European Journal of Social Psychology, *Eur. J. Soc. Psychol.* **45**, 285–297 (2015)
Published online 31 July 2014 in Wiley Online Library (wileyonlinelibrary.com) **DOI**: 10.1002/ejsp.2049

Special section article: Putting the Social (Psychology) into Social Media

Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors

TOBIAS DIENLIN* AND SABINE TREPTE
School of Communication, University of Hohenheim, Stuttgart, Baden-Württemberg, Germany

Abstract

The privacy paradox states that online privacy concerns do not sufficiently explain online privacy behaviors on social network sites (SNSs). In this study, it was first asked whether the privacy paradox would still exist when analyzed as in prior research. Second, it was hypothesized that the privacy paradox would disappear when analyzed in a new approach. The new approach featured a multidimensional operationalization of privacy by differentiating between informational, social, and psychological privacy. Next to privacy concerns, also, privacy attitudes and privacy intentions were analyzed. With the aim to improve methodological aspects, all items were designed on the basis of the theory of planned behavior. In an online questionnaire with N = 595 respondents, it was found that online privacy concerns were not significantly related to specific privacy behaviors, such as the frequency or content of disclosures on SNSs (e.g., name, cell-phone number, or religious views). This demonstrated that the privacy paradox still exists when it is operationalized as in prior research. With regard to the new approach, all hypotheses were confirmed: Results showed both a direct relation and an indirect relation between privacy attitudes and privacy behaviors, the latter mediated by privacy intentions. In addition, also an indirect relation between privacy concerns and privacy behaviors was found, mediated by privacy attitudes and privacy intentions. Therefore, privacy behaviors can be explained sufficiently when using privacy attitudes, privacy concerns, and privacy intentions within the theory of planned behavior. The behaviors of SNS users are not as paradoxical as was once believed.

Many social network site (SNS) users have pronounced privacy concerns and are afraid that their privacy might be violated online (European Commission, 2011; Hoy & Milne, 2010; Yao, Rice, & Wallis, 2007). However, these concerns and fears rarely impact actual SNS use (Gross & Acquisti, 2005; Nosko, Wood, & Molema, 2010). In prior research, this phenomenon of contradicting privacy attitudes and behaviors was referred to as the *privacy paradox* (Barnes, 2006). Now, several years after its detection in 2006, it seems fruitful to ask: Does the privacy paradox still exist?

This study has three aims: first, to replicate prior research—to see if the privacy paradox still occurs; second, to develop a new and optimized approach that reflects the widely shared understanding of privacy as a multidimensional construct; and third, to find a way to connect both privacy attitudes and privacy behaviors with privacy concerns—to determine if privacy concerns are relevant or not.

The Privacy Paradox

The privacy paradox was first mentioned in an essay by Barnes (2006):

> Herein lies the privacy paradox. Adults are concerned about invasion of privacy, while teens freely give up personal information. This occurs because often teens are not aware of the public nature of the Internet (para. 15).

More specifically, Barnes observed four controversial phenomena of SNS use: (i) the large quantity of information disclosed online, (ii) the illusion of privacy on SNSs, (iii) the discrepancy between context and behavior (indicating that even when people realize that SNSs are a public realm, they still behave as if it was a private place), and (iv) the users' poor understanding of data processing actions by online enterprises (Barnes, 2006). The privacy paradox was debated in many disciplines (Trepte & Reinecke, 2011b) and has been investigated in a number of studies (Trepte, Dienlin, & Reinecke, 2014; Utz & Krämer, 2009). It can be defined as follows: People's concerns toward privacy are unrelated to the privacy behaviors. Even though users have substantial concerns with regard to their online privacy (European Commission, 2011), they engage in self-disclosing behaviors that do not adequately reflect their concerns.

Since that time, several studies have investigated the privacy paradox also empirically. A considerable number of studies have found support for the privacy paradox (Acquisti & Gross, 2006; Ellison, Vitak, Steinfield, Gray, & Lampe, 2011; Gross & Acquisti, 2005; Nosko et al., 2012; Stutzman & Kramer-Duffield, 2010; Taddei & Contena, 2013; Tufekci,

*Correspondence to: Tobias Dienlin, School of Communication, University of Hohenheim, Lehrstuhl für Medienpsychologie (540 F), Stuttgart, Baden-Württemberg, 70599, Germany.
E-mail: tobias.dienlin@uni-hohenheim.de

Received 15 November 2013, Accepted 28 May 2014

2008). For example, Tufekci (2008) demonstrated that "Findings show little to no relationship between online privacy concerns and information disclosure on online social network sites" (p. 20). Tufekci reported that privacy concerns did not relate to the disclosure of the users' authentic names, their political/religious views, and addresses. Similarly, Acquisti and Gross (2006) showed that there was no relation between privacy concerns and posting of cell-phone number on SNSs. Also, Taddei and Contena (2013) found that privacy concerns did not correspond to the posting behavior on Facebook.

However, results on the privacy paradox are manifold, and some studies did not support the privacy paradox (Debatin, Lovejoy, Horn, & Hughes, 2009; Joinson, Reips, Buchanan, & Paine Schofield, 2010; Krasnova, Spiekermann, Koroleva, & Hildebrand, 2010; Mohamed & Ahmad, 2012; Stutzman, Vitak, Ellison, Gray, & Lampe, 2012). Krasnova et al. (2010) found that the perceived privacy risk—a construct that closely resembles privacy concerns—was associated significantly with the respondents' amount of self-disclosure on SNSs. Mohamed and Ahmad (2012) came to the conclusion that "Information privacy concerns explain privacy measure use in social networking sites" (p. 2366). The study of Trepte et al. (2014) on negative online experiences found that even when users were insulted online, they changed only their informational but not their social or psychological privacy behavior. The empirical findings of the privacy paradox, thus, can be considered inconsistent in nature. As a consequence, it seems important to first replicate previous research.

RQ1: Will privacy concerns be related to specific online privacy behaviors such as the indication of (i) the authentic first name, (ii) the authentic last name, (iii) the personal address, (iv) the cell-phone number, (v) political or religious views, and (vi) the frequency of posts on SNSs?

The Privacy Paradox Explicated

In the following, we will explicate the privacy paradox in more detail. First, we will start with the definitions of privacy behaviors and privacy concerns. Afterward, we will aim to unveil the privacy paradox by elaborating on the relation between privacy concerns and privacy behaviors. As a final point, we will suggest a new approach to analyze the privacy paradox.

Privacy Behaviors and Privacy Concerns

Behaviors are usually referred to as any observable actions that are taken by individuals. Privacy behaviors are generally referred to as any behaviors that are intended to optimize the relationship with others by either limiting self-disclosure or by withdrawing from interactions with others (e.g., Altman, 1975; Burgoon, 1982; Dienlin, 2014; Petronio, 2002; Warren & Brandeis, 1890; Westin, 1967). Burgoon (1982), for example, defines privacy on the basis of the following four dimensions: *informational privacy*, which captures the individual control over the processing and transferring of personal information; *social privacy*, which captures the dialectic process of regulating proximity and distance toward others (Burgoon, 1982); *psychological privacy*, which captures the perceived control over emotional and cognitive inputs and outputs; and *physical privacy*, which captures the personal freedom from surveillance and unwanted intrusions upon one's territorial space.

Privacy concerns have been described as "the desire to keep personal information out of the hands of others" (Buchanan, Paine, Joinson, & Reips, 2007, p. 158). Privacy concerns capture the negatively valenced emotional attitude that people feel when personal rights, information, or behaviors are being regressed by others. Privacy concerns can be related to the concept of attitudes. An attitude is "an evaluative integration of cognitions and affects experienced in relation to an object" (Crano & Prislin, 2006, p. 347). Attitudes are studied on two dimensions: instrumental (cognitive) attitudes and experiential (affective) attitudes (Courneya & Bobick, 2000). Generally, attitudes can be both positive and negative. Privacy attitudes and privacy concerns have two major differences with regard to polarity and scope: Concerning polarity, privacy concerns are unipolar, whereas privacy attitudes are bipolar. Privacy concerns measure if, for example, people are afraid that their bank account would be compromised—which can be only a negative feeling. Privacy attitudes measure if, for example, people think that it is either advantageous or disadvantageous to use online banking—which can be either a positive or negative feeling. Concerning scope, the potential application area of privacy attitudes is larger. Privacy attitudes can be specified for every single online privacy action, such as having a Facebook account, indicating one's authentic name, or posting family pictures. Privacy concerns, by contrast, refer to online phenomena that are considered only negative: for example, online identity theft, misuse of personal data, or willful deception in communication processes.

Unveiling the Privacy Paradox

To answer the question of why users engage in paradoxical behavior, we suggest three approaches that are interconnected with each other. First, we will reconsider the definitions of privacy concerns and privacy behaviors. Second, we will refer to social-psychological research and to the general finding of the *attitude–behavior gap* (Fazio & Roskos-Ewoldsen, 1994; LaPiere, 1934). Third, we will critically ask how well previous methodological operationalizations are able to reflect the influence of users' privacy attitudes on behaviors.

With regard to the definition of privacy behaviors, we suggest the following: Burgoon's approach toward privacy was largely acknowledged in the field of online privacy research (Peter & Valkenburg, 2011; Trepte & Reinecke, 2011a). However, so far, only Ruddigkeit, Penzel, and Schneider (2013) used Burgoon's approach in an empirical work. In the majority of studies, a multitude of singular behaviors were used that did not consider the multidimensional nature of privacy (Acquisti & Gross, 2006; Ellison et al., 2011; Gross & Acquisti, 2005; Nosko et al., 2012; Stutzman & Kramer-Duffield, 2010; Taddei & Contena, 2013; Tufekci, 2008). We suggest that a multidimensional approach toward privacy by referring to Burgoon's (1982) definition seems worthwhile. With regard to the definition of privacy concerns, we suggest that it is important to also empirically distinguish between privacy concerns, on the one hand, and privacy attitudes, on the other hand. From a methodological viewpoint, the aforementioned considerations imply a limitation of variance when looking at privacy concerns only.

Generally, a limitation of variance decreases the likelihood to detect significant relations (Schmidt, Hunter, & Urry, 1976). This might partly explain why, so far, it has not been possible to find significant correlations between privacy behaviors and privacy concerns. Integrating privacy attitudes might account for more variance and, thus, statistical power. We therefore suggest that it is important to consider both privacy concerns and privacy attitudes when analyzing the privacy paradox.

A second answer to the question of why users engage in paradoxical behavior might be found in social-psychological research, which has identified the attitude–behavior gap (Fazio & Roskos-Ewoldsen, 1994; LaPiere, 1934). The attitude–behavior gap indicates that attitudes and behaviors are oftentimes unrelated (Kaiser, Byrka, & Hartig, 2010). A number of boundary conditions have been proposed with regard to why and when this gap occurs (cf. Trepte et al., 2014). The first condition addresses the situations in which respondents are asked to express their attitudes (Fazio & Roskos-Ewoldsen, 1994). It has been shown that subjective norms, peer pressure, and situational constraints can have a substantial influence on respondent answering behavior. Respondents might withhold their true opinions or even provide false answers if they perceive strong situational constraints and norms forcing them to do so. Especially with regard to online privacy, users might be aware of contemporary reports in the mass media that often focus on prevailing privacy risks (Teutsch & Niemann, 2014). As a consequence, respondents' answers might largely reflect the public's opinion rather than their own. Another boundary condition states that the strength of the association between attitudes and behaviors largely depends on the strength of the attitude. When attitudes are pronounced or extreme, they are more likely to determine behavior (Kaiser et al., 2010; Petty & Krosnick, 1995). The last condition addresses personal experiences, which determine whether attitudes allow for adequately predicting behaviors. The societal threat posed by online privacy intrusions remains rather obscure, because only a few users have actually experienced privacy violations (European Commission, 2012; Trepte, Dienlin, & Reinecke, 2013). Thus, it seems that privacy attitudes are largely built on heuristics and secondhand experiences. However, firsthand personal experiences are important when it comes to building sustainable attitudes (Tormala, Petty, & Brunol, 2002). A lack of personal experiences with online privacy issues might have the effect that respondents are authentic when indicating that they are afraid of privacy violations; at the same time, this aspect is not relevant and consolidated enough to influence subsequent behavior significantly. In sum, social-psychological research suggests taking into consideration the situational constraints, the prevailing peer pressure, and to refer to both personal experiences and attitude strength when operationalizing privacy attitudes.

A third reason why users may seem to engage in paradoxical behavior comes from a methodological viewpoint. Presumably, privacy behaviors and attitudes have not significantly been related in previous research, because of the ways that they were operationalized. For example, Lewis (2011) operationalized privacy behaviors by asking respondents if they had an open or a public profile, which is a dichotomous measure. Similarly, Acquisti and Gross (2006) asked if their respondents had a Facebook account or not. These measures were then related to metric scales of privacy attitudes. The dichotomy of the dependent variables again implies a possible limitation of variance (Schmidt et al., 1976), which might lead to lower statistical power. In conclusion, methodological considerations suggest operationalizing both privacy attitudes and privacy behaviors on at least ordinal scales.

A New Approach Toward the Privacy Paradox

To carefully consider and combine the aforementioned points in a new approach, it seems important to adopt a theory-based approach that is explicitly configured to explain privacy behaviors by privacy attitudes. For this study, the theory of planned behavior (TPB; Ajzen, 1985; Fishbein & Ajzen, 2010) will, thus, be used owing to four reasons: First, the TPB's variables are conceptualized according to the *principle of compatibility* (Fishbein & Ajzen, 2010). Questions operationalizing attitudes and behaviors comply in terms of *action*, *target*, *context*, and *time* (Fishbein & Ajzen, 2010). Broad and abstract attitudes such as privacy concerns are less likely to predict narrow behaviors such as the use of public versus private profile on SNSs. Questions that share the same content as the behavior—for example, attitudes regarding the use of friend lists on Facebook as a predictor for the factual use of friend lists—are more likely to reflect the reality of users. Second, in the TPB, specific behaviors (e.g., "How often do you go running?") as well as categorical behaviors (e.g., "How often do you exercise?") can be analyzed (Fishbein & Ajzen, 2010). Third, the TPB introduces a third variable to bridge the attitude behavior gap, the *behavioral intention*. For example, some smokers have the attitude that smoking is bad; nonetheless, they continue to smoke. This discrepancy can be explained partly by means of the intention: Although some smokers disapprove of smoking, they simply do not want to stop—because, for example, they think that they are not capable of doing so. Fourth, the TPB was already successfully used to predict diverse behaviors, including physical activities (Hagger, Chatzisarantis, & Biddle, 2002) or sexual intercourse (Terry, Gallois, & McCamish, 1993). For online contexts, Yao (2011) advised an application of the TPB, and Burns and Roberts (2013) used the TPB in a more general study on online privacy behaviors.

Taking into account the findings from the groundwork of psychological research on privacy, it seems important to furthermore consider the different dimensions of privacy (informational, social, psychological, and physical) as suggested by Burgoon (1982). Because physical privacy is not particularly relevant for online contexts and also problematic to operationalize,[1] it will not be addressed in this study. Also, privacy attitudes and privacy concerns will be distinguished; privacy attitudes will be used as main predictor for privacy behaviors. The TPB will, thus, be applied three times: for linking informational privacy attitudes with informational privacy behaviors, for linking social privacy attitudes with social privacy behaviors, and for linking psychological privacy attitudes with psychological privacy behaviors. In conclusion, in Hypothesis 1,

[1]Trepte and Reinecke (2011a) as well as Krämer and Haferkamp (2011) stated that transferring physical privacy to SNSs does not seem to be feasible; Ruddigkeit et al. (2013) also reported difficulties in their empirical attempt to measure physical privacy with regard to digital behaviors. As SNSs deal with the digital representations of people, no physical points of contact are possible.

it is assumed that privacy attitudes and privacy behaviors are related with each other on the basis of an application of the TPB and a multidimensional understanding of privacy attitudes and behaviors.

H1: (i) Informational, (ii) social, and (iii) psychological privacy attitudes will be related significantly to (i) informational, (ii) social, and (iii) psychological privacy behaviors.

As advanced before, the TPB also integrates the behavioral intentions as a mediator between attitudes and behaviors. It has been demonstrated previously that attitudes do not always influence behaviors directly (Fazio & Roskos-Ewoldsen, 1994). Although people might hold a positive attitude, they do not necessarily express this attitude in overt behaviors. The TPB emphasizes that peoples' behavioral intentions are determined not only by their attitudes but also by their subjective norms or their perceived control over changing a behavior (Ajzen, 1991). For aspects of online privacy, looking at behavioral intentions for linking privacy attitudes with privacy behaviors seems fruitful also. Some users might be of the opinion that it is advantageous to use a nickname on Facebook; however, it could well be that all of their friends use their authentic names, which might refrain them from choosing a nickname (subjective norms; c.f., Lewis, 2011). Furthermore, some users might want to employ a friend list on Facebook to restrict access to their profile, but at the same time cannot handle the complex technical infrastructure of Facebook (perceived control). As a result, in Hypothesis 2, the privacy paradox will be addressed accordingly: Intentions will be used as a mediator between privacy attitudes and privacy behaviors, because they include additional information referring to subjective norms and the perceived behavioral control.

H2: (i) Informational, (ii) social, and (iii) psychological privacy attitudes positively influence (i) informational, (ii) social, and (iii) psychological privacy intentions, which in turn positively influence (i) informational, (ii) social, and (iii) psychological privacy behaviors.

The question remains: What is the relation between privacy behaviors and privacy concerns? As shown earlier, privacy concerns differ from privacy attitudes in terms of polarity and scope. Both capture people's opinions toward various aspects in online contexts, but privacy concerns tend to be less specific. For example, one item of the scale used by Buchanan et al. (2007) is "How concerned are you about your privacy online?" By contrast, privacy attitudes are more specific. For example, one item could be "I think that communicating personal information on Facebook is disadvantageous/advantageous." Prior research has shown that privacy concerns do not determine privacy behaviors (Acquisti & Gross, 2006; Tufekci, 2008). However, it can be suggested that privacy concerns might determine privacy attitudes: The general skepticism people have toward actions on the Internet presumably influences their more differentiated attitudes toward diverse privacy behaviors. Although there is not a direct relation of privacy concerns with privacy behaviors, there might be an indirect one. As final assumption, in Hypothesis 3, we, thus, suggest that privacy concerns first influence privacy attitudes, which will then affect privacy behaviors both directly (cf. Hypothesis 1) and indirectly (cf. Hypothesis 2).

H3: Privacy concerns will positively influence (i) informational, (ii) social, and (iii) psychological privacy attitudes, which will in turn positively influence (i) informational, (ii) social, and (iii) psychological privacy intentions and (i) informational, (ii) social, and (iii) psychological privacy behaviors.

METHODS

Procedure and Participants

The study was designed as an online questionnaire with the online tool Sosci Scientific Survey (Leiner, 2014). Participants were recruited from the Socio-Scientific Panel (soscisurvey, 2014). At the time of the study, the panel consisted of 97 199 persons. The panel is noncommercial and based on voluntary participation. Each year, panel members receive on average three emails with invitations to take part in selected studies. In order for a study to be picked for the panel, a formal application and review process takes place. The soscisurvey panel is used regularly for both German and international studies. For example, Gottschalk and Kirn (2013) used the panel in a study on cloud computing featuring the theory of reasoned action (Fishbein & Ajzen, 1975). For further information about the Socio-Scientific Panel itself, see, for example, Leiner (2012) or Soscisurvey (2014).

Five thousand invitation emails were sent to members of the panel. The contact rate was 98.2%; 88 emails could not be delivered successfully. The cooperation rate was 16.3%; 800 people started filling out the questionnaire. The completion rate was 74.5%; 595 respondents finished the questionnaire. Overall, the response rate was 11.9%. The panel's average cooperation rate is 17% (Soscisurvey, 2014), and the response rate of a similar survey 8–10% (Pew Research Center, 2014). Considering the panel objectives and comparable studies, the response rate can be considered satisfactory.

The data for this study consist of $N = 595$ respondents who finished the questionnaire (66.67% women, 33.33% men, $M_{age} = 29.75$ years, age range 15–78 years, $SD = 10.43$ years). The sample is a convenience sample, as participation was on a voluntary basis.

Measures

Fishbein and Ajzen's (2010) guidelines were used for designing the TPB items. Categorical behaviors were conceptualized according to the principle of compatibility (Fishbein & Ajzen, 2010). For example, the item measuring informational privacy behavior was "How much identifying information (*content*) have you now (*time*) posted (*action*) on Facebook (*context*)?" All items were designed and presented in German. The items that were used for this study can be found translated into English in Table 1. Back and forward translation was carried out in order to guarantee translation accuracy. For each variable's mean, standard deviation, internal consistency, range, and skewness, see Table 2.

Privacy Behaviors

Informational privacy behaviors measured how many identifying pieces of information people shared on their Facebook

Table 1. Item pool used for H1, H2, and H3

	Informational privacy	Social privacy	Psychological privacy
Behaviors	How much identifying information have you now posted on FB? How much identifying information can generally be found on your FB profile? How precisely can you be identified on FB by strangers?	Do you right now restrict access to your FB profile? How strongly is the visibility of content on your FB profile restricted? How strongly is your FB profile restricted regarding the accessibility for particular persons?	How many personal things do you communicate on FB? How exactly is your personality resembled by your FB profile? How personal is your FB profile?
Intentions	How much identifying information do you currently want to provide on FB? How much identifying information about yourself do you generally want to have on your FB profile? How precisely do you want to be identifiable for strangers on FB?	How strongly do you want to restrict your FB profile right now? How strongly do you want that the visibility of content on your FB profile is restricted? How strongly restricted do you want your FB profile to be for certain persons?	How much personal information do you want to communicate on FB? How exactly do you want your FB profile to resemble your entire personality? How personal do you want your FB profile to be?
Attitudes	I think that giving information on FB that identifies me is: 1. not useful–very useful 2. disadvantageous–advantageous 3. worrying–not worrying 4. very dangerous–not dangerous 5. careless–not careless 6. very bad–very good	I think that restricting access to one's FB profile is: 1. not useful–very useful 2. disadvantageous–advantageous 3. worrying–not worrying 4. unpleasant–not unpleasant 5. very mean–very fair 6. very bad–very good	I think that communicating personal information on FB is: 1. not useful–very useful 2. disadvantageous–advantageous 3. worrying–not worrying 4. very dangerous–not dangerous 5. not pleasant–very pleasant 6. very bad–very good
Privacy concerns	1. In general, how concerned are you about your privacy while you are using the internet? Are you concerned 2. about online organizations not being who they claim they are? 3. that you are asked for too much personal information when you register or make online purchases? 4. about online identity theft? 5. about people online not being who they say they are? 6. that information about you could be found on an old computer? 7. about people you do not know obtaining personal information about you from your online activities? 8. that a message you send online may be read by someone else besides the person you sent it to? 9. that a message you send someone online may be inappropriately forwarded to others? 10. about messages you receive online not being from whom they say they are?		

Table 2. Psychometric properties of the study variables

				Range		
Variable	*M*	*SD*	α	Potential	Actual	Skew
Privacy behaviors (specific)						
Indication of						
First name	85%	36%		0–1	0–1	−1.43
Last name	72%	45%		0–1	0–1	−0.96
Address	6%	24%		0–1	0–1	3.49
Phone number	3%	16%		0–1	0–1	5.84
Religious/political views	39%	49%		0–1	0–1	0.42
Frequency of posts	4.98	1.35		1–7	1–7	−0.56
Privacy behaviors (categorical)						
Informational	4.83	1.33	.77	1–7	1.0–7.0	−0.51
Social	5.28	1.48	.85	1–7	1.0–7.0	−1.07
Psychological	4.96	1.28	.82	1–7	1.0–7.0	−0.45
Privacy intentions						
Informational	5.42	1.21	.81	1–7	1.3–7.0	−0.70
Social	5.50	1.26	.78	1–7	1.0–7.0	−1.02
Psychological	4.98	1.36	.85	1–7	1.0–7.0	−0.50
Privacy attitudes						
Informational	4.50	1.10	.87	1–7	1.0–7.0	0.11
Social	5.85	0.93	.81	1–7	2.5–7.0	−0.58
Psychological	4.72	1.11	.89	1–7	1.3–7.0	0.22
Privacy concerns	3.22	0.76	.84	1–5	1.2–5.0	−0.11

profile. Participants answered three items on 7-point Likert scales, ranging from (for example) 1 = *none* to 7 = *very much*. The scale was recoded for analyses with lower values expressing lesser extent as opposed to higher values expressing a higher extent of privacy behavior. Social privacy behaviors captured whether people restricted access to their Facebook profile. Participants answered three items on 7-point Likert scales, ranging from (for example) 1 = *not at all* to 7 = *very much*. No recoding was applied. Psychological privacy captured the degree to which people had an intimate and personal Facebook profile. Participants answered three items on 7-point Likert scales, ranging from (for example) 1 = *very impersonal* to 7 = *very personal*. For psychological privacy, the scale was recoded with lower scale values expressing lower and higher values expressing a higher level of psychological privacy.

Privacy Intentions

Adhering to the principle of compatibility (Fishbein & Ajzen, 2010), three corresponding privacy intention items were modeled that paralleled items for privacy behavior in terms of action, target, context, and time. Three informational privacy intention items measured how many identifying pieces of information people currently *wanted* to share on their Facebook profile. Three social privacy intention items comprised how strongly people *wanted* to restrict access to their Facebook profile. Three psychological privacy intention items encompassed the degree to which people *wanted* to have an intimate and personal Facebook profile.

Privacy Attitudes

Privacy attitudes were operationalized by items that measured the general appraisal of each particular privacy behavior (Fishbein & Ajzen, 2010). Informational privacy attitudes measured respondents' appraisal of posting identifying information on Facebook. For each dimension, items consisted of an introduction, which was followed by six different semantic differentials. Semantic differentials work for both unidimensional (*dangerous* versus *not dangerous*) and bidimensional (*bad* versus *good*) pairs (Fishbein & Ajzen, 2010). For the informational privacy attitude, the introduction was "I think that providing information on FB that identifies me is: …" The following semantic differentials were answered on a 7-point scale and ranged, for example, from 1 = *useful* to 7 = *not useful.* Social privacy attitude comprised respondents' appraisal of restricting access to a Facebook profile. The introduction was "I think that restricting access to one's FB profile is: …" The semantic differentials were answered on a 7-point scale ranging from, for example, 1 = *very mean* to 7 = *very fair*. Psychological privacy attitude captured respondents' appraisal of sharing personal pieces of information on Facebook. The introduction was "I think that communicating personal information on FB is: …" Again, respondents indicated their answers on a 7-point semantic differential, ranging from, for example, 1 = *very dangerous* to 7 = *not dangerous.*

Online Privacy Concerns

Online privacy concerns measure the degree to which people are worried regarding their online privacy. Ten items from the 18-item scale by Buchanan et al. (2007) were used (Table 1). For reasons of parsimony, only 10 items that fit the study's needs best were chosen. One example item was "Are you concerned about people online not being who they say they are?" Respondents answered all items on a 5-point Likert scale, ranging from 1 = *not at all* to 5 = *very strongly*.

Specific Privacy Behaviors

In order to answer the research questions, respondents were asked several questions that captured specific privacy behaviors. Items were chosen with the aim to replicate those studies that found evidence in favor of the privacy paradox. Thus, all items resembled the ones used by Tufekci (2008), Acquisti and Gross (2006), and Taddei and Contena (2013). For all items, possible answers were 0 = *no*, 1 = *yes*. Respondents were asked the following questions: (i) "On Facebook, I use my authentic first name (that is, the exact way it is written in my passport)." (ii) "On Facebook, I use my authentic second name (that is, the exact way it is written in my passport)." (iii) "On Facebook, I indicate my current address." (iv) "On Facebook, I indicate my telephone number." (v) "On Facebook, have you ever posted a religious, political, or ethical statement?" (vi) "How often do you leave a post on Facebook?" This time, possible answers were 1 = *never*, 2 = *every other month*, 3 = *on a monthly basis*, 4 = *several times a month*, 5 = *several times a week*, 6 = *once a day*, and 7 = *several times a day*.

Data Analysis

The results of Cronbach's alpha tests showed that all variables had at least satisfactory internal consistencies (Table 2). All variables were tested for normal distribution with Kolmogorov–Smirnov tests. With large sample sizes, Kolmogorov–Smirnov tests overestimate significant differences from the normal distribution (Field, 2009). Hence, random subsamples of $n = 30$ were drawn. The tests did not produce significant results; thus, the results did not imply that the data were not distributed normally.

One of the aims of the study was to replicate already existing research. In those studies, regression analyses were used (e.g., Utz & Krämer, 2009). As a result, RQ1 was answered via bivariate regressions. The hypotheses were analyzed with structural equation models (SEMs). H1, H2, and H3 were analyzed together in one single SEM. As the hypotheses were tested along three dimensions—informational, social, and psychological privacy—three different SEMs were computed: In SEM_{INF}, H1, H2, and H3 were tested for the dimension of informational privacy; in SEM_{SOC}, H1, H2, and H3 were tested for the dimension of social privacy; and in SEM_{PSY}, H1, H2, and H3 were tested for the dimension of psychological privacy. The structure of the SEMs was configured *a priori*. For the design of the SEMs, see Figure 1.

Missing values were considered missing at random and were replaced with the full information maximum likelihood (Arbuckle, 1996). To estimate effect sizes, the correlation coefficient r was used as suggested by Field (2009). Values exceeding $r = .1$ were considered small effects, $r = .3$ medium effects, and $r = .5$ large effects. For structural equation modeling, beta coefficients can be interpreted as r-values (Durlak, 2009). Hypotheses were tested with a two-tailed .05 level of significance. The data

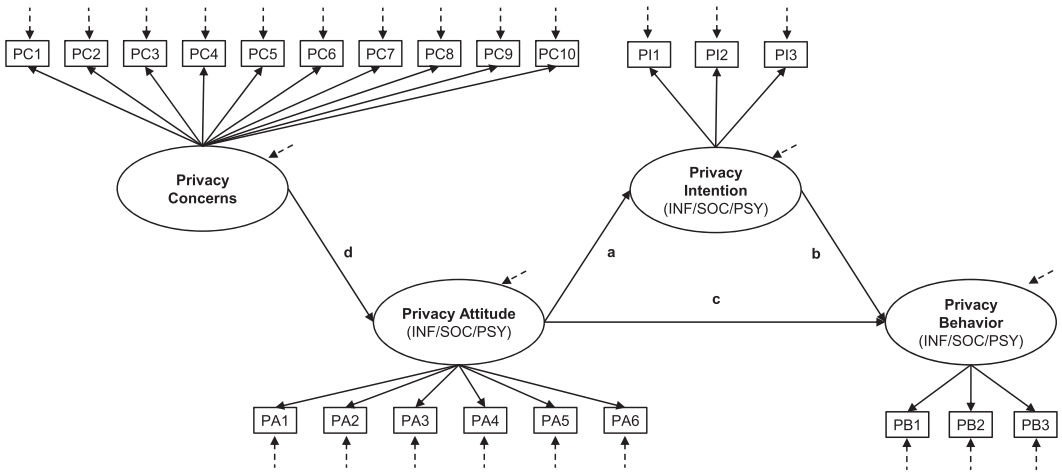

Figure 1. SEMs with the direct and indirect influences of privacy attitudes and privacy concerns on privacy behaviors. Latent variables are represented by ovals, and observed variables by rectangles. Dashed arrows represent error terms/residuals. The model was designed for informational privacy (SEM_{INF}), social privacy (SEM_{SOC}), and psychological privacy (SEM_{PSY})

were analyzed with the Software R, version 3.0.1 (R Core Team, 2014). To conduct the SEMs, the package lavaan, version 0.5-14 (2012), was used (Rosseel, 2012). Furthermore, the packages QuantPsyc, moments, boot, psych, and memisc were used.

RESULTS

Research Questions: Replicating Previous Research on the Privacy Paradox

RQ1 asked if privacy concerns were related to specific privacy behaviors, such as the indication of (i) the authentic first name, (ii) the authentic second name, (iii) the personal address, (iv) the cell-phone number, (v) political or religious views, and (vi) the frequency of posts on SNSs. The results indicated the following:

RQ1a: Regression analyses showed privacy concerns to be unrelated to the online disclosure of the authentic first name ($F(1, 586) = 0.51$, $p = .478$, $b < -0.01$, $\beta = -.03$).

RQ1b: Privacy concerns were again unrelated to the online disclosure of the authentic second name ($F(1, 586) = 3.00$, $p = .084$, $b < -0.01$, $\beta = -.07$).

RQ1c: Here, privacy concerns were related to the online disclosure of the personal address ($F(1, 586) = 9.40$, $p = .002$, $b = -0.03$, $\beta = -.13$). This implies that people who are more concerned about their privacy are less likely to disclose their personal address online. The size of the effect of privacy concerns on the online disclosure of the personal address was small.

RQ1d: Privacy concerns were unrelated to the disclosure of the cell-phone number ($F(1, 582) = 0.35$, $p = .552$, $b < -0.01$, $\beta = -.02$).

RQ1e: Privacy concerns were not associated with postings of political or religious views on Facebook ($F(1, 585) = 2.32$, $p = .128$, $b < -0.01$, $\beta = -.063$).

RQ1f: Privacy concerns were not related to the frequency of posts on SNSs ($F(1, 585) = 2.25$, $p = .134$, $b < 0.01$, $\beta = .06$).

In sum, with the exception of the minor correlation with address disclosure, the results are consistent with previous research. The results indicate that online privacy concerns remain unrelated to specific privacy behaviors such as the frequency and contents of online disclosures.

Hypotheses: A Multidimensional Perspective on the Privacy Paradox

Model Fit

H1, H2, and H3 were tested for the three dimensions informational, social, and psychological privacy. Thus, three different SEMs were computed. The three SEMs were first tested regarding model fit. The following guidelines for testing model fit criteria were applied: χ^2 divided by degrees of freedom was not to exceed a value of 5 (as referred to by Marsh & Hocevar, 1985); as a combined rule, together with an standardized root mean square residual (SRMR) of 0.06, the comparative fit index (CFI), Tucker–Lewis coefficient (TLI), and relative noncentrality index (RNI) were not to fall below 0.90 (Hu & Bentler, 1999); the root mean square error of approximation (RMSEA) were not to exceed values of 0.08 (Browne & Cudeck, 1992).

SEM_{INF} showed adequate model fit ($\chi^2/df = 3.57$, $p < .001$, CFI = 0.91, TLI = 0.90, RNI = 0.91, RMSEA = 0.07, 90% CI [0.06, 0.07], SRMR = 0.06). SEM_{SOC} also showed adequate model fit ($\chi^2/df = 3.35$, $p < .001$, CFI = 0.90, TLI = 0.89, RNI = 0.90, RMSEA = 0.06, 90% CI [0.06, 0.07], SRMR = 0.06). However, the TLI did not reach the expected 0.90. SEM_{PSY} showed good model fit ($\chi^2/df = 3.14$, $p < .001$, CFI = 0.93, TLI = 0.92, RNI = 0.93, RMSEA = 0.06, 90% CI [0.06, 0.07], SRMR = 0.05). For a comprehensive overview, see Table 3. In conclusion, the *a priori* models showed adequate model fit. However, further analyses suggested model adjustments, which will be explained later.

Factorial Validity

Table 4 shows the SEMs' measurement model. All items except item $ATT_{soc}3$ exceeded a threshold of 0.50, implying

Table 3. Fit indices for the three SEMs of informational (SEM_{INF}), social (SEM_{SOC}), and psychological (SEM_{PSY}) privacy

		SEM_{INF}		SEM_{SOC}		SEM_{PSY}	
Fit indices	Criteria	*A priori*	*Post hoc*	*A priori*	*Post hoc*	*A priori*	*Post hoc*
χ^2		720.34	534.38	677.26	443.50	634.68	449.07
df		202	179	202	178	202	179
χ^2/df	<5[a]	3.57	2.99	3.35	2.49	3.14	2.51
CFI	>0.90[b]	0.91	0.94	0.90	0.94	0.93	0.96
TLI	>0.90[b]	0.90	0.93	0.89	0.93	0.92	0.95
RNI	>0.90[b]	0.91	0.94	0.90	0.94	0.93	0.96
RMSEA	<0.08[c]	0.07 [0.06, 0.07]	0.06 [0.05, 0.06]	0.06 [0.06, 0.07]	0.05 [0.04, 0.06]	0.06 [0.06, 0.07]	0.05 [0.05, 0.06]
SRMR	<0.08[d]	0.06	0.06	0.06	0.05	0.05	0.05

Note:
[a]Marsh and Hocevar (1985).
[b]Hu and Bentler (1999).
[c]Browne and Cudeck (1992).
[d]Hu and Bentler (1999).

Table 4. Indices for measurement models: factor loadings (γ), composite reliability (Rel(ξ)), and average variance extracted (AVE) of the SEMs

	SEM			SEM			SEM		
	Informational privacy			Social privacy			Psychological privacy		
	γ	Rel(ξ)	AVE	γ	Rel(ξ)	AVE	γ	Rel(ξ)	AVE
Privacy behaviors		0.79	0.57		0.85	0.66		0.83	0.62
PB1	0.88***			0.83***			0.62***		
PB2	0.83***			0.88***			0.83***		
PB3	0.51***			0.72***			0.89***		
Privacy intentions		0.85	0.66		0.95	0.60		0.86	0.68
PI1	0.92***			0.57***			0.65***		
PI2	0.91***			0.85***			0.88***		
PI3	0.54***			0.83***			0.92***		
Privacy attitudes		0.93	0.55		0.93	0.54		0.95	0.60
PA1	0.77***			0.77***			0.86***		
PA2	0.77***			0.70***			0.82***		
PA3	0.67***			0.46[a]***			0.62***		
PA4	0.63***			0.69***			0.63***		
PA5	0.71***			0.56***			0.77***		
PA6	0.81***			0.71***			0.85***		
Privacy concerns		0.83	0.35		0.83	0.35		0.83	0.35
PC1	0.58***			0.57***			0.56***		
PC2	0.61***			0.62***			0.62***		
PC3	0.62***			0.61***			0.61***		
PC4	0.56***			0.56***			0.57***		
PC5	0.57***			0.58***			0.58***		
PC6	0.51[a]***			0.52[a]***			0.51[a]***		
PC7	0.63***			0.64***			0.62***		
PC8	0.61***			0.61***			0.61***		
PC9	0.50***			0.50***			0.50***		
PC10	0.61***			0.61***			0.62***		

Note:
[a]Item was deleted *post hoc*.
***$p < .001$.

adequate overall model fit. Two items were removed: item $ATT_{soc}3$ ("I think that restricting access to one's FB profile is: worrying—not worrying") was removed for inadequate fit ($\gamma = 0.46$). Item PC6 ("Are you concerned that information about you could be found on an old computer?") was removed because it is not necessarily associated with privacy concerns in online contexts and was thus deemed theoretically irrelevant. To check for individual cross-loadings and error covariances, modification indices were computed. No significant cross-loadings were found that warranted inclusion in the model. With respect to error covariances, indices showed that some items ($ATT_{soc}5 + ATT_{soc}6$, PC4 + PC5, and PC8 + PC9 + PC10) were correlated substantially. As the items' formulations were especially parallel (Table 1), the correlations seemed plausible and were integrated into the new model. To further check for factorial validity, the average variance extracted (AVE) was computed. Except for the privacy concerns, the values for all variables were above the minimum of AVE = 0.5 (Fornell & Larcker, 1981; Table 5).

Table 5. Estimates of effects for privacy concerns and privacy attitudes on privacy behaviors for the three SEMs of informational (SEM_{INF}), social (SEM_{SOC}), and psychological (SEM_{PSY}) privacy

	SEM_{INF}			SEM_{SOC}			SEM_{PSY}		
Effects	*b*	95% CI	*β*	*b*	95% CI	*β*	*b*	95% CI	*β*
Direct effects									
a	0.67	[0.59, 0.76]	.68***	0.72	[0.58, 0.86]	.61***	0.40	[0.34, 0.47]	.58***
b	0.70	[0.59, 0.82]	.65***	0.68	[0.49, 0.86]	.45***	0.73	[0.63, 0.82]	.79***
c [H1]	0.12	[0.01, 0.23]	.11*	0.36	[0.16, 0.56]	.20***	0.05	[0.01, 0.10]	.08*
d	0.92	[0.69, 1.15]	.42***	0.44	[0.30, 0.59]	.33***	0.63	[0.39, 0.88]	.25***
Indirect effects									
$a \times b$ [H2]	0.47	[0.38, 0.57]	.44***	0.49	[0.34, 0.63]	.28***	0.29	[0.23, 0.35]	.46***
$d \times a \times b$	0.43	[0.30, 0.57]	.18***	0.22	[0.13, 0.31]	.09***	0.19	[0.10, 0.27]	.11***
$d \times c$	0.11	[0.01, 0.21]	.05*	0.16	[0.06, 0.26]	.07**	0.03	[0.01, 0.07]	.02*
Total effects									
$(a \times b) + c$	0.59	[0.49, 0.69]	.55***	0.85	[0.68, 1.02]	.48***	0.35	[0.28, 0.41]	.55***
$(d \times c) + (d \times a \times b)$ [H3]	0.54	[0.39, 0.70]	.23***	0.38	[0.24, 0.51]	.16***	0.22	[0.13, 0.31]	.14***

Note:
$^{*}p < .05$; $^{**}p < .01$; $^{***}p < .001$.

To analyze factor reliability, the composite reliability Rel(ξ) was computed. All variables were above the minimum of Rel(ξ) = 0.6 (Bagozzi & Yi, 1988). In general, analyses showed that the privacy concern scale did not perform well. However, it was maintained owing to its importance in answering research questions. The removal of the two items ($ATT_{soc}3$ and PC5) and the inclusion of the item error covariances improved model fit significantly. The three new models showed good fit (Table 3).

Hypothesis 1

Hypothesis 1 stated that (i) informational, (ii) social, and (iii) psychological privacy attitudes would have a direct positive effect on corresponding privacy behaviors. Results indicated that informational privacy attitudes did have a positive direct effect on informational privacy behavior ($b = 0.12$, 95% CI [0.05, 0.19], $\beta = .11$, $p = .04$, $SE = 0.06$). This implies that people who favor disguising their identity on Facebook are also less identifiable on Facebook. The effect is small. For social privacy, results showed that social privacy attitudes also did have a positive direct effect on social privacy behavior ($b = 0.36$, 95% CI [0.16, 0.56], $\beta = .20$, $p = .001$, $SE = 0.10$), demonstrating that people who have a positive opinion toward restricting access to their profiles on Facebook also employ more profile restrictions on Facebook. The effect is also small. In terms of psychological privacy, results showed that psychological privacy attitudes did have a positive direct effect on psychological privacy behavior ($b = 0.05$, 95% CI [0.01, 0.10], $\beta = .08$, $p = .030$, $SE = 0.02$). This implies that people who hold the belief that it is not good to have a Facebook profile full of personal information also have a Facebook profile that is less personal. Again, the effect is small.

Hypothesis 2

Hypothesis 2 stated that (i) informational, (ii) social, and (iii) psychological privacy attitudes would positively influence (i) informational, (ii) social, and (iii) psychological privacy intentions, which in turn would positively influence (i) informational, (ii) social, and (iii) psychological privacy behaviors. Results showed that informational privacy attitudes did have a positive indirect effect on informational privacy behaviors, mediated by informational privacy intentions ($b = 0.47$, 95% CI [0.38, 0.57], $\beta = .44$, $p < .001$, $SE = 0.05$). This implies that people who have a positive opinion on disguising their identity on Facebook also report an increased intention to do so, which finally leads to the fact that they are less identifiable on Facebook. The effect can be considered medium to large. For social privacy, it was revealed that social privacy attitudes also had a positive indirect effect on social privacy behaviors, mediated by social privacy intentions ($b = 0.49$, 95% CI [0.34, 0.63], $\beta = .28$, $p < .001$, $SE = 0.07$). This indicates that people who have a positive opinion on restricting access to their profiles on Facebook also have an increased intention to do so, which in turn leads to the fact that they employ more profile restrictions on Facebook. The effect is to be considered small to medium. Regarding psychological privacy, results demonstrated that attitudes also had a positive indirect effect on psychological privacy behaviors mediated by psychological privacy intentions ($b = 0.29$, 95% CI [0.23, 0.35], $\beta = .46$, $p < .001$, $SE = 0.03$). People who disapprove of having a Facebook profile showing personal information also have the intention to withhold personal information and therefore have a Facebook profile that is less personal. The effect can be considered medium to large.

In technical terms, the three significant direct effects of H1 and the three significant indirect effects of H2 demonstrate partial mediation. To assess mediation size, the proportion of mediation was computed (e.g., Iacobucci, Saldanha, & Deng, 2007). For all three dimensions, the proportion of the indirect effect on the total effect was large (informational = 0.80, social = 0.59, psychological = 0.84). Hence, mediation analyses also confirmed the importance of using intentions as mediator between privacy attitudes and privacy behaviors.

Hypothesis 3

Hypothesis 3 posited that privacy concerns would positively influence (i) informational, (ii) social, and (iii) psychological privacy attitudes, which in turn would positively influence (i) informational, (ii) social, and (iii) psychological privacy intentions and the (i) informational, (ii) social, and (iii) psychological privacy behaviors. Results showed that privacy concerns did

have an indirect effect on informational privacy behaviors ($b = 0.54$, 95% CI [0.39, 0.70], $\beta = .23$, $p < .001$, $SE = 0.08$). First, privacy concerns were related to informational privacy attitudes; informational privacy attitudes in turn had both a direct effect on informational privacy behaviors (as was already shown in H1) and an indirect effect (as already shown in H2). This implies that respondents who have pronounced privacy concerns are also more skeptical regarding the posting of identifiable information on Facebook, which in turn is both directly and indirectly associated with a profile that features less identifiable information online. The effect is small. The effect also was shown for social privacy behaviors ($b = 0.38$, 95% CI [0.24, 0.51], $\beta = .16$, $p < .001$, $SE = 0.07$). This indicates that people who have pronounced privacy concerns also think that it is good to restrict access to their Facebook profile, which in turn is directly and indirectly associated with a more restricted Facebook profile. The effect is small. Finally, the effect also existed for psychological privacy behaviors ($b = 0.22$, $\beta = .12$, $p < .001$, $SE = 0.05$). This implies that respondents who have increased privacy concerns also believe that it is good not to post too much personal information on Facebook. This attitude is then both directly and indirectly accompanied with a less personal Facebook profile. The effect is small.

Additional analyses and modification indices showed that no direct effect of privacy concerns on privacy behavior existed. For an overview of all effects, see Table 5. For a visual representation of the results of H1–H3, see Figure 2.

DISCUSSION

Implications of Results

Replication of the Privacy Paradox

The first aim of this study was to replicate former studies that investigated the privacy paradox. Results of prior research were twofold: Some studies showed that privacy concerns were not associated with specific privacy behaviors (Acquisti & Gross, 2006; Trepte et al., 2014; Ellison et al., 2011; Gross & Acquisti, 2005; Nosko et al., 2012; Stutzman & Kramer-Duffield, 2010; Taddei & Contena, 2013; Tufekci, 2008); others found that by using variables that closely refer to privacy concerns (e.g., perceived privacy risks, Mohamed & Ahmad, 2012), privacy behaviors can be explained to a certain degree (Debatin et al., 2009; Joinson et al., 2010; Krasnova et al., 2010; Mohamed & Ahmad, 2012; Stutzman et al., 2012).

The results of this study showed that privacy concerns were mostly unrelated to specific privacy behaviors on SNSs. People who were concerned about their privacy were not less likely to indicate their authentic first name, their authentic second name, their cell-phone number, or their political views on Facebook. Also, privacy concerns were demonstrated to be unrelated to the frequency of status posts on Facebook. However, one inconsistent observation was made: Privacy concerns were negatively associated with the disclosure of the personal address on Facebook. Taken together, the results suggest the following: Privacy concerns do not sufficiently predict specific privacy behaviors, and even when they do, the effects are small. This shows that privacy concerns do not play a major part when it comes to explaining specific actions on SNSs. Thus, it can be summarized that also after several years, the privacy paradox can still be found—as long as it is investigated as suggested and outlined earlier.

New Approach to the Privacy Paradox

In a second aim of the research, a new approach toward the privacy paradox was suggested. This new approach was based on the TPB and a multidimensional definition of privacy as referring to informational, psychological, and social aspects.

It was demonstrated that informational, social, and psychological privacy attitudes are significantly related to informational, social, and psychological privacy behaviors. It did make a difference if people thought that it is, for example, (i) useful to indicate one's authentic name on Facebook (informational privacy dimension), (ii) good to use friend lists to restrict access to one's profile (social privacy dimension), or (iii) dangerous to disclose personal pieces of information on Facebook

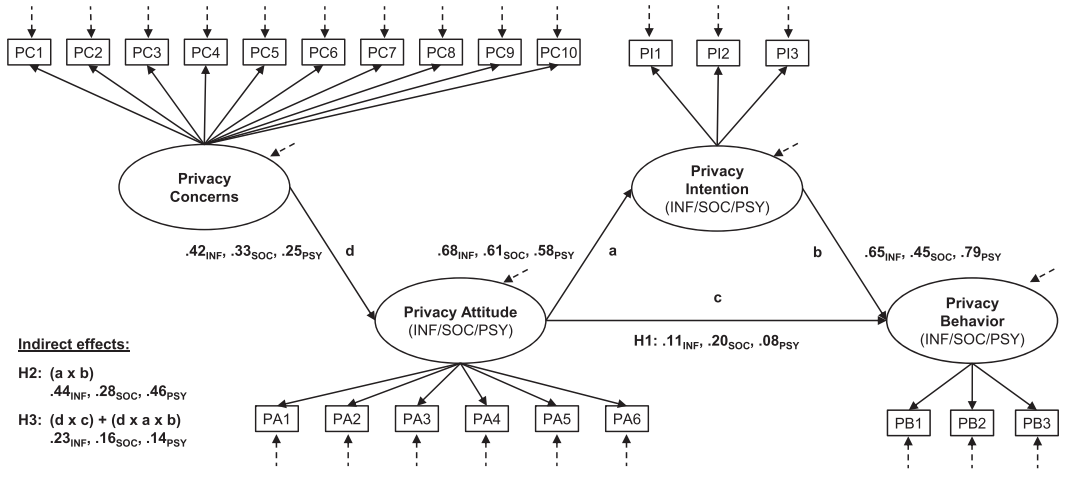

Figure 2. Visualization of effects for the three SEMs of informational privacy (SEM_{INF}), social privacy (SEM_{SOC}), and psychological privacy (SEM_{PSY}). Path *c* represents Hypothesis 1, path $a * b$ represents Hypothesis 2, and path $(d * c) + (d * a * b)$ represents Hypothesis 3. All effects are significant on the basis of a level of significance of $p < .05$

(psychological privacy dimension). If users of SNSs are of these opinions, their attitudes do affect their corresponding privacy behaviors. In addition to the direct effect, attitudes were found to also indirectly affect behavior through intentions: Attitudes are associated with an increased intention to show these behaviors, which in turn is associated with an increased privacy behavior. More important, effect sizes indicate that these associations are substantial: Privacy attitudes are decisive when it comes to understanding people's privacy behaviors.

In addition, results showed that privacy concerns were indirectly associated with privacy behaviors on all three dimensions. Although privacy concerns are not directly related to privacy behaviors, they nonetheless affect privacy behaviors indirectly. Thus, when operationalized adequately, it can be shown that privacy concerns play a significant role when it comes to explaining privacy behaviors. The results correspond with the findings of Taddei and Contena (2013): In their study, privacy concerns also did not relate directly to privacy behaviors. The authors nevertheless found that privacy concerns interact with the general trust users have toward webpages, which is then associated directly with self-disclosure behaviors.

Arguably, the methodological alterations have proven to be worthwhile. The significant effects showed that applying the principle of compatibility to measures (Fishbein & Ajzen, 2010) generally narrowed and even bridged the attitude–behavior gap (Kaiser et al., 2010). Also, the differentiation between the three dimensions of privacy can be considered worthwhile: The three SEMs differed regarding the coefficients' estimates. For example, the relation between intentions and behaviors was the strongest in SEM_{PSY}. The coefficient $\beta = .79$ implies that people are capable of disclosing almost exactly as much information as they want to disclose. By contrast, the coefficient $\beta = .47$ for the same relation in the SEM_{SOC} indicates that even when people intend to restrict access to their Facebook profile, they are not equally capable of showing that behavior.

Limitations and Future Perspective

First, the results are based on cross-sectional data. Thus, the direction or causality of effects cannot be demonstrated statistically. It appears that attitudes influence behaviors; however, as has been shown for cognitive dissonance (Festinger, 1957), actions can also influence attitudes. Second, participation was voluntary, self-selective, and resulted in a convenience sample. This implies that the sample cannot be considered statistically representative. Third, the data are based on respondents' self-reports. This is especially relevant when it comes to measuring behavior; an objective procedure is to be preferred here. All the same, it has been shown for behaviors on SNSs that self-reports correspond closely to objective data (Hampton, Sessions Goulet, Marlow, & Rainie, 2012). Fourth, with respect to the SEM's quality, although adequate, the factorial validity and the model fit could have been better: Of the 58 items in use, one item performed poorly, and eight only just adequately. Also, the privacy concern scale needs to be reconsidered regarding the just acceptable internal factorial validity. It might prove worthwhile to update the scale as to better correspond to contemporary online contexts. As a final note, the TPB was designed to measure repeated behavior from a longitudinal perspective (Fishbein & Ajzen, 2010). This suggests an experimental or panel study with multiple measurements. Behaviors that were used in this study cannot be regarded as repeated; most people choose their profile name only once. Even so, it has been shown that a substantial part of users do change their privacy settings at some point—Utz and Krämer (2009) found that 90% of all users already did so.

The present study can be further analyzed regarding the three dimensions' distinct characteristics; for reasons of parsimony, those analyses were not included here. In addition, to corroborate the findings, future studies might want to develop alternative ways to measure overt behaviors. For example, the current results could be validated in experimental settings: Do observable privacy behaviors change when privacy attitudes are manipulated by, for example, exposure to news stories of online data fraud?

Conclusion

The findings of our study suggest the following: First, the privacy paradox is still a phenomenon to be detected in empirical data when analyzed exactly as it was carried out in prior research. Second, and more important, the privacy paradox disappears (i) when distinguishing between privacy concerns and privacy attitudes, (ii) by using the TPB as a theory-driven framework to operationalize the research design, and (iii) by differentiating privacy dimensions (informational, social, and psychological) as proposed by Burgoon (1982). In conclusion, the privacy paradox can be dissolved: The results of our study clearly show that online privacy behaviors are not paradoxical in nature but that they are based on distinct privacy attitudes. The privacy paradox can be considered a relic of the past.

REFERENCES

Acquisti, A., & Gross, R. (2006, June). *Imagined communities: Awareness, information sharing, and privacy on the Facebook*. Paper presented at the 6th Workshop on privacy enhancing technologies, Cambridge, UK. Retrieved from: http://people.cs.pitt.edu/~chang/265/proj10/zim/imaginedcom.pdf

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179–211. doi:10.1016/0749-5978(91)90020-T

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In J. Kuhl, & J. Beckmann (Eds.), *Action control* (pp. 11–39). Berlin, Germany: Springer.

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

Arbuckle, J. L. (1996). Full information estimation in the presence of incomplete data. In G. A. Marcoulides, & R. E. Schumacker (Eds.), *Advanced structural equation modeling* (pp. 243–277). Mahwah, NJ: Lawrence Erlbaum.

Bagozzi, R. P., & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science, 16*(1), 74–94. doi:10.1007/BF02723327

Barnes, S. B. (2006). A privacy paradox: Social networking in the Unites States. *First Monday*, *11*(9). Retrieved from http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1394/1312

Browne, M. W., & Cudeck, R. (1992). Alternative ways of assessing model fit. *Sociological Methods & Research, 21*(2), 230–258. doi:10.1177/0049124192021002005

Buchanan, T., Paine, C., Joinson, A. N., & Reips, U.-D. (2007). Development of measures of online privacy concern and protection for use on the internet. *Journal of the American Society for Information Science and Technology, 58*(2), 157–165. doi:10.1002/asi.20459

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

Burns, S., & Roberts, L. (2013). Applying the theory of planned behaviour to predicting online safety behaviour. *Crime Prevention and Community Safety, 15*(1), 48–64. doi:10.1057/cpcs.2012.13

Courneya, K. S., & Bobick, T. M. (2000). Integrating the theory of planned behavior with the processes and stages of change in the exercise domain. *Psychology of Sport and Exercise, 1*(1), 41–56. doi:10.1016/S1469-0292(00)00006-6

Crano, W. D., & Prislin, R. (2006). Attitudes and persuasion. *Annual Review of Psychology*, *57*(1), 345–374. doi:10.1146/annurev.psych.57.102904.190034

Debatin, B., Lovejoy, J. P., Horn, A.-K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication, 15*(1), 83–108. doi:10.1111/j.1083-6101.2009.01494.x

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

Durlak, J. A. (2009). How to select, calculate, and interpret effect sizes. *Journal of Pediatric Psychology*, *34*(9), 917–928. doi:10.1093/jpepsy/jsp004

Ellison, N. B., Vitak, J., Steinfield, C., Gray, R., & Lampe, C. (2011). Negotiating privacy concerns and social capital needs in a social media environment. In S. Trepte, & L. Reinecke (Eds.), *Privacy online. Perspectives on privacy and self-disclosure in the social web* (pp. 19–32). Berlin, Germany: Springer.

European Commission. (2011). *Special Eurobarometer 359: Attitudes on data protection and electronic identity in the European Union*. Brussels, Belgium: European Commission. Retrieved from http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

European Commission. (2012). *Pan-European survey of practices, attitudes and policy preferences as regards personal identity data management.* Brussels, Belgium: European Commission. Retrieved from http://bookshop.europa.eu/en/pan-european-survey-of-practices-attitudes-and-policy-preferences-as-regards-personal-identity-data-management-pbLFNA25295/?CatalogCategoryID=zQoKABstlL0AAAEjCpEY4e5L

Fazio, R. H., & Roskos-Ewoldsen, D. R. (1994). Acting as we feel: When and how attitudes guide behavior. In T. C. Brock, & S. Shavitt (Eds.), *Persuasion: Psychological insights and perspectives* (2nd ed., pp. 41–62). Thousand Oaks, CA: Allyn & Bacon.

Festinger, L. (1957). *A theory of cognitive dissonance*. Stanford, CA: Stanford University Press.

Field, A. P. (2009). *Discovering statistics using SPSS* (3rd ed.). Los Angeles, CA: Sage Publications.

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention, and behavior: An introduction to theory and research*. Reading, MA: Addison-Wesley.

Fishbein, M., & Ajzen, I. (2010). *Predicting and changing behavior: The reasoned action approach*. New York, NY: Psychology Press.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39–50.

Gottschalk, P. D. I., & Kirn, S. (2013). Cloud computing as a tool for enhancing ecological goals? *Business & Information Systems Engineering, 5*(5), 299–313. doi:10.1007/s12599-013-0284-2

Gross, R., & Acquisti, A. (2005, November). *Information revelation and privacy in online social networks*. Paper presented at the ACM Workshop on Privacy in the Electronic Society, Alexandria, VA.

Hagger, M. S., Chatzisarantis, N. L. D., & Biddle, S. J. H. (2002). A meta-analytic review of the theories of reasoned action and planned behavior in physical activity: Predictive validity and the contribution of additional variables. *Journal of Sport & Exercise Psychology, 7*(3), 3–32.

Hampton, K., Sessions Goulet, L., Marlow, C., & Rainie, L. (2012). Why most Facebook users get more than they give. Retrieved from Pew Internet & American Life Project website: http://www.pewinternet.org/2012/02/03/why-most-facebook-users-get-more-than-they-give/

Hoy, M. G., & Milne, G. R. (2010). Gender differences in privacy-related measures for young adult Facebook users. *Journal of Interactive Advertising, 10*(2), 28–45. doi:10.1080/15252019.2010.10722168

Hu, L.-T., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling, 6*(1), 1–55. doi:10.1080/10705519909540118

Iacobucci, D., Saldanha, N., & Deng, X. (2007). A meditation on mediation: Evidence that structural equations models perform better than regressions. *Journal of Consumer Psychology, 17*(2), 140–154. doi:10.1016/S1057-7408(07)70020-7

Joinson, A. N., Reips, U.-D., Buchanan, T., & Paine Schofield, C. B. (2010). Privacy, trust, and self-disclosure online. *Human–Computer Interaction, 25*(1), 1–24. doi:10.1080/07370020903586662

Kaiser, F. G., Byrka, K., & Hartig, T. (2010). Reviving Campbell's paradigm for attitude research. *Personality and Social Psychology Review, 14*(4), 351–367. doi:10.1177/1088868310366452

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

Krämer, N. C., & Haferkamp, N. (2011). Online self-presentation: Balancing privacy concerns and impression construction on social networking sites. In S. Trepte, & L. Reinecke (Eds.), *Privacy online. Perspectives on privacy and self-disclosure in the social web* (pp. 127–141). Berlin, Germany: Springer.

LaPiere, R. T. (1934). Attitudes vs. actions. *Social Forces*, *13*(2), 230–237. doi:10.2307/2570339

Leiner, D. J. (2012, March). *SoSci Panel: The noncommercial online access panel*. Poster presented at the General Online Research (GOR 12) conference, Mannheim, Germany. Retrieved from https://www.soscisurvey.de/panel/download/SoSciPanel.GOR2012.pdf

Leiner, D. J. (2014). SoSci Survey (Version 2.4.00-i) [Computer Software]. Available from https://www.soscisurvey.de.

Lewis, K. (2011). The co-evolution of social network ties and online privacy behavior. In S. Trepte, & L. Reinecke (Eds.), *Privacy online. Perspectives on privacy and self-disclosure in the social web* (pp. 91–110). Berlin, Germany: Springer.

Marsh, W. M., & Hocevar, D. (1985). Application of confirmatory factor analysis to the study of self-concept: First- and higher order factor models and their invariance across groups. *Psychological Bulletin, 97*(3), 562–582. doi:10.1037/0033-2909.97.3.562

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

Nosko, A., Wood, E., Kenney, M., Archer, K., Pasquale, D., Molema, S., & Zivcakova, L. (2012). Examining priming and gender as a means to reduce risk in a social networking context: Can stories change disclosure and privacy setting use when personal profiles are constructed? *Computers in Human Behavior, 28*(6), 2067–2074. doi:10.1016/j.chb.2012.06.010

Nosko, A., Wood, E., & Molema, S. (2010). All about me: Disclosure in online social networking profiles: The case of FACEBOOK. *Computers in Human Behavior, 26*(3), 406–418. doi:10.1016/j.chb.2009.11.012

Peter, J., & Valkenburg, P. M. (2011). Adolescents' online privacy: Toward a developmental perspective. In S. Trepte, & L. Reinecke (Eds.), *Privacy online. Perspectives on privacy and self-disclosure in the social web* (pp. 221–234). Berlin, Germany: Springer.

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

Petty, R. E., & Krosnick, J. (1995). *Attitude strength: Antecedents and consequences*. Hillsdale, NY: Erlbaum.

Pew Research Center. (2014). Survey questions. Retrieved from Pew Research Center website: http://www.pewresearch.org/files/2014/01/Survey-Questions_Facebook.pdf

R Core Team. (2014). R: A Language and Environment for Statistical Computing [Computer Software]. Vienna, Austria: R Foundation for Statistical Computing. Available from http://www.R-project.org

Rosseel, Y. (2012). lavaan: An R package for structural equation modeling. *Journal of Statistical Software, 48*(2). Retrieved from http://www.jstatsoft.org/v48/i02/paper

Ruddigkeit, A., Penzel, J., & Schneider, J. (2013). Dinge, die meine Eltern nicht sehen sollten. Strategien der Privacy-Regulierung unter deutschen Facebook-Nutzern [Things my parents should not get to see: Strategies of privacy regulation by German Facebook users]. *Publizistik, 58*(3), 305–325. doi:10.1007/s11616-013-0183-z

Schmidt, F. L., Hunter, J. E., & Urry, V. W. (1976). Statistical power in criterion-related validation studies. *Journal of Applied Psychology, 61*(4), 473–485. doi:10.1037/0021-9010.61.4.473

Soscisurvey. (2014). SoSci Panel für Wissenschaftler [SoSci panel for researchers]. Retrieved from https://www.soscisurvey.de/panel/researchers.php

Stutzman, F., & Kramer-Duffield, J. (2010). Friends only: Examining a privacy-enhancing behavior in Facebook. In E. Mynatt (Ed.), *Proceedings of the 28th International Conference on Human Factors in Computing Systems* (pp. 1553–1562). New York, NY: ACM.

Stutzman, F., Vitak, J., Ellison, N. B., Gray, R., & Lampe, C. (2012). Privacy in interactions: Exploring disclosure and social capital in Facebook. In J. Breslin (Ed.), *Proceedings of the 8th International AAAI Conference on Weblogs and Social Media*. Palo Alto, CA: AAAI Press.

Taddei, S., & Contena, B. (2013). Privacy, trust and control: Which relationships with online self-disclosure? *Computers in Human Behavior, 29*(3), 821–826. doi:10.1016/j.chb.2012.11.022

Terry, D., Gallois, C., & McCamish, M. (Eds.). (1993). *The theory of reasoned action and health care behaviour*. Oxford, UK: Pergamon Press.

Teutsch, D., & Niemann, J. (2014, May). *Social network sites as a threat to users' self-determination and security: A framing analysis of German newspapers*. Paper presented at the 64th Annual Conference of the International Communication Association, Seattle, WA.

Tormala, Z. L., Petty, R. E., & Brunol, P. (2002). Ease of retrieval effects in persuasion: A self validation analysis. *Personality and Social Psychology Bulletin, 28*(12), 1700–1712. doi:10.1177/014616702237651

Trepte, S., Dienlin, T., & Reinecke, L. (2014). Risky behaviors: How online experiences influence privacy behaviors. In B. Stark, O. Quiring, & N. Jackob (Eds.), *Von der Gutenberg-Galaxis zur Google-Galaxis [From the Gutenberg galaxy to the Google galaxy]* (pp. 225–244). Wiesbaden, Germany: UVK.

Trepte, S., Dienlin, T., & Reinecke, L. (2013). Privacy, self-disclosure, social support, and social network site use. *Research report of a three-year panel study.* Retrieved from University of Hohenheim website: https://opus.uni-hohenheim.de/volltexte/2013/889/

Trepte, S., & Reinecke, L. (2011a). The social web as shelter for privacy and authentic living. In S. Trepte, & L. Reinecke (Eds.), *Privacy online. Perspectives on privacy and self-disclosure in the social web* (pp. 61–74). Berlin, Germany: Springer.

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

Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society, 28*(1), 20–36. doi:10.1177/0270467607311484

Utz, S., & Krämer, N. (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). Retrieved from: http://cyberpsychology.eu/view.php?cisloclanku=2009111001&article=2

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, *4*(5), 193–220.

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

Yao, M. Z. (2011). Self-protection of online privacy: A behavioral approach. In S. Trepte, & L. Reinecke (Eds.), *Privacy online. Perspectives on privacy and self-disclosure in the social web* (pp. 111–126). Berlin, Germany: Springer.

Yao, M. Z., Rice, R. E., & Wallis, K. (2007). Predicting user concerns about online privacy. *Journal of the American Society for Information Science and Technology, 58*(5), 710–722. doi:10.1002/asi.20530