Article

SM+S
social media + society

Social Media + Society
July-September 2022: 1–18

DOI: 10.1177/20563051221126085
journals.sagepub.com/home/sms
SAGE

Twitter Users' Privacy Behavior: A Reasoned Action Approach

Peter Schmidt[1,2], Galit Gordoni[3], Icek Ajzen[4], Christoph Beuthner[5], Eldad Davidov[6,7], Henning Silber[5], Holger Steinmetz[8], and Bernd Weiß[5]

Abstract

Social networking sites have become a predominant means of communication across the globe. Activities on these sites generate massive amounts of personal information and raise concerns about its potential abuse. Means designed to protect the user's privacy and prevent exploitation of confidential data often go unused. In this study, we draw on the theory of planned behavior, a reasoned action approach, to explain intentions to adopt privacy behaviors on social networking sites, with a focus on Twitter users. Consistent with the theory, an online survey of Twitter users ($n = 1{,}060$) found that instrumental and experiential attitudes and descriptive and injunctive subjective norms regarding these behaviors were direct predictors of intentions. Perceived behavioral control had a moderating effect, such that subjective norm was a better predictor of intentions for participants high as opposed to low in perceived control. We briefly discuss the implications of these results for developing theory-driven and evidence-based interventions to promote privacy behavior.

Keywords

online privacy behavior, reasoned action approach, theory of planned behavior, social network sites, Twitter users, attitudes

Introduction

The use of social networking sites has become a ubiquitous phenomenon on a global scale. These sites promote interpersonal communication as one of their primary activities. They enable users to create a personal profile, establish and maintain social connections, and interact with streams of content (Rains & Brunner, 2015). One important driver of the popularity of social networking sites is their business model, which provides a platform for users to create and share information free of charge while creating a profit by selling the individual's private information to stakeholders (e.g., for marketing purposes) (Masur & Scharkow, 2016; Zhong et al., 2011). The exponential increase in the amount of personal information collected by the platforms combined with the development of powerful technologies to analyze users' information, preferences, and behavior raises serious concerns about users' vulnerability to abuse of their disclosed data. A recent example is the Facebook-Cambridge Analytica scandal where, without consent, the personal data of Facebook users were harvested by the company Cambridge Analytica, to be used predominantly for political advertising (Epstein & Quinn, 2020; Liang et al., 2017; Matzner et al., 2016). In line with these concerns, the privacy precautions taken by social networking providers and responsible privacy-protecting behaviors by users have become a highly debated issue (Nissenbaum, 2015; Rains & Brunner, 2015; Stoycheff et al., 2017). Following Nissenbaum's conceptualization of privacy and her discussion of the societal and individual problems involved (Nissenbaum, 2004, 2010), research interest in understanding the underlying conditions and context of an individual's decision to disclose personal information is rising (Wu et al., 2020). Therefore, learning about the prevalence and antecedents of privacy-protecting behavior is important.

[1]University of Giessen, Germany
[2]University Medical Center Mainz, Germany
[3]The Open University of Israel, Israel
[4]University of Massachusetts, USA
[5]GESIS—Leibniz Institute for Social Sciences, Germany
[6]University of Cologne, Germany
[7]University of Zurich, Switzerland
[8]University of Trier, Germany

Corresponding Author:
Peter Schmidt, Center for International Development and Environmental Research (ZEU), University of Giessen, Senckenbergstraße 3, 35390 Giessen, Germany and Department of Psychosomatics, University Medical Centre Mainz, Untere Zahlbacherstrasse 8, Mainz, 55131, Germany.
Email: peter.schmidt@sowi.uni-giessen.de

Most previous social networking studies have concentrated on Facebook, a focus that has been criticized as too limited in scope and that has resulted in calls for more research examining social networking as part of a larger media repertoire (see, for example, Phua et al., 2017; Rains & Brunner, 2015; Stoycheff et al., 2017). Consistent with this recommendation, in the present study, we examined intentions to engage in privacy behavior on Twitter, a currently popular social networking site that serves as a platform for interpersonal communication as well as a microblogging platform (Marwick & Boyd, 2011) for mass communication (French & Bazarova, 2017). On Twitter, information is open to everyone unless users actively customize their privacy settings (Liang et al., 2016). Studying privacy behavior on this alternative platform has the potential to enrich our understanding of the processes underlying privacy behavior in a high-vulnerability environment.

Not only has considerable online privacy research tended to focus narrowly on Facebook but this research has also been largely descriptive in nature, relying primarily on ad hoc hypotheses to predict and explain online privacy behavior with an emphasis on risk perception and privacy concerns (see Baruh et al., 2017). This research is discussed below. Other hypothesized predictors have included privacy management abilities (Dienlin & Metzger, 2016; Dienlin & Trepte, 2015; Epstein & Quinn, 2020), need for self-identity (Marwick & Boyd, 2011; Wu, 2019), attitude (Dienlin & Trepte, 2015; Epstein & Quinn, 2020), norms (Dienlin & Trepte, 2015), personality traits and intelligence (Nardis & Panek, 2019; Sindermann et al., 2021), privacy literacy (Desimpelaere et al., 2020), trust in online relationships (Aïmeur & Sahnoune, 2020), and background variables such as culture (Baruh et al., 2017; Liang et al., 2016), gender, and age (Baruh et al., 2017; Walrave et al., 2012).

In contrast, we relied on an empirically validated general theory of human behavior, the theory of planned behavior (TPB; Ajzen, 1991, 2012), to identify the primary determinants of intentions to adopt online privacy measures. In addition, we tested several novel aspects of the TPB introduced in its most recent version (Fishbein & Ajzen, 2010): the distinctions between experiential and instrumental attitudes and between descriptive and injunctive norms, as well as interactions among the predictors of intention. The application of this latest version of the TPB to online privacy was designed to enrich existing knowledge on a highly disputed topic with substantial relevance for the well-being of individuals and society.

Online Privacy Behavior

Privacy behavior is an active process in which individuals limit access to personal information to attain a balance between desired and actual privacy (Altman, 1975; Petronio, 2002). According to communication privacy management theory (Petronio, 2002), individuals regard their private information as their personal assets, that is, information that belongs to them. Thus, information, as any other private asset, can be managed according to self-calculation of the risks and benefits of information disclosure. Management of the privacy boundary (i.e., drawing the border between private and public information) includes boundary regulation (Masur & Scharkow, 2016; Petronio, 2002). In the sphere of social networking sites (SNS), privacy setting is conceived of as a type of privacy boundary management ranging between passive and active behaviors (Choi & Bazarova, 2015). On SNS, users can manage the disclosure of private information by passively accepting the platform's default privacy settings or by actively changing the settings in accordance with their own preferences for information sharing (Choi & Bazarova, 2015). The user's control over which content to share and with whom is, however, limited to the set of privacy settings available on a given platform and can change over time in accordance with the company's policy, public regulations, and technological progress. Twitter, the platform we are investigating here, offers two privacy settings: *public* and *protected*. When signing up for a Twitter account, tweets are public by default; anyone with or without a Twitter account can view and interact with the user's tweets. Activation of the protected mode requires changing the account's default settings. In this mode, users receive a request when new people want to follow them, which they can approve or deny, and only approved followers have access to the users' tweets (see Twitter Safety and Security Information, 2020).

Of course, in either mode, it is up to the user to decide how much and what kind of private information to disclose in their tweets. Even so, the default public setting creates a high level of potential vulnerability. It can make information available to the public that the user would prefer to keep limited to a certain group of individuals. For instance, public disclosure of geolocation data can invite burglary by showing that the user is far away from home, perhaps on vacation (Humphreys et al., 2014).

The changes in Twitter's account settings offer additional options related to matters of privacy. Among other things, users can decide whether anyone can send messages to them or add them to group conversations. In addition, the individual user can decide whether people who already have the user's email address or phone number can be allowed to find and connect with the user on Twitter. Clearly, it is in the best interest of Twitter users to inform themselves about the platform's privacy options and to make an active decision on whether to retain the default settings or change them to fit their privacy preferences. The processes underlying this decision are the focus of the present investigation.

The theory of communication privacy management (Petronio, 2002) suggests that privacy decisions involve balancing the perceived risks of disclosure (privacy concerns) and the perceived benefits of sharing private

information (see also Kehr et al., 2015). A meta-analysis of 166 studies on online privacy conducted in 34 countries (Baruh et al., 2017) examined the relationship between privacy concerns and the use of social networking sites and the relationship between privacy concerns and disclosure of private information among people who do use such sites. While correlations between privacy concerns and intentions to use social networking sites or actual use of such sites were not significant (see also Norberg et al., 2007), users of social networking sites with higher privacy concerns had weaker intentions to share personal information ($r = -.22$) and had stronger intentions to adopt privacy protective measures ($r = .31$). Moreover, users with higher privacy concerns actually shared less personal information ($r = -.13$) and were more likely to employ privacy protective measures ($r = .17$). Although statistically significant, it should be noted that the effects of privacy concerns were, on average, rather weak, accounting for no more than 10% of the variance in intentions to disclose private information and for less than 3% of the variance in disclosure behavior.

The Theory of Planned Behavior

In the present study, we relied on the theory of planned behavior (TPB; Ajzen, 1991, 2012), a reasoned action approach (Fishbein & Ajzen, 2010), as our conceptual framework. This theory has been used successfully to explain and predict behavior in a multitude of behavioral domains (Bosnjak et al., 2020), from physical activity to drug use, recycling to choice of travel mode, and safer sex to consumer behavior, to name just a few (for meta-analytic syntheses of this research see, for example, Albarracin et al., 1997; Armitage & Conner, 1999; Boerman et al., 2018; Buechi et al., 2021; Hagger et al., 2002; McDermott et al., 2015; Riebl et al., 2015; Sheeran & Taylor, 1999; Winkelnkemper et al., 2019; Young & Quan-Haase, 2013).

Application of the TPB to online privacy behavior has been recommended in systematic literature reviews, referring to the merits of employing a well-established theoretical model to enrich our understanding of this behavior (e.g., Barth & de Jong, 2017; Baruh et al., 2017). The benefits of applying this theory are its continuous and replicated utility for the prediction of intentions and behavior and for designing theory-driven interventions (Ajzen & Schmidt, 2020; for a meta-analysis, see Steinmetz et al., 2016). A few prior studies of privacy-related behavior in the context of the TPB have addressed the disclosure of sensitive attitudes in survey research (Gordoni & Schmidt, 2010), intentions to share personal information in a blogging context (Hsu & Lin, 2008), posting a comment on an online news website (Soffer & Gordoni, 2018), and adopting general safety measures, such as reading a website's privacy policy and checking one's computer for spyware (Burns & Roberts, 2013).

As in other "reasoned action" approaches (see Fishbein & Ajzen, 2010), the immediate antecedent of behavior in the TPB is the *intention* to perform the behavior in question; the stronger the intention, the more likely it is that the behavior will follow. Thus, all else equal, intentions to adopt online privacy measures should be predictive of actual privacy behavior. However, various factors may prevent people from acting on their intentions. The degree to which people have control over their behavior depends on their ability to overcome barriers such as a lack of knowledge about online privacy options and on the presence of facilitating factors such as assistance provided by others. In light of these considerations, the TPB postulates that the degree of *behavioral control* moderates the effect of intention on behavior: The greater the actor's control over the behavior, the more likely it is that the intention will be carried out.

In the present study, our focus is on the determinants of intentions to use the means provided on the Twitter platform to increase user privacy. According to the TPB, three kinds of considerations guide the formation of intentions. One type of consideration are beliefs about the likely positive and negative consequences and experiences resulting from the performance of the behavior (*behavioral beliefs*). Aggregated, these beliefs lead to the formation of a favorable or unfavorable *attitude toward the behavior (a)*. As noted, the focus of much research in the domain of online privacy behavior has been on the perceived risks and benefits of disclosing private information. These perceptions may be viewed as beliefs about possible positive and negative outcomes of disclosure or, conversely, as possible beliefs about adopting privacy measures. As such, these considerations would be expected to influence attitudes toward the adoption of privacy measures.

A second type (b) of consideration are beliefs about the expectations and behaviors of significant social referents (*normative beliefs*), which produce perceived social pressure to engage or not to engage in the behavior, or *subjective norm*. The third type of consideration *(c) are control beliefs*, which result in *perceived behavioral control (PBC)* or a sense of *self-efficacy* (Bandura, 1997). In the TPB, a hierarchical model is hypothesized, in which instrumental and experiential evaluations constitute the first-order factors and (a) attitude a second-order factor; injunctive and descriptive norms constitute the first-order factors and (b) subjective norm a second-order factor; and capacity and autonomy constitute the first-order factors and (c) PBC a second-order factor (see Figure 1). Empirical evidence supports the hierarchical structure of these components in the model of behavioral prediction (Hagger & Chatzisarantis, 2005).

In most applications of the TPB, the three second-order predictors of intention (attitude, subjective norm, and PBC) have been treated as additive factors although, in the original formulation of the theory, Ajzen (1985) discussed the possibility of an interaction between attitude and subjective norm with PBC. In the theory's current formulation (Fishbein & Ajzen, 2010), favorable attitudes and supportive subjective norms *motivate* people to perform the behavior, but this motivation leads them to form an intention to

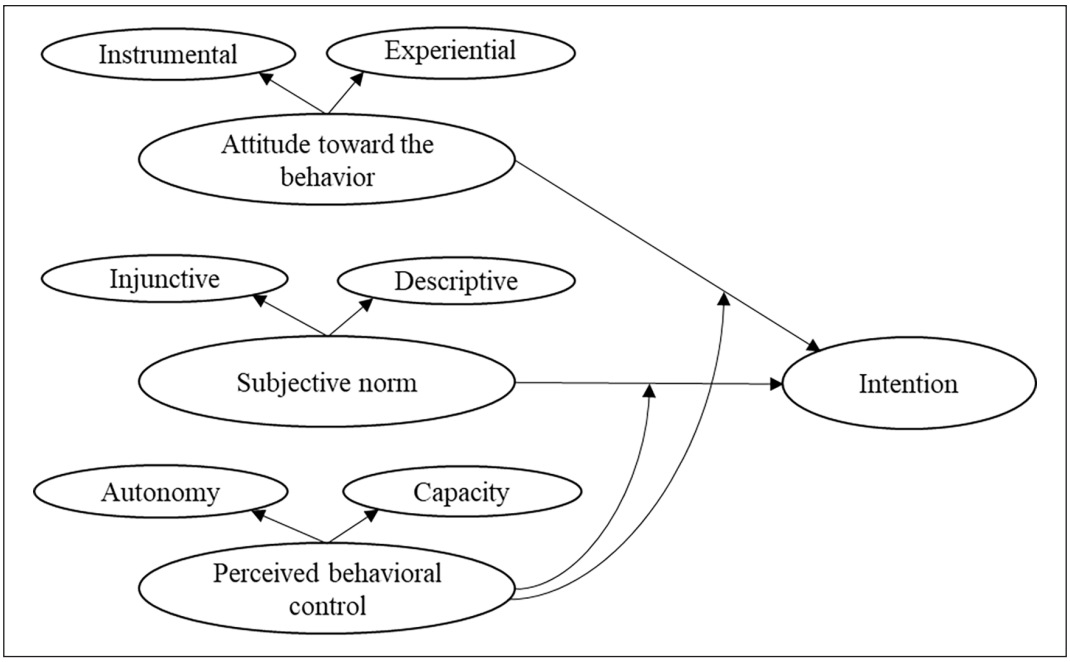

Figure 1. TPB model for the intention to use online privacy settings. Attitudes toward the behavior, subjective norm, and perceived behavioral control serve as second-order factors (Brown, 2015).

engage in the behavior only to the extent that they believe they are capable of performing the behavior in question. This implies that PBC moderates the effects of attitude and of subjective norm on intention. A few recent studies provide empirical evidence in support of the proposed interaction effects (e.g., Hukkelberg et al., 2014; La Barbera & Ajzen, 2020; Yzer & Van Den Putte, 2014). The version of the TPB model applied in the present study is depicted in Figure 1.

Past Behavior as a Background Factor

Many factors not included in the TPB may influence intentions, including demographic characteristics (age, gender, race, education, income, etc.), personality traits, life values, political ideology, mood and emotions, and so forth. In the TPB, these kinds of variables are considered *background factors* that have no direct effects on intention or behavior but can influence them indirectly by way of the more proximal antecedents of intention and behavior specified in the theory. General privacy concerns may also be considered a background factor in relation to online privacy behavior (see Dienlin & Trepte, 2015). Of particular interest for the present study is the past performance of the behavior under investigation. Past experience with the behavior can provide information about the *actual* (as opposed to anticipated) outcomes and experiences, about reactions by significant others, as well as about facilitating or impeding factors. This feedback is likely to change some of the behavioral, normative, and control beliefs and thus influences future behavioral intentions. Like other background factors, past behavior can influence intentions in two ways. First, it can exert its influence indirectly by affecting the proximal determinants of intentions, that is, attitudes, subjective norm, and/or PBC. Although the theory predicts full mediation, past research has frequently also reported direct effects of past behavior on intentions (see Fishbein & Ajzen, 2010, pp. 287–290, for a discussion). Second, past behavior can moderate the effects of attitudes, subjective norm, and/or PBC on intentions. As past experience with a behavior increases, the relative importance of these variables as predictors of intentions may change. All of these possibilities are examined in the present study.

Hypotheses

The present study affords an overall test of the hierarchical TPB model in the context of privacy intentions (excluding behavior), as depicted in Figure 1. Beyond the expectation of a good fit between model and data, the following hypotheses are advanced.

1. The more positive the attitude toward the use of Twitter's options to increase user privacy, the higher is the intention to perform the behavior.
2. The stronger the subjective norm for the use of Twitter's options to increase user privacy, the higher is the intention to perform the behavior.
3. PBC over the use of Twitter's options to increase user privacy moderates the relation between attitude and

intention: The association of attitude with intention is stronger when PBC is high than when it is low.
4. PBC over the use of Twitter's options to increase user privacy moderates the relation between subjective norm and intention: The association of subjective norm with intention is stronger when PBC is high than when it is low.
5. The relation between past use of Twitter's options to increase user privacy and intentions to use these options is at least partially mediated by attitude, subjective norm, and/or PBC.

In addition to the fifth hypothesis, we also examined the possibility that past use of Twitter's options to increase user privacy moderates the relations between attitude, subjective norm, and PBC on the one hand and intention on the other.

Method

Data, Variables, and Statistical Analysis

Respondents were invited to participate by a commercial online access panel provider (respondi). A quota sample of German adults was drawn with quotas on age (six levels of web usage based on the age distribution in the panel), education (three levels based on the educational system, equally distributed), and sex (two levels, equally distributed). In addition, respondents were screened based on their Twitter usage and the manufacturer of their smartphone (Apple or Samsung). All respondents who owned a Twitter account received the target questions. The participants were shown a list of privacy measures and they were asked whether these are among Twitter's privacy measures. The list included such items as "The option to limit the visibility of updates or content to a selected, specific selected, specific group (e.g., friends)," "The option to remove tags (e.g., your own name) from postings or photos," and "The possibility to decide that the own profile cannot be found by others." Due to space limitations, we cannot show the full list of privacy measures here, but it can be found in Appendix E.

The survey was fielded between 28 November and 17 December 2019 ($N = 3{,}136$). Invited panel members received an email from the panel provider that included a link to the survey. Those who clicked on the link were directed to the first page of the survey, which delivered general information on the survey and explained the data protection procedure. This was followed by screening questions. In response to the 26,339 invitations that were issued, a total of 10,484 respondents viewed the first page of the survey (participation rate: 39.8%); 6,963 panel members who did not fulfill the quota assignment were screened out (screen-out rate: 65.5%). Another 485 respondents dropped out of the survey, leading to a completion rate of 86.2%.

In this study, we used a subsample that includes Twitter users only ($N = 1{,}060$). The median response time of the survey was 12.4 min. The Twitter user sample consisted of 32.9% female respondents and 67.1% male respondents of which 22.5% were low-educated (up to 9 years of schooling), 29.3% medium-educated (10 years of schooling), and 48.1% high-educated (at least 12 years of schooling). Moreover, 38.3% of the respondents were aged between 18 and 29 years, 21% aged between 30 and 39 years, 24.2% aged between 40 and 49 years, and 16.4% aged 50 and older.

Items measuring the TPB constructs, that is, attitude, subjective norm, PBC, and intention to use the platform's options to increase user's privacy were administered to the subsample of Twitter users. Table 1 lists the items used to measure the TPB constructs, their means, standard deviation, median, skewness, and kurtosis.

No indication for non-normality of individual univariate distributions was evident, with skewness and kurtosis $<|1|$ for all items (see Curran et al., 1996). The percentage frequency distribution of TPB items is presented in Appendix A. Correlations among the TPB items are presented in Appendix B.

Our measurement model contains three second-order factors and seven first-order factors. The model adheres to the TPB postulation that attitude, subjective norm, and PBC each have a second-order factorial structure (see Figure 1). All questionnaire items were measured on 7-point scales (item wordings are reported in Table 1).

The analysis included the following steps. First, we validated our measures of the TPB constructs using confirmatory factor analysis (CFA). CFA is the recommended procedure for validating measurement models when a theory-driven item development procedure is used (Brown, 2015). The second step included validation of the structural relations among the TPB constructs. AMOS program Version 25 (Arbuckle, 2017) was used for testing the measurement (step 1) and structural models (step 2). Missing data were dealt with by using pairwise deletion (item nonresponse for all items was less than 1%; see, e.g., Schafer & Graham, 2002). We employed multigroup structural equation modeling (MGSEM) (Rigdon et al., 1998) and compared the effect of attitude and subjective norm between two groups: respondents with low PBC and respondents with high PBC. To form the two groups, the PBC variable was dichotomized into two categories (low and high PBC) based on the calculation of the composite score for the PBC scale, with the scale median ($Me = 5.5$) serving as a cutoff value for inclusion in the two groups. In the second model, past behavior served as a moderator for the effects of attitude, subjective norm, and PBC on intention. Past behavior (one-indicator measure) was dichotomized into two groups—low frequency and high frequency—with the item median serving as the cutoff value ($Me = 3$).

Multiple fit statistics were used for evaluating different aspects of model fit (Brown, 2015; Kline, 2015; West et al., 2012): (1) absolute fit indices (an exact-fit test of model chi-square and the standardized root-mean-square residual [SRMR]), (2) incremental fit indices (mean-square error of

Table 1. Descriptive Statistics of Items in the TPB Measures.

Items	*N*	*M*	*SD*	Me	Sk	Kur
Attitude						
For me, to use one or more of Twitter's options to increase user privacy is all items range from 1 (*extremely negative* to 7 (*extremely positive*)						
att1. bad–good	1,056	4.93	1.23	5	−0.31	0.27
att2. useless–useful	1,057	5.12	1.22	5	−0.35	0.03
att3. unpleasant–pleasant	1,056	5.06	1.16	5	−0.12	−0.21
att4. uninteresting–interesting	1,052	4.99	1.26	5	−0.25	0.08
Subjective norm						
s_n1. I believe that most people who are important to me think that I should make more use of the privacy options of Twitter. Item range from 1 (*completely false*) to 7 (*completely true*).	1,058	3.76	1.61	4	0.02	−0.63
s_n2. Most people whose opinions I value would approve of my use of one or more of Twitter's options to increase my privacy. Item range from 1 (*extremely unlikely*) to 7 (*extremely likely*).	1,057	3.8	1.58	4	−0.1	−0.69
s_n3. Most people I respect and admire use one or more of the options, on Twitter, to improve their privacy. Item range from 1 (*extremely unlikely*) to 7 (*extremely likely*).	1,055	4.29	1.46	4	−0.3	−0.2
s_n4. In Twitter, most people who are similar to me use one or more of the options to improve their privacy. Item range from 1 (*extremely disagree*) to 7 (*extremely agree*).	1,056	4.42	1.4	4	−0.32	0.02
Perceived behavioral control (All items range from 1 [*extremely disagree*] to 7 [*extremely agree*])						
pbc1. I am confident that I am able to use one or more of the options in Twitter to secure my privacy.	1,056	5.25	1.36	5	−0.73	0.44
pbc2. To use one or more of Twitter's options to increase my privacy is up to me.	1,057	5.44	1.37	6	−0.7	0.13
pbc3. If I wanted to, I could easily use one or more of the options in Twitter to protect my privacy.	1,055	5.4	1.33	6	−0.67	0.16
pbc4. To use one or more of Twitter's options to increase my privacy is under my control.	1,057	5.27	1.35	5	−0.55	-0.03
Intention						
int1. I intend to use one or more of Twitter's options to increase user privacy. Item range (after recode) from 1 (*definitely do not intend to*) to 7 (*definitely intend to*).	1,056	4.6	1.52	5	−0.26	−0.45
int2. I will use one or more of Twitter's options to increase user privacy. Item range from 1 (*extremely unlikely*) to 7 (*extremely likely*).	1,053	4.75	1.45	5	−0.49	−0.1
int3. I am ready to use one or more of Twitter's options to increase user privacy. Item range from 1 (*extremely false*) to 7 (*extremely true*).	1,053	5.09	1.26	5	−0.48	0.36
int4. I plan to use one or more of Twitter's options to increase user privacy. Item range from 1 (*extremely disagree*) to 7 (*extremely agree*).	1,054	4.84	1.45	5	−0.44	−0.2
Past behavior						
beh1. How often do use one or more of Twitter's options to increase user privacy? Item range from 1 (*never*) to 7 (*always*).	1,058	3.33	1.66	3	0.25	−0.65

Note. *N* = valid responses; *M* = mean value; *SD* = standard deviation; Me = median; Sk = skewness; Kur = kurtosis.

approximation [RMSEA] and the comparative fit index [CFI]), and (3) information-theoretic fit measures, the Akaike information criterion (AIC) and the consistent AIC (CAIC) that take into account sample size and the number of free parameters (West et al., 2012, p. 223). For indicating the quality of the model fit, the following cutoff criteria (using maximum likelihood [ML] estimation) were applied. Values smaller than .08 for the SRMR, smaller than .06 for RMSEA,

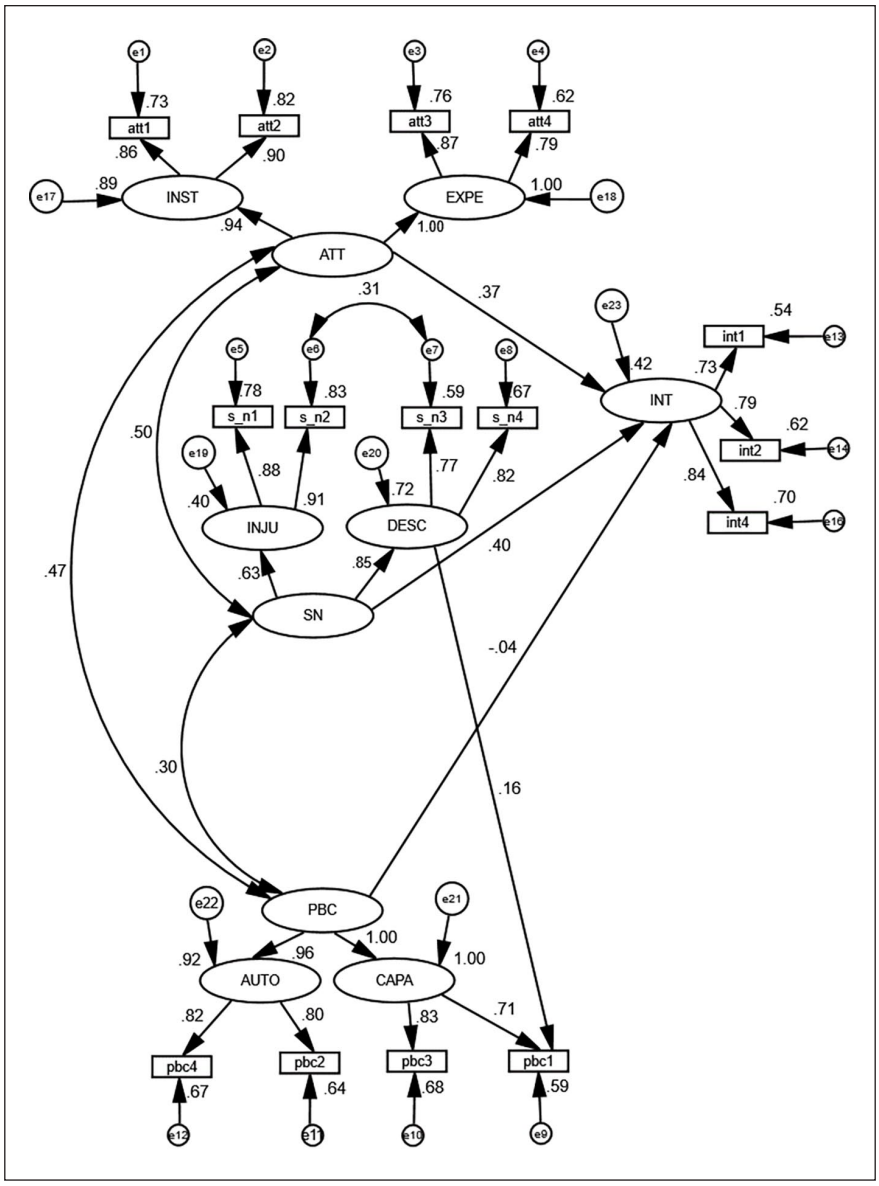

Figure 2. TPB structural equation model explaining intention to use online privacy settings (standardized coefficients).
Note. ATT = attitude; AUTO = autonomy; CAPA = capacity; DESC = descriptive; EXPE = experiential; INJU = injunctive; INST = instrumental; INT = intention; PBC = perceived behavioral control; SN = subjective norm.

and greater than .95 for CFI (Hu & Bentler, 1999) were considered indicative of an acceptable fit. Finally, the models with the smallest AIC and CAIC were selected.

Results

Measurement Model

All the factor loadings were higher than 0.45 (Brown, 2015), and the fit indices suggested an acceptable fit for the measurement model, with an SRMR value of 0.039, an RMSEA value of .0047, and a CFI value of .980. Unstandardized and standardized loadings of the measurement model are displayed in Appendices C and D.

Structural Equation Model

Privacy intention model. Results for the structural model in which attitude, subjective norm, and PBC as direct predictors of intention are presented in Figure 2 (standardized regression coefficients) assuming that PBC has no direct effect. The structural model had a good fit to the data (SRMR = 0.057; CFI = 0.963; RMSEA = 0.059). Consistent with our first two hypotheses, attitude and subjective norm displayed significant associations ($p < .05$) with intention, exerting similar effects (.37 and .40, respectively) and explaining 42% of the variance in intentions, whereas PBC had no significant direct effect on intention.

Table 2. Unstandardized and Standardized Estimated Coefficients for MGSEM of PBC Moderating Effect on the Effect of Attitude and Subjective Norm on Intention

	Moderating variable			
	PBC			
	Low PBC		High PBC	
	Unstandardized	Standardized	Unstandardized	Standardized
Attitude → Intention	.363	.443	.363	.301
Subjective norm → Intention	.201	.248	.449	.431

Note. PBC = perceived behavioral control.

Privacy Intention Model With PBC as a Moderator

We constrained factor loadings to be equal across the two groups (Steenkamp & Baumgartner, 1998), and additionally, we constrained the associations between the factors to be the same across the groups. The fit of the model assuming equal regression coefficients of attitudes and norms on the intention for high and low PBC groups became significantly worse ($p = .002$) compared with the model allowing different coefficients for attitudes and norms. We had to release the equality constraint on the effect of subjective norms on intention. This model had the best fit. Consistent with our fourth hypothesis, Table 2 shows a stronger effect of subjective norm on intention in the high PBC group in comparison to the low PBC group, but contrary to Hypothesis 3, the attitude–intention relation was not affected by the level of PBC. The model with PBC as a moderating variable in the low PBC group accounted for 34.8% of the variance in intentions, while in the high PBC group, it contributed 39% of the explained variance of intention.

Mediated Effects of Past Behavior

Tests of the extent to which the relation between past behavior and intention was mediated by attitude, subjective norm, and PBC provided support for partial mediation. Beyond its positive effects on attitude, subjective norm, and PBC, past behavior also had a significant and positive direct effect on intention. Based on the partial mediation model, the direct effect (standardized regression coefficient) of past behavior on intention was .251, the indirect effect was .230, and the total effect was .481 (see Table 2). In the partially mediated model, the regression coefficient of past behavior on attitude was .31, on subjective norm it was .43, and on PBC, it was .11. Finally, the effect of attitude on intention was .33, and the effect of subjective norm on intention was .31. However, the effect of PBC on intention was .03 (see Table 3).

Table 3. Determinants of Intention.

	Standardized regression coefficient
Past behavior → Intention (direct)	.251
Past behavior → Intention (indirect)	.230
Past behavior → Attitude	.310
Past behavior → Subjective norm	.430
Past behavior → PBC	.110
Attitude → Intention	.330
Subjective norm → Intention	.310
PBC → Intention	.030

Note. PBC = perceived behavioral control.

Past Behavior as a Moderator

Next, we performed an MGSEM analysis to examine possible moderating effects of past behavior. We found that the effects of all three predictors, attitude, subjective norm, and PBC, significantly differed in the high and the low past behavior groups. The results presented in Table 4 show that the effect of subjective norm was much stronger in the low- than the high-frequency group. By way of contrast, the effects of PBC and attitude were *weaker* in this group, that is, perceived control and attitudes were more important in determining intention to perform safe internet behavior when respondents had more rather than less past experience with safety behavior.

Summary and Conclusions

Social networking sites have become a predominant means of communication across the globe. Activities on these sites

Table 4. Unstandardized and Standardized Estimated Coefficients for MGSEM of Past Behavior Moderating Effect on the Effect of Attitude, Perceived Norm, and PBC on Intention.

	Moderating variable			
	Past behavior			
	Low frequency		High frequency	
	Unstandardized	Standardized	Unstandardized	Standardized
Attitude → Intention	.33	302	.407	.375
Subjective norm → Intention	.520	438	.273	.230
PBC → Intention	-.138	-146	.199	.176

Note. PBC = perceived behavioral control.

generate massive amounts of personal information and raise concerns about its potential abuse. Indeed, the exponential increase in the amount of personal information collected by the platforms from their users, combined with the development of powerful technologies to analyze users' information, preferences, and behavior, raises serious concerns about users' vulnerability to abuse of their disclosed data. To reduce this risk, the promotion of behaviors designed to prevent malicious exploitation of confidential data is one of the most important challenges in the information age. In this study, we tried to contribute to research that aims to assess determinants of safe internet behavior. We drew on the theory of planned behavior to predict and explain intentions to adopt privacy behaviors on social networking sites. In an online survey of Twitter users in Germany, we assessed instrumental and experiential attitudes toward adopting privacy measures, injunctive and descriptive subjective norms, as well as capacity and autonomy aspects of PBC. Consistent with the theory, (1) attitudes and subjective norms regarding safe privacy behaviors were direct predictors of intentions to perform such behaviors and (2) PBC had a moderating effect, such that subjective norms were a better predictor of intentions for participants who were high as opposed to low in perceived control. Thus, the results of the present study provide strong support for a reasoned action approach to online privacy behavior.

We also explored how past behavior contributed to the explanation of intentions to perform safe internet behavior. We found that the importance of subjective norm increased for participants with relatively little past experience, whereas for participants with relatively more past experience in safe internet behavior, attitude and PBC took on added importance. These findings can be explained as follows. Past performance of the behavior provides Twitter users with information about the behavior's consequences, the basis for their attitudes, and about the ease or difficulty of performing privacy behavior, the basis for their PBC. With extensive past experience they have a well-established, stable attitudes and firm perceptions of control, and stable dispositions predict intentions and behavior better than less stable dispositions (Doll & Ajzen, 1992). On the other hand, when past experience with the behavior is low, attitude and PBC are less stable, and Twitter users are apt to rely on subjective norms, that is, on what others do or think one should do.

The results of our study compare favorably with findings from past research that tried to predict online privacy intention and behavior, summarized in a recent and comprehensive meta-analysis (Baruh et al., 2017). In this meta-analysis, privacy concerns explained only about 10% of the variance in intentions. By way of comparison, our TPB model accounted for 47% of the variance. Specifically, we found that people are likely to form an intention to protect their internet privacy when they view this as being in their own best interest and when they believe that they have the support of significant others. PBC seems to play a secondary role, strengthening the effect of subjective norms—but not of attitudes—on intentions. Clearly, for a better understanding of intentions to adopt internet privacy measures, we must go beyond privacy concerns to focus more broadly on attitudes toward adopting privacy measures (which may reflect privacy concerns among other considerations), subjective norms, as well as PBC.

Our findings also have important implications for interventions designed to encourage the adoption of internet privacy measures. Such interventions must be designed to strengthen attitudes toward protecting one's online privacy, to increase perceived social pressure to do so, and to provide the requisite knowledge. This requires identification of the beliefs that social networking users hold regarding the likely consequences and experiences associated with the adoption of privacy measures, beliefs that provide the basis for their attitudes; identification of significant others whose opinions and behaviors exert social pressure to adopt privacy measures; and identification of the factors that facilitate or impede their adoption. Thus, for example, it may be found that favorable attitudes toward adopting online privacy

measures could be reinforced by emphasizing that such measures can fend off identity theft, prevent disclosure of intimate information to strangers, and results in a more satisfying networking experience; subjective norms in support of adopting online privacy measures could perhaps be strengthened by pointing to normative expectations of peers, family members, and experts as well as the online privacy behavior of these social referents; and information about available privacy protection measures and how to use them could be provided to increase PBC.

Limitations

The present study is not without its limitations. First and foremost is the question of our findings' generalizability beyond the intentions of Twitter users in Germany. The adoption of privacy measures is an important issue not only on Twitter but also on other social networking sites and in relation to such internet activities as information search, online shopping, and banking. It is conceivable that the levels and relative importance of attitudes, subjective norm, PBC, and past behavior differ across these various platforms. Similar concerns apply to the research population. Our data were collected in Germany, but results may well differ from one country to another. Future studies could address these issues by applying the theory of planned behavior to the prediction of intentions to adopt privacy behaviors on social networking platforms other than Twitter, on additional kinds of internet sites, and in other cultural contexts.

Another potential limitation of the present study is its focus on behavioral intentions. Like much research on internet privacy behavior, we examined the determinants of intentions to adopt privacy-shielding measures without a follow-up assessment of actual privacy behavior. The extent to which intentions and perceived control are predictive of y behavior should be examined in future research that goes beyond intentions to include a measure of actual privacy behavior.

Acknowledgements

The authors would like to thank Lisa Trierweiler for the English proof of the manuscript. We thank Julia Petersen for checking the final version.

Declaration of Conflicting Interests

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

Funding

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

ORCID iD

Peter Schmidt https://orcid.org/0000-0001-6954-8590

References

Aïmeur, E., & Sahnoune, Z. (2020). Privacy, trust, and manipulation in online relationships. *Journal of Technology in Human Services*, *38*(2), 159–183. https://doi.org/10.1080/15228835.2019.1610140

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In J. Kuhl & J. Beckmann (Eds.), *SSSP Springer series in social psychology: Action control* (pp. 11–39). Springer. https://doi.org/10.1007/978-3-642-69746-3_2

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

Ajzen, I. (2012). The theory of planned behavior. In P. A. M. Van Lange, A. W. Kruglanski, & E. T. Higgins (Eds.), *Handbook of theories of social psychology* (Vol. 1, pp. 438–459). SAGE. https://doi.org/10.4135/9781446249215.n22

Ajzen, I., & Schmidt, P. (2020). Changing behavior using the theory of planned behavior. In M. S. Hagger, L. D. Cameron, K. Hamilton, N. Hankonen, & T. Lintunen (Eds.), *The handbook of behavior change* (pp. 17–31). Cambridge University Press.

Albarracin, D., Fishbein, M., Goldestein, de Muchinik, E. G. (1997). Seeking social support in old age as reasoned action: Structural and volitional determinants in a middle-aged sample of Argentinean women. *Journal of Applied Social Psychology*, *27*(6), 463–476. https://doi.org/10.1111/j.1559-1816.1997.tb00642.x

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

Arbuckle, J. L. (2017). *IBM SPSS Amos 25 user's guide*. Amos Development Corporation.

Armitage, C. J., & Conner, M. (1999). Distinguishing perceptions of control from self-efficacy: Predicting consumption of a low-fat diet using the theory of planned behavior. *Journal of Applied Social Psychology*, *29*(1), 72–90. https://doi.org/10.1111/j.1559-1816.1999.tb01375.x

Bandura, A. (1997). *Self-efficacy: The exercise of control*. W. H. Freeman/Times Books/Henry Holt.

Barth, S., & de Jong, M. D. (2017). The privacy paradox–Investigating discrepancies between expressed privacy concerns and actual online behavior–A systematic literature review. *Telematics and Informatics*, *34*(7), 1038–1058. https://doi.org/10.1016/j.tele.2017.04.013

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication*, *67*(1), 26–53. https://doi.org/10.1111/jcom.12276

Boerman, S., Kruikemeier, S., & Borgesius, F. J. (2018). Exploring motivations for online privacy protection behavior: Insights from panel data. *Communication Research*, *48*(7), 1–25. https://doi.org/10.1177/0093650218800915

Bosnjak, M., Ajzen, I., & Schmidt, P. (2020). The theory of planned behavior: Selected recent advances and applications. *Europe's Journal of Psychology*, *16*(3), 352–356. https://doi.org/10.5964/ejop.v16i3.3107

Brown, T. A. (2015). *Confirmatory factor analysis for applied research*. The Guilford Press.

Buechi, M., Festic, N., Just, N., & Latzer, M. (2021). Digital inequalities in online privacy protection: Effects of age, education and gender. In E. Hargittai (Ed.), *Handbook of digital inequality* (pp. 296–310). Edward Elgar Publishing.

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

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. https://doi.org/10.1111/hcre.12053

Curran, P. J., West, S. G., & Finch, J. F. (1996). The robustness of test statistics to nonnormality and specification error in confirmatory factor analysis. *Psychological Methods*, *1*(1), 16–29. https://doi.org/10.1037/1082-989X.1.1.16

Desimpelaere, L., Hudders, L., & Van de Sompel, D. (2020). Knowledge as a strategy for privacy protection: How a privacy literacy training affects children's online disclosure behavior. *Computers in Human Behavior*, *110*, Article 106382. https://doi.org/10.1016/j.chb.2020.106382

Dienlin, T., & Metzger, M. J. (2016). An extended privacy calculus model for SNSs: Analyzing self-disclosure and self-withdrawal in a representative US sample. *Journal of Computer-Mediated Communication*, *21*(5), 368–383. https://doi.org/10.1111/jcc4.12163

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. https://doi.org/10.1002/ejsp.2049

Doll, J., & Ajzen, I. (1992). Accessibility and stability of predictors in the theory of planned behavior. *Journal of Personality and Social Psychology*, *63*, 754–765. https://doi.org/10.1037/0022-3514.63.5.754

Epstein, D., & Quinn, K. (2020). Markers of online privacy marginalization: Empirical examination of socioeconomic disparities in social media privacy attitudes, literacy, and behavior. *Social Media + Society*, *6*(2), 1–13. https://doi.org/10.1177/2056305120916853

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

French, M., & Bazarova, N. N. (2017). Is anybody out there? Understanding masspersonal communication through expectations for response across social media platforms. *Journal of Computer-Mediated Communication*, *22*(6), 303–319. https://doi.org/10.1111/jcc4.12197

Gordoni, G., & Schmidt, P. (2010). The decision to participate in social surveys: The case of the Arab minority in Israel—An application of the theory of reasoned action. *International Journal of Public Opinion Research*, *22*(3), 364–391. https://doi.org/10.1093/ijpor/edq022

Hagger, M. S., & Chatzisarantis, N. L. (2005). First- and higher-order models of attitudes, normative influence, and perceived behavioural control in the theory of planned behaviour. *British Journal of Social Psychology*, *44*(4), 513–535. https://doi.org/10.1348/014466604X16219

Hagger, M. S., Chatzisarantis, N. L., & Biddle, S. (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*, *24*(1), 3–32. https://doi.org/10.1123/jsep.24.1.3

Hsu, C. L., & Lin, J. C. C. (2008). Acceptance of blog usage: The roles of technology acceptance, social influence and knowledge sharing motivation. *Information & Management*, *45*(1), 65–74. https://doi.org/10.1016/j.im.2007.11.001

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. https://doi.org/10.1080/10705519909540118

Hukkelberg, S. S., Hagtvet, K. A., & Kovac, V. B. (2014). Latent interaction effects in the theory of planned behaviour applied to quitting smoking. *British Journal of Health Psychology*, *19*(1), 83–100. https://doi.org/10.1111/bjhp.12034

Humphreys, L., Gill, P., & Krishnamurthy, B. (2014). Twitter: A content analysis of personal information. *Information, Communication & Society*, *17*(7), 843–857. https://doi.org/10.1080/1369118X.2013.848917

Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal*, *25*(6), 607–635. https://doi.org/10.1111/isj.12062

Kline, R. B. (2015). *Principles and practice of structural equation modeling* (4th ed.). The Guilford Press.

La Barbera, F., & Ajzen, I. (2020). Control interactions in the theory of planned behavior: Rethinking the role of subjective norm. *Europe's Journal of Psychology*, *16*(3), 401–417. https://doi.org/10.5964/ejop.v16i3.2056

Liang, H., Shen, F., & Fu, K. W. (2017). Privacy protection and self-disclosure across societies: A study of global Twitter users. *New Media & Society*, *19*(9), 1476–1497. https://doi.org/10.1177/1461444816642210

Liang, H., Wu, D., Liu, S., Dai, H., & Liu, H. (2016). Providing privacy protection and personalization awareness for android devices. *International Journal of Distributed Sensor Networks*. Advance online publication. https://doi.org/10.1177/155014774645256

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. https://doi.org/10.1177/1461444810365313

Masur, P. K., & Scharkow, M. (2016). Disclosure management on social network sites: Individual privacy perceptions and user-directed privacy strategies. *Social Media + Society*, *2*(1), 1–3. https://doi.org/10.1177/2056305116634368

Matzner, T., Masur, P. K., Ochs, C., & von Pape, T. (2016). Do-it-yourself data protection—Empowerment or burden? In S. Gutwirth, R. Leenes, & P. De Hert (Eds.), *Law, governance and technology series: Data protection on the move* (Vol. 24, pp. 277–305). Springer.

McDermott, F. D., Heeney, A., Kelly, M. E., Steele, R. J., Carlson, G. L., & Winter, D. C. (2015). Systematic review of preoperative, intraoperative and postoperative risk factors for colorectal anastomotic leaks. *British Journal of Surgery*, *102*(5), 462–479. https://doi.org/10.1002/bjs.9697

Nardis, Y., & Panek, E. (2019). Explaining privacy control on Instagram and Twitter: The roles of narcissism and self-esteem. *Communication Research Reports*, *36*(1), 24–34. https://doi.org/10.1080/08824096.2018.1555522

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, *79*(1), 119–157.

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

Nissenbaum, H. (2015). Respecting context to protect privacy: Why meaning matters. *Science and Engineering Ethics*, *24*(3), 831–852. https://doi.org/10.1007/s11948-015-9674-9

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus

behaviors. *Journal of Consumer Affairs*, *41*(1), 100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

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

Phua, J., Jin, S. V., & Kim, J. J. (2017). Uses and gratifications of social networking sites for bridging and bonding social capital: A comparison of Facebook, Twitter, Instagram, and Snapchat. *Computers in Human Behavior*, *72*, 115–122. https://doi.org/10.1016/j.chb.2017.02.041

Rains, S. A., & Brunner, S. R. (2015). What can we learn about social network sites by studying Facebook? A call and recommendations for research on social network sites. *New Media & Society*, *17*(1), 114–131. https://doi.org/10.1177/1461444814546481

Riebl, S. K., Estabrooks, P. A., Dunsmore, J. C., Savla, J., Frisard, M. I., Dietrich, A., Peng, Y., Zhang, X., & Davy, B. M. (2015). A systematic literature review and meta-analysis: The theory of planned behavior's application to understand and predict nutrition-related behaviors in youth. *Eating Behaviors*, *18*, 160–178. https://doi.org/10.1016/j.eatbeh.2015.05.016

Rigdon, E. E., Schumacker, R. E., & Wothke, W. (1998). A comparative review of interaction and nonlinear modeling: Interaction and nonlinear effects in structural equation modeling. In R. E. Schumacker & G. A. Marcoulides (Eds.), *Interaction and nonlinear effects in structural equation modeling* (pp. 1–16). Lawrence Erlbaum.

Schafer, J. L., & Graham, J. W. (2002). Missing data: Our view of the state of the art. *Psychological Methods*, *7*(2), 147–177. https://doi.org/10.1037/1082-989X.7.2.147

Sheeran, P., & Taylor, S. (1999). Predicting intentions to use condoms: A meta-analysis and comparison of the theories of reasoned action and planned behavior. *Journal of Applied Social Psychology*, *29*(8), 1624–1675. https://doi.org/10.1111/j.1559-1816.1999.tb02045.x

Sindermann, C., Schmitt, H. S., Kargl, F., Herbert, C., & Montag, C. (2021). Online privacy literacy and online privacy behavior—The role of crystallized intelligence and personality. *International Journal of Human-computer Interaction*, *37*(15), 1455–1466. https://doi.org/10.1080/10447318.2021.1894799

Soffer, O., & Gordoni, G. (2018). To post or not to post? Anonymous user comments in the Israeli journalistic sphere. *Journalism Studies*, *19*(10), 1390–1408. https://doi.org/10.1080/1461670X.2017.1279027

Steenkamp, J.-B. E. M., & Baumgartner, H. (1998). Assessing measurement invariance in cross-national consumer research. *Journal of Consumer Research*, *25*(1), 78–90. https://doi.org/10.1086/209528

Steinmetz, H., Knappstein, M., Ajzen, I., Schmidt, P., & Kabst, R. (2016). How effective are behavior change interventions based on the theory of planned behavior? A three-level meta-analysis. *Zeitschrift für Psychologie*, *224*(3), 216–233. https://doi.org/10.1027/2151-2604/a000255

Stoycheff, E., Liu, J., Wibowo, K. A., & Nanni, D. P. (2017). What have we learned about social media by studying Facebook? A decade in review. *New Media & Society*, *19*(6), 968–980. https://doi.org/10.1177/1461444817695745

Twitter Safety and Security Information. (2020). *About public and protected tweets*. https://help.twitter.com/en/safety-and-security/public-and-protected-tweets

Walrave, M., Vanwesenbeeck, I., & Heirman, W. (2012). Connecting and protecting? Comparing predictors of self-disclosure and privacy settings use between adolescents and adults. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *6*(1), Article 3. https://doi.org/10.5817/CP2012-1-3

West, S. G., Taylor, A. B., & Wu, W. (2012). Model fit and model selection in structural equation modeling. In R. H. Hoyle (Ed.), *Handbook of structural equation modeling* (pp. 209–231). The Guilford Press.

Winkelnkemper, P., Ajzen, I., & Schmidt, P. (2019). *The theory of planned behavior: A meta-analysis and structural equation modeling* University of Giessen [Unpublished manuscript].

Wu, P. F. (2019). The privacy paradox in the context of online social networking: A self-identity perspective. *Journal of the Association for Information Science and Technology*, *70*(3), 207–217. https://doi.org/10.1002/asi.24113

Wu, P. F., Vitak, J., & Zimmer, M. T. (2020). A contextual approach to information privacy research. *Journal of the Association for Information Science and Technology*, *71*(4), 485–490. https://doi.org/10.1002/asi.24232

Young, A., & Quan-Haase, A. (2013). Privacy protection strategies on Facebook. *Information, Communication & Society*, *16*, 479–500.

Yzer, M., & Van Den Putte, B. (2014). Control perceptions moderate attitudinal and normative effects on intention to quit smoking. *Psychology of Addictive Behaviors*, *28*(4), 1153–1161. https://doi.org/10.1037/a0037924

Zhong, B., Hardin, M., & Sun, T. (2011). Less effortful thinking leads to more social networking? The associations between the use of social network sites and personality traits. *Computers in Human Behavior*, *27*(3), 1265–1271. https://doi.org/10.1016/j.chb.2011.01.008

Author Biographies

Peter Schmidt (University of Mannheim) is a sociologist and social researcher and Professor emeritus for empirical research and methodology at the Faculty for Cultural and Social Sciences and Member at the Centre for International Development and Environment (ZEU) at the University of Giessen as well as Research Fellow and P.I. at the Department of Psychosomatics at the University of Mainz. His research interests include theory of planned behavior, values, and structural equation modeling.

Galit Gordoni (PhD, University of Haifa) is a sociologist and survey methodologist. She was a visiting scholar at the Open Media and Information Lab (OMILab) at the Open University of Israel. Her research focuses on psychological and sociological antecedents of human behavior and interpersonal communication.

Icek Ajzen (PhD/MA, University of Illinois) is a professor emeritus at the University of Massachusetts Amherst (USA). He is the author of the theory of planned behavior and his research interests include use of the theory to predict and explain behavior in various domains and as a framework for designing behavior change interventions.

Christoph Beuthner (MA, TU Dresden) is a doctoral researcher at GESIS—Leibniz Institute for the Social Sciences. His research interests include machine and deep learning.

Eldad Davidov (Dr/MA, University of Giessen and University of Tel Aviv) is a professor at the University of Cologne and at the University of Zurich and co-director of the University of Zurich Research Priority Program "Social Networks." His research interests include use of structural equation modeling to measure, explain, and compare values and attitudes in different social groups.

Henning Silber (PhD, University of Göttingen) is senior researcher at GESIS—Leibniz Institute for the Social Sciences. His research interests include survey methodology, political sociology, and the experimental social sciences.

Holger Steinmetz (University of Giessen) is senior researcher at the Chair of Management at Trier University. He was Chair of the department for big data in psychology for 3 years at the Leibniz Institute for Psychology. His research interests are on causal inference and structural equation modeling topics on the interface between psychology, management, and entrepreneurship. One example is his research on the motivation to start a business.

Bernd Weiß (University of Cologne) is head of the GESIS Panel, a probabilistic mixed-mode panel, and deputy head of the Department of Survey Design and Methodology at GESIS—Leibniz Institute for the Social Sciences. His research interests range from survey methodology, research synthesis, and open science to family sociology and juvenile delinquency.

Appendix A. Percentage Frequency Distribution of TPB Items.

Items	1	2	3	4	5	6	7
Attitude							
For me, to use one or more of Twitter's options to increase user privacy is. . .	Extremely negative						Extremely positive
att1. bad-good	1.2	1.7	5	30.5	28.5	22.3	10.8
att2. useless-useful	.8	1.2	5	25.1	28	26.2	13.7
att3. unpleasant-pleasant	.4	1.3	3.4	30.8	27.5	24.4	12.2
att4. uninteresting-interesting	1.2	1.4	4.5	32	25.4	22	13.5
Subjective norm							
s_n1. I believe that most people who are important to me think that I should make more use of the privacy options of Twitter.	Completely false 10.9	12.2	17.9	28.1	16.3	9.7	Completely true 5
s_n2. Most people whose opinion I value would approve of my use of one or more of Twitter's options to increase my privacy.	Extremely unlikely 10.3	12.6	15.9	27.3	19.5	10.8	Extremely likely 3.6
s_n3. Most people I respect and admire use one or more of the options, on Twitter, to improve their privacy.	Extremely unlikely 5	7.1	12.2	31.5	23.3	14.9	Extremely likely 6
s_n4. In Twitter, most people who are similar to me use one or more of the options to improve their privacy.	Extremely disagree 4	5.2	11.1	32.8	24.8	15.3	Extremely agree 6.8
Perceived behavioral control	Extremely disagree						Extremely agree
pbc1. I am confident that I am able to use one or more of the options in Twitter to secure my privacy.	1.8	2	4.9	18.8	25.2	27.7	19.7
pbc2. To use one or more of Twitter's options to increase my privacy is up to me.	1.2	1.8	3.9	19.1	21.6	24	28.4
pbc3. If I wanted to, I could easily use one or more of the options in Twitter to protect my privacy.	1	1.7	4	19.3	22.3	27.1	24.5
pbc4. To use one or more of Twitter's options to increase my privacy is under my control.	1.1	1.9	5.4	20.8	24.1	24.6	22
Intention							
int1. I intend to use one or more of Twitter's options to increase user privacy.	Definitely do not intend to 3.1	6.3	10.9	29.5	19	19.2	Definitely intend to 11.9
int2. I will use one or more of Twitter's options to increase user privacy.	Extremely unlikely 2.9	5.1	8.4	25.3	24.8	22.8	Extremely likely 10.7
int3. I am ready to use one or more of Twitter's options to increase user privacy	Extremely false 1.3	1.6	4.9	23.5	30.4	23.8	Extremely true 14.4
int4. I plan to use one or more of Twitter's options to increase user privacy.	Extremely disagree 2.4	4	9.7	24.3	23.7	22.9	Extremely agree 13.1
Past behavior	Never						Always
beh1. How often do use one or more of Twitter's options to increase user privacy?	18.9	14.9	17.6	25.8	13.3	4.9	4.5

Appendix B. Correlation Matrix for the 16 TPB Items and Past Behavior.

	int1	int2	int3	int4	pbc1	pbc2	pbc3	pbc4	s_n1	s_n2	s_n3	s_n4	att1	att2	att3	att4	beh1
int1	1																
int2	.52	1															
int3	.57	.68	1														
int4	.61	.68	.74	1													
pbc1	.26	.21	.31	.23	1												
pbc2	.15	.17	.27	.15	.53	1											
pbc3	.19	.18	.32	.17	.58	.67	1										
pbc4	.08	.13	.23	.13	.50	.67	.71	1									
sn1	.13	.13	.13	.25	.05 (ns)	.03 (ns)	.02 (ns)	.03 (ns)	1								
sn2	.12	.13	.14	.23	.08	.05 (ns)	.02 (ns)	.04 (ns)	.79	1							
sn3	.25	.27	.29	.33	.30	.21	.18	.20	.37	.46	1						
sn4	.34	.36	.42	.42	.39	.25	.25	.19	.34	.37	.64	1					
att1	.27	.32	.37	.33	.40	.34	.33	.32	.07	.13	.26	.31	1				
att2	.33	.38	.44	.39	.41	.36	.36	.34	.13	.17	.29	.36	.77	1			
att3	.34	.37	.42	.40	.40	.31	.28	.29	.15	.16	.27	.36	.71	.76	1		
att4	.35	.39	.42	.42	.31	.25	.22	.21	.19	.19	.25	.36	.59	.67	.68	1	
beh1	.36	.37	.34	.41	.20	.05(ns)	.09	.06	.17	.14	.30	.34	.24	.26	.25	.27	1

Note. Due to pairwise deletion, sample sizes varied between 1,046 and 1,057. ns = nonsignificant ($p > .05$).

Appendix C. CFA Results: Standardized Factor Loadings in the TPB Model (3 Second-Order Factors and 7 First-Order Factors).

Items	Standardized factor loadings
Instrumental attitude	
att1	.84
att2	.92
Experiential attitude	
att3	.88
att4	.77
Injunctive norm	
s_n1	.85
s_n2	.92
Descriptive norm	
s_n3	.74
s_n4	.88
pbc1	.26
PBC capacity	
pbc1	.59
pbc3	.88
PBC autonomy	
pbc2	.80
pbc4	.83
Intention	
int1	.69
int2	.77
int4	.88

Note. The item pbc1 ("I am confident that I am able to use one or more of the options in Twitter to secure my privacy") has a cross-loading on the descriptive norm factor (.26). PBC = perceived behavioral control.

Appendix D. CFA Results: Standardized Factor Loadings of First-Order Factors on Second-Order Factors in the TPB Model.

Second-order factors	First-order factors	Factor loadings	Factor correlations
Attitude			
	Instrumental	.96	
	Experiential	.98	
Subjective norm			
	Injunctive	.48	
	Descriptive	1	
PBC			
	Capacity	.97	
	Autonomy	.99	
Attitude—perceived norm			.44
Attitude—PBC			.46
Attitude—intention			.54
Subjective norm—PBC			.30
Subjective norm—intention			.50
PBC—intention			.23

Note. The item pbc1 ("I am confident that I am able to use one or more of the options in Twitter to secure my privacy") has a cross-loading on the descriptive norm factor (.26).

Appendix E

Questionnaire

TPB Model (PGID 6310361)

Options Social Network Twitter (PGID 6335641). The following questions relate to privacy in Twitter. Each network has certain default settings that should ensure privacy. There are also additional settings that you can enable or disable. Some users make use of changing these basic settings, while others leave the basic settings unchanged. Thinking about Twitter, which of the following privacy settings does this network provide? (q_11449177—Typ 311)

Variable name	External variable name	Int	
v_76	tpopsich		The option to limit the visibility of updates or content to a selected, specific group (e.g., friends)
		1	The setting is available in Twitter
		2	The setting does not exist in Twitter
v_77	tpopmark		The option to remove tags (e.g., your own name) from postings or photos
		1	The setting is available in Twitter
		2	The setting does not exist in Twitter
v_78	tpopgefu		The possibility to set that the own profile cannot be found by others
		1	The setting is available in Twitter
		2	The setting does not exist in Twitter
v_79	tpoperei		The possibility of limiting the accessibility of one's profile to certain people
		1	The setting is available in Twitter
		2	The setting does not exist in Twitter
v_80	tpopinha		The ability to restrict access to your own content to specific people
		1	The setting is available in Twitter
		2	The setting does not exist in Twitter
v_81	tpopkont		The ability to prevent certain people from contacting you (i.e., "block")
		1	The setting is available in Twitter
		2	The setting does not exist in Twitter
v_82	tpopstan		The option to restrict or prevent the forwarding of information about your location
		1	The setting is available in Twitter
		2	The setting does not exist in Twitter
v_83	tpoploes		The ability to delete personal data such as posts, photos, and correspondence with specific individuals
		1	The setting is available in Twitter
		2	The setting does not exist in Twitter

Privacy Behavior (PGID 6335781). Related to Twitter, how often do you use one or more of the privacy options Twitter offers? (q_11449322—Typ 111)

Variable name	External variable name	Int	
v_84	tpve		
		1	Never
		2	Very rarely
		3	Rarely
		4	Neither often nor rarely
		5	Quite often
		6	Very often
		7	Always

Privacy 1 (PGID 6353962). Please select the answer that best describes your opinion of the following statements. All statements refer to Twitter. Using Twitter's privacy options to protect my privacy, I find. . . (q_11465820—Typ 111)

Variable name	External variable name	Int	
v_153	tpprschl		
		1	Very bad
		2	Quite bad
		3	Rather bad
		4	Neither good nor bad
		5	Rather good
		6	Quite good
		7	Very good

Privacy 2 (PGID 6353963). Please select the answer that best describes your opinion of the following statements. All statements refer to Twitter. Using Twitter's privacy options to protect my privacy, I find. . . (q_11465821—Typ 111)

Variable name	External variable name	Int	
v_154	tpprnutz		
		1	Very useless
		2	Quite useless
		3	Rather useless
		4	Neither useless nor useful
		5	Rather useful
		6	Quite useful
		7	Very useful

Privacy 3 (PGID 6360230). Please select the answer that best describes your opinion of the following statements. All statements refer to Twitter. Using Twitter's privacy options to protect my privacy, I find. . . (q_11488224—Typ 111)

Variable name	External variable name	Int	
v_387	tpprange		
		1	Very unpleasant
		2	Quite unpleasant
		3	Rather unpleasant
		4	Neither unpleasant nor pleasant
		5	Rather pleasant
		6	Quite pleasant
		7	Very pleasant

Privacy 4 (PGID 6360231). Please select the answer that best describes your opinion of the following statements. All statements refer to Twitter. Using Twitter's privacy options to protect my privacy, I find. . . (q_11488226—Typ 111)

Variable name	External variable name	Int	
v_388	tpprunin		
		1	Very uninteresting
		2	Quite uninteresting
		3	Rather uninteresting
		4	Neither uninteresting nor interesting
		5	Rather interesting
		6	Quite interesting
		7	Very interesting

Subjective Norm 1 (PGID 6335838). Please choose the answer that best describes your opinion of the following statements. All statements refer to Twitter. I believe that most people I care about think I should make more use of Twitter's rivacy options. (q_11449447—Typ 111)

Variable name	External variable name	Int	
v_89	tpsnnut1		
		1	Does not apply at all
		2	Does not apply
		3	Rather does not apply
		4	Partly applies partly not
		5	Rather applies
		6	Applies
		7	Completely applies

Subjective Norm 2 (PGID 6335868). Please choose the answer that best describes your opinion of the following statements. All statements refer to Twitter. I believe that most people I care about think I should make more use of Twitter's privacy options. (q_11449509—Typ 111)

Variable name	External variable name	Int	
v_90	tpsnnut2		
		1	Very unlikely
		2	Quite unlikely
		3	Rather unlikely
		4	Neither likely nor unlikely
		5	Rather likely
		6	Quite likely
		7	Very likely

Subjective Norm 3 (PGID 6336583). Please choose the answer that best describes your opinion of the following statements. All statements refer to Twitter. Most people close to me use one or more of the options on Twitter to better secure their privacy. (q_11450433—Typ 111)

Variable name	External variable name	Int	
v_91	tpsnand1		
		1	Very unlikely
		2	Quite unlikely
		3	Rather unlikely
		4	Neither likely nor unlikely
		5	Rather likely
		6	Quite likely
		7	Very likely

Subjective Norm 4 (PGID 6336595). Please choose the answer that best describes your opinion of the following statements. All statements refer to Twitter. Most people similar to me use one or more of the options in Twitter to protect their privacy. (q_11450450—Typ 111)

Variable name	External variable name	Int	
v_89	tpsnnut1		
		1	Does not apply at all
		2	Does not apply
		3	Rather does not apply
		4	Partly applies partly not
		5	Rather applies
		6	Applies
		7	Completely applies

Behavioral Control 1 (PGID 6353932). I am confident that I am able to use one or more of Twitter's options to protect my privacy. (q_11478603—Typ 111)

Variable name	External variable name	Int	
v_361	tpvkzuve		
		1	Does not apply at all
		2	Does not apply
		3	Rather does not apply
		4	Partly applies partly not
		5	Rather applies
		6	Applies
		7	Completely applies

Behavioral Control 2 (PGID 6353933). It is solely up to me to use one or more of Twitter's options to protect my privacy. (q_11478607—Typ 111)

Variable name	External variable name	Int	
v_366	tpvkalle		
		1	Does not apply at all
		2	Does not apply
		3	Rather does not apply
		4	Partly applies partly not
		5	Rather applies
		6	Applies
		7	Completely applies

Behavioral Control 3 (PGID 6353936). If I wanted to, I could easily use one or more of Twitter's options to protect my privacy. (q_11478608—Typ 111)

Variable name	External variable name	Int	
v_367	tpvkwoel		
		1	Does not apply at all
		2	Does not apply
		3	Rather does not apply
		4	Partly applies partly not
		5	Rather applies
		6	Applies
		7	Completely applies

Behavioral Control 4 (PGID 6353935). It is completely under my control to use one or more of Twitter's options to protect my privacy. (q_11478609—Typ 111)

Variable name	External variable name	Int	
v_368	tpvkkont		
		1	Does not apply at all
		2	Does not apply
		3	Rather does not apply
		4	Partly applies partly not
		5	Rather applies
		6	Applies
		7	Completely applies

Intention 1 (PGID 6336613). Please select the answer that best describes your opinion of the following statements. All statements refer to Twitter. I intend to use one or more of Twitter's options to protect my privacy. (q_11465913—Typ 111)

Variable name	External variable name	Int	
v_174	ttpinbeab		
		1	I definitely intend to
		2	I quite intend to
		3	I rather intend to
		4	Neither
		5	I rather do not intend to
		6	I quite do not intend to
		7	I definitely do not intend to

Intention 2 (PGID 6346525). Please select the answer that best describes your opinion of the following statements. All statements refer to Twitter. I will use one or more of Twitter's options to protect my privacy. (q_11465915—Typ 111)

Variable name	External variable name	Int	
v_175	tpinwahr		
		1	Very unlikely
		2	Quite unlikely
		3	Rather unlikely
		4	Neither likely nor unlikely
		5	Rather likely
		6	Quite likely
		7	Very likely

Intention 3 (PGID 6346526). Please select the answer that best describes your opinion of the following statements. All statements refer to Twitter. I am willing to use one or more of Twitter's privacy options. (q_11465917—Typ 111)

Variable name	External variable name	Int	
v_176	tpinfals		
		1	Completely wrong
		2	Quite wrong
		3	Rather wrong
		4	Neither wrong nor right
		5	Rather right
		6	Quite right
		7	Completely right

Intention 4 (PGID 6346527). Please select the answer that best describes your opinion of the following statements. All statements refer to Twitter. I plan to use one or more of Twitter's options to protect my privacy. (q_11465920—Typ 111)

Variable name	External variable name	Int	
v_177	tpintrif		
		1	Does not apply at all
		2	Does not apply
		3	Rather does not apply
		4	Partly applies partly not
		5	Rather applies
		6	Applies
		7	Completely applies