from the context of automobiles: To date, separate strands of research have analyzed either how cars accelerate or how they slow down. However, research should always aim to answer related questions together within one single model, because this offers the advantage to analyze influences that are either specific to both processes (e.g., engine/brakes) or more general (e.g., aerodynamic drag). Regarding SNSs, the extended privacy calculus model is the first integrated model to show that expected benefits are a specific influence for self-disclosure, whereas self-efficacy is a specific influence for self-withdrawal. Privacy concerns, adversely, influence both SNS self-disclosure and self-withdrawal. Overall, this study thus supports the basic tenets of privacy theory in SNSs (Petronio, 2012), finds further evidence against the privacy paradox, and proposes a novel extended privacy calculus model for SNSs.

Notes

[1] Unlike the other studies cited here that focused on the privacy calculus within SNSs only, Taddicken (2014) examined privacy behavior across SNSs, blogs, wikis, discussion forums, and photo and video sharing sites. While her study does not explicitly examine the privacy calculus, it does analyze the relationship between privacy concern and self-disclosure.

[2] https://osf.io/e3j98/?view_only = cf4c10222def4efdbecae20c1dca7dc6

[3] To improve representativeness, GFK offers poststratification weights that account for systematic under- and oversampling of specific parts of the population. The question of whether or not to use weights is somewhat ambivalent. We followed the U.S. Bureau of Labor Statistics advice to not use weights when conducting inferential statistics (i.e., regressions). For the results with weights, please see the online supplementary material. Generally, demographic control variables should only be included if they are theoretically related to the variables of interest. Even though demographic variables are related to privacy behavior online, they were not of major theoretical interest. For results without the control variables, please see the online supplementary material. Both alternative SEMs produced very similar results to the main SEM.

[4] When all items are measured on the basis of a single online questionnaire—as was the case for this study—a bias due to common method might occur. Several statistical methods exist to test for common method bias. However, the practice of testing for common method bias by means of statistical post hoc test has been criticized. As a result, we used a priori precautions; for example, we took care that items did not semantically overlap on different constructs or used some inverted items (see online supplementary material).

References

Altman, I. (1975). *The environment and social behavior*. Monterey, CA: Brooks Cole.

Burgoon, J. K. (1982). Privacy and communication. *Communication Yearbook,* 6, 206–249.

Cheung, C., Lee, Z. W. Y., & Chan, T. K. H. (2015). Self-disclosure in social networking sites. *Internet Research*, 25(2), 279–299. doi:10.1108/IntR-09-2013-0192

Choi, Y. H., & Bazarova, N. N. (2015). Self-disclosure characteristics and motivations in social media: Extending the functional model to multiple social network sites. *Human Communication Research,* 41(4), 480–500. doi:10.1111/hcre.12053

Christofides, E., Muise, A., & Desmarais, S. (2009). Information disclosure and control on Facebook: Are they two sides of the same coin or two different processes? *CyberPsychology & Behavior,* 12(3), 341–345. doi:10.1089/cpb.2008.0226

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science,* 10(1), 104–115. doi:10.1287/orsc.10.1.104

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(3), 285–297. doi:10.1002/ejsp.2049

Hair, J., Black, W., Babin, B., & Anderson, R. (2010). *Multivariate data analysis* (7th ed.). Upper Saddle River, NJ: Prentice-Hall, Inc.

Homans, G. C. (1974). *Social behavior: Its elementary forms*. New York, NY: Harcourt Brace.

Hong, W., & Thong, J. Y. (2013). Internet privacy concerns: An integrated conceptualization and four empirical studies. *MIS Quarterly,* 37(1), 275–298. doi:10.1089/cyber.2011.0511

Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. *Journal of Information Technology,* 25(2), 109–125. doi:10.1057/jit.2010.6

Krasnova, H., Veltri, N. F., & Günther, O. (2012). Self-disclosure and privacy calculus on social networking sites: The role of culture. *Business & Information Systems Engineering,* 4(3), 127–135. doi:10.1007/s12599-012-0216-6

Krämer, N. C., & Winter, S. (2008). Impression management 2.0. *Journal of Media Psychology,* 20(3), 106–116. doi:10.1027/1864-1105.20.3.106

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues,* 33(3), 22–42. doi:10.1111/j.1540-4560.1977.tb01880.x

Lee, D., LaRose, R., & Rifon, N. (2008). Keeping our network safe: A model of online protection behaviour. *Behaviour & Information Technology,* 27(5), 445–454. doi:10.1080/01449290600879344

Little, T. D., Cunningham, W., Shahar, G., & Widaman, K. (2002). To parcel or not to parcel: Exploring the question, weighing the merits. *Structural Equation Modeling: A Multidisciplinary Journal,* 9(2), 151-173. doi:10.1207/S15328007SEM0902_1

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research,* 15(4), 336–355. doi:10.1287/isre.1040.0032

Marwick, A. E., & boyd, d. (2011). I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media & Society,* 13(1), 114–133. doi:10.1177/1461444810365313

Metzger, M. J. (2004). Privacy, trust, and disclosure: Exploring barriers to electronic commerce. *Journal of Computer-Mediated Communication,* 9(4), 00. doi:10.1111/j.1083-6101.2004.tb00292.x

Min, J., & Kim, B. (2015). How are people enticed to disclose personal information despite privacy concerns in social network sites? The calculus between benefit and cost. *Journal of the Association for Information Science and Technology,* 66(4), 839–857. doi:10.1002/asi.23206

Mohamed, N., & Ahmad, I. H. (2012). Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior,* 28(6), 2366–2375. doi:10.1016/j.chb.2012.07.008

Niemann, J., & Schenk, M. (2014). Im Spannungsfeld zwischen Risiko und Nutzen Selbstoffenbarung auf Social-Networking-Sites. In B. Stark, O. Quiring, & N. Jackob (Eds.), *Von der Gutenberg-Galaxis zur Google-Galaxis* (pp. 207–223). Konstanz, Germany: UVK.

Park, Y. J. (2013). Digital literacy and privacy behavior online. *Communication Research,* 40(2), 215–236. doi:10.1177/0093650211418338

Park, Y. J. (2015). Do men and women differ in privacy? Gendered privacy and (in)equality in the Internet. *Computers in Human Behavior,* 50, 252–258. doi:10.1016/j.chb.2015.04.011

Petronio, S. (2012). *Boundaries of privacy: Dialectics of disclosure.* Albany, NY: State University of New York Press.

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. T. Cacioppo, R. E. Petty, & R. E. Petty (Eds.), *Social psychophysiology: A sourcebook* (pp. 153–177). New York: Guilford Press.

Shibchurn, J., & Yan, X. (2015). Information disclosure on social networking sites: An intrinsic–extrinsic motivation perspective. *Computers in Human Behavior,* 44, 103–117. doi:10.1016/j.chb.2014.10.059

Sun, Y., Wang, N., Shen, X.-L., & Zhang, J. X. (2015). Location information disclosure in location-based social network services: Privacy calculus, benefit structure, and gender differences. *Computers in Human Behavior*, 52, 278–292. doi:10.1016/j.chb.2015.06.006

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(2), 248–273. doi:10.1111/jcc4.12052

Trepte, S., Dienlin, T., & Reinecke, L. (2014). Influence of social support received in online and offline contexts on satisfaction with social support and satisfaction with life: A longitudinal study. *Media Psychology,* 18(1), 74–105. doi:10.1080/15213269.2013.838904

Utz, S., & Kramer, N. C. (2009). The privacy paradox on social network sites revisited: The role of individual characteristics and group norms. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace,* 3(2).

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

Xu, F., Michael, K., & Chen, X. (2013). Factors affecting privacy disclosure on social network sites: An integrated model. *Electronic Commerce Research,* 13(2), 151–168. doi:10.1007/s10660-013-9111-6

Xu, H., Luo, X., Carroll, J. M., & Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems,* 51(1), 42–52. doi:10.1016/j.dss.2010.11.017

Zlatolas, L. N., Welzer, T., Heričko, M., & Hölbl, M. (2015). Privacy antecedents for SNS self-disclosure: The case of Facebook. *Computers in Human Behavior,* 45, 158–167.

About the Authors

Tobias Dienlin is a Ph.D. candidate and research assistant at the Department of Media Psychology, University of Hohenheim (Germany), and a fellow of the German Academic Scholarship Foundation. His research focuses on privacy, self-disclosure, online social support, identity, and media effects on well-being and political knowledge. **Address:** Tobias Dienlin, University of Hohenheim, Department of Media Psychology (540F), 70599 Stuttgart, Germany. E-Mail: tobias.dienlin@uni-hohenheim.de

Miriam J. Metzger is Professor of communication and faculty affiliate of the Center for Information, Technology and Society (CITS) at the University of California, Santa Barbara. Her research interests lie at the intersection of media, information technology, and trust, centering on how information and communication technologies alter our understandings of credibility, privacy, and the processes of media effects.