Computers in Human Behavior 56 (2016) 147–154

Contents lists available at ScienceDirect

Computers in Human Behavior

journal homepage: www.elsevier.com/locate/comphumbeh

Full length article

Control your Facebook: An analysis of online privacy literacy

Miriam Bartsch [a, *, 1], Tobias Dienlin [b, 1]

[a] University of Hamburg, Institute of Media and Communication, Von-Melle-Park 6, 20146 Hamburg, Germany
[b] Department of Media Psychology, University of Hohenheim, Wollgrasweg 23, 70599 Stuttgart, Germany

ARTICLE INFO

Article history:
Received 9 March 2015
Received in revised form
26 October 2015
Accepted 12 November 2015
Available online 2 December 2015

Keywords:
Privacy literacy
Social network site
Facebook
Media psychology
Structural equation modeling

ABSTRACT

For an effective and responsible communication on social network sites (SNSs) users must decide between withholding and disclosing personal information. For this so-called privacy regulation, users need to have the respective skills—in other words, they need to have online privacy literacy. In this study, we discuss factors that potentially contribute to and result from online privacy literacy. In an online questionnaire with 630 Facebook users, we found that people who spend more time on Facebook and who have changed their privacy settings more frequently reported to have more online privacy literacy. People with more online privacy literacy, in turn, felt more secure on Facebook and implemented more social privacy settings. A mediation analysis showed that time spend on Facebook and experience with privacy regulation did not per se increase safety and privacy behavior directly, stressing the importance of online privacy literacy as a mediator to a safe and privacy-enhancing online behavior. We conclude that Internet experience leads to more online privacy literacy, which fosters a more cautious privacy behavior on SNSs.

1. Introduction

In offline contexts, personal privacy is important: We need it for personal autonomy, emotional release, self-evaluations, and protected communication (Westin, 1967). In order to achieve privacy offline, several privacy behaviors exist: We lock doors, lower voices, and close curtains. These behaviors are commonplace and we use them in order to protect our privacy. In online contexts, personal privacy is important also: Next to the aforementioned aspects, we nowadays also need online privacy to foster our own authenticity (Trepte & Reinecke, 2011). In order to achieve privacy online, different privacy behaviors exist: Users of social network sites (SNSs) can present only particular aspects of themselves (e.g., Kobsa, Patil, & Meyer, 2012), limit the audience via friends lists (e.g., Krämer & Haferkamp, 2011), or maintain different user profiles (e.g., Rosenbaum, Johnson, Stepman, & Nuijten, 2010). However, in online contexts we do not seem to show as many privacy behaviors as compared with offline contexts (Barnes, 2006; Eurobarometer, 2010; Taddicken, 2014). In other words, in online contexts we arguably do not really "lock our doors".

This lack of privacy behavior is relevant, given the omnipresence of SNSs in everyday life: In Germany, people spend almost 3 h a day online (Frees & Koch, 2015), and worldwide, the most popular SNS Facebook attracts more than 1.49 billion users on a monthly basis (Facebook, 2015). This is somewhat problematic, given that privacy concerns are ubiquitous either: A survey by the European Union with 27,761 participants of 27 EU States showed that 84% of European Internet users and 51% European SNS users were concerned about their privacy (Eurobarometer, 2010). In a study with 975 telephone interviews, Hoofnagle, King, Li, and Turow (2010) found that 55% of all users were more concerned about their privacy in 2009 than they were five years before. Furthermore, they asked for the reasons of their fear: 48% named a better knowledge of privacy risks, 30% argued that they would have more to lose once their privacy was violated, and 17% stated that they have had an experience that changed their mind about privacy.

Hence, the question arises: Why do people not protect their privacy online as much as offline? With this study, we want to analyze this discrepancy and suggest a first explanation for its existence. That is, people might not protect their online lives appropriately, because they lack online privacy literacy (Trepte et al., 2015). In other words, users do not show sufficient online privacy behaviors because they might not be capable of putting them into

* Corresponding author.
E-mail addresses: miriam.bartsch@studium.uni-hamburg.de (M. Bartsch), tobias.dienlin@uni-hohenheim.de (T. Dienlin).

[1] The study was conducted while Miriam Bartsch was student at the Institute for Psychology at University of Hamburg and Tobias Dienlin was research assistant at Hamburg Media School.

http://dx.doi.org/10.1016/j.chb.2015.11.022
0747-5632/

practice. To date, only few empirical studies on online privacy literacy exist and our knowledge of the basic underlying mechanisms is limited. As a result, this study aims to be innovative in terms of two aspects: It is the first study that analyzes which factors might increase online privacy literacy, and how privacy literacy might change Internet behavior and perceived online safety. As main feature, we propose a single model that includes antecedents and both behavioral and psychological outcomes of online privacy literacy.

2. Theoretical background

2.1. Definition of online privacy literacy

In what follows, we will outline our understanding of online privacy literacy. Online privacy literacy is still a comparatively new concept in online research. Regarding its theoretical definition, the following notions are relevant: Debatin (2011) stated that privacy literacy "encompasses an informed concern for […] privacy and effective strategies to protect it" (p. 51). Trepte et al. (2015) further elaborated that *"Online privacy literacy* may be defined as a combination of factual or declarative ('knowing that') and procedural ('knowing how') knowledge about online privacy. In terms of declarative knowledge, online privacy literacy refers to the users' knowledge about technical aspects of online data protection, and about laws and directives as well as institutional practices. In terms of procedural knowledge, online privacy literacy refers to the users' ability to apply strategies for individual privacy regulation and data protection" (p. 339). Regarding its empirical measurement, aspects of online privacy literacy were included in the Internet privacy concerns scale by Hong and Thong (2013). The scale includes items such as: "It is very important to me that I am aware and knowledgeable about how my personal information will be used by commercial/government websites." No direct assessment of online privacy literacy based on test scores is part of the scale.

2.2. Empirical research on online privacy literacy

Looking at empirical research on online privacy literacy, we found a handful of studies. For example, in one study that featured interviews with 16 teenagers, Livingstone (2008) found that students had severe problems with handling privacy settings on SNSs. As explanation for the problems, Livingstone suggested a combination of imperfect interface design and a lack of Internet literacy. Next to this finding, levels of online privacy are, in general, considered to be low: For example, many users incorrectly believe that in terms of legal aspects their privacy is better protected than actually is the case (Hoofnagle et al., 2010). In a knowledge test with five questions about online and offline privacy, results showed that privacy knowledge was poor: 30% did not provide one correct answer at all, 45% had one or two correct answers, and only 3% were capable of answering all questions correctly (Hoofnagle et al., 2010). Similarly, in a sample with 419 adults, Park (2013) found low online privacy literacy in terms of technical familiarity and policy knowledge. Besides that, Park also detected an only moderate awareness of institutional surveillance practices. Finally, in an experimental study with 297 Korean students, Baek (2014) also confirmed the importance of digital literacy for privacy protection. The results showed that students with more literacy held privacy opinions that were more robust and that could not be changed as easily by reading privacy related news stories. According to the author, this showed that it is harder to manipulate peoples' privacy opinions if they have more Internet literacy. In general, online privacy behaviors exist for several dimensions, for example, the informational, social, and psychological dimension (Burgoon, 1982). Informational privacy behaviors measure how much identifying information people share about themselves. Social privacy behaviors capture how many other people can access shared information. Psychological privacy behaviors represent the intimacy of shared information. Several studies have tested and validated these dimensions in empirical research: For example, Dienlin and Trepte (2015) analyzed the influence of informational, social, and psychological privacy intentions on informational, social, and psychological privacy behaviors. The authors found that the relation between privacy intentions and the corresponding privacy behavior was weakest for the social privacy dimension (social: $\beta = 0.46$; informational: $\beta = 0.64$; psychological: $\beta = 0.79$). This implies that people who had the intention to limit access to their Facebook profiles did not always succeed in putting this limitation into practice. We suggest that a lack of online privacy literacy might be a relevant reason why people did not contrive to protect their privacy. Hence, it seems important to analyze online privacy literacy as a potential mediator.

2.3. Literature analysis

The literature analysis shows three gaps: First, to date no study analyzed which aspects might foster online privacy literacy. Second, to date no study analyzed if online privacy literacy might affect online privacy behavior. For example, do people who have more online privacy use more mechanisms to restrict access to their online profiles? Likewise, to date no study analyzed if online privacy literacy might affect psychological aspects. For example, does online privacy literacy increase the perceived online safety? Third, existing studies analyzed online privacy literacy with a rather broad and general understanding of privacy. By contrast, the study by Dienlin and Trepte (2015) suggests that online privacy literacy might be especially relevant for aspects of social privacy regulation, which is why in this study, we thus focus on social aspect of online privacy literacy.

3. Research model and hypotheses

3.1. Potential antecedents of online privacy literacy

One aim of this study is to discuss aspects that might foster online privacy literacy. We assume that two aspects are relevant: The time users have already spent on SNSs and the number of privacy changes users have already implemented. In what follows, we explain why we expect that time on SNSs and privacy changes are relevant for the development of privacy literacy.

For example, results from a project on UK children's and adolescents' online literacy (Livingstone, Bober, & Helsper, 2005) showed that the more time users have spent online, the more skilled they became at using the Internet (see also Livingstone, Haddon, Görzig, & Ólafsson, 2011). In a study with a sample of $N = 2739$ German Internet users, Taddicken (2011) similarly found that those users with a better school education and longer history of Internet usage were better able to evaluate privacy risks of social media than those users with less experience and lower education. In accordance, Lin (2015) found a positive association between frequency of visits and changes of privacy settings on Facebook, and Park and Jang (2014) reported a positive association between frequency of mobile Internet access and privacy knowledge. We thus suggest that the more time users spend online, the higher their online privacy literacy will be.

Hypothesis 1. The time spent on SNSs is associated with more online social privacy literacy.

In addition, it seems worthwhile to focus on specific past actions. Besides the aforementioned strategies such as limiting the audience (e.g., Krämer & Haferkamp, 2011) or maintaining different profiles (Rosenbaum et al., 2010), other strategies to protect social privacy can be found, such as: excluding contact information, not accepting befriending requests from strangers, deleting comments, or untagging and removing photographs (Litt, 2013; Young & Quan-Haase, 2013). We suggest that someone who has already used these strategies might show more online social privacy literacy than someone who has not. Moreover, users who have better Internet skills are more likely to change their privacy settings more often (boyd & Hargittai, 2010). We thus conclude that users who have already changed their privacy settings will also show more online social privacy literacy.

Hypothesis 2. Users who have changed their privacy settings more frequently show higher levels of online social privacy literacy.

3.2. Potential effects of online privacy literacy

Which aspects might be associated with higher levels of online social privacy literacy? We suggest that two aspects are especially relevant: social privacy behaviors and perceived privacy safety. In what follows, we explain why we suggest this relation.

In general, explaining user behavior on SNSs seems to be somewhat difficult. For example, several studies already addressed the issue that attitudes toward privacy behavior are distinct from the behavior itself (e.g., Acquisti & Gross, 2006; Dienlin & Trepte, 2015)—Barnes (2006) called this phenomenon the privacy paradox. However, current research increasingly refutes the privacy paradox, as significant relations between informational, social, as well as psychological privacy attitudes and the respective privacy behavior were found (Dienlin & Trepte, 2015). Besides attitudes, gratifications such as social capital, social support, or staying in touch with others are often found as motivational reasons behind the greater self-disclosure on SNSs (Ellison, Steinfield, & Lampe, 2007; Taddicken & Jers, 2011; Trepte & Reinecke, 2013). Likewise, we suggest that online privacy literacy might be a further factor that could relate to privacy behaviors. Thus, the question arises, in which way might online social privacy literacy influence social privacy behavior? One study suggested that the awareness of consequences resulting from privacy violations predicted information disclosure (i.e., use of privacy settings; Christofides, Muise, & Desmarais, 2012). Debatin, Lovejoy, Horn, and Hughes (2009) similarly found a significant positive relation between the understanding of privacy settings and the limitation of profile visibility. With a focus on privacy threats via phishing, Arachchilage and Love (2014) found that the combination of declarative and procedural knowledge positively influences self-efficacy, which in turn improved the behavior to thwart phishing attacks. The authors concluded that a lack of knowledge might account for the users' falling for privacy traps such as phishing. We thus reason that users who report more online social privacy literacy also show more online social privacy behaviors.

Hypothesis 3. Users who report higher levels of online social privacy literacy show social privacy behaviors.

Looking at the bigger picture, what might be the use of obtaining social privacy literacy? Will social privacy literacy eventually lead to positive outcomes, for example such as more perceived privacy safety? In what follows, we focus on the concept of safety as possible outcome of privacy literacy.

Safety is a basic need for humans (Maslow & Mittelmann, 1941). Maurice et al. (2001) defined safety as "a state in which hazards and conditions leading to physical, psychological or material harm are controlled in order to preserve the health and well-being of individuals and the community" (p. 238). This definition implies that one basic factor contributing to safety is control. In general, control is associated with positive outcomes. For example, looking at offline contexts, perceived control closely related to work satisfaction (Dwyer & Ganster, 1991). Looking at online contexts, similar positive results of control were obtained: A survey study with 576 students from a Midwestern University showed that the ability to execute software protections online was one of the two determinants for safe online behavior (LaRose, Rifon, Liu, & Lee, 2005). Hence, we argue that online privacy literacy will be associated with more perceived safety.

Hypothesis 4. Users, who report higher higher levels of online social privacy literacy, also perceive more online safety.

3.3. Open research questions

So far, we have analyzed potential antecedents and outcomes of online privacy literacy. This opens up a new question: Do the antecedents of online privacy literacy might also have a direct influence on the outcomes? Or, by contrast, does privacy literacy completely mediate the effect of time spent on SNSs and privacy regulation experience on privacy safety and social privacy behavior? Some evidence exists that there is a direct relationship between the antecedents and the outcomes—however, at this point, we do not know if this relation persists after controlling for the influence of online privacy literacy.

One piece of evidence for a direct relation is the longitudinal study by Lewis, Kaufman, and Christakis (2008), who asked 1710 American students and found that activity on Facebook predicted if users had a public or a private profile. Park (2013) reported similar results: Education as well as Internet experience were both positive predictors of information control behavior. Likewise, Litt (2013) found evidence for a trend pointing in the same direction: The more SNS accounts a user has or the more often a user is active on SNSs, the more diverse are the privacy tools he or she uses. Besides, Litt (2013) also found that technical familiarity is important for controlling technological boundaries. Finally, someone who is posting frequently on Facebook is also more likely to change his or her privacy settings (boyd & Hargittai, 2010). Consequently, the authors conclude that those who use Facebook more intensely have better privacy skills and—more importantly—are more certain in handling their privacy settings.

In conclusion, we suggest that there is a direct relation between the antecedents and outcomes of online privacy literacy. However, to date and to our knowledge no studies exist that analyzed this relation by including online privacy literacy. Therefore, even though there is evidence for a direct relation, it might be that online privacy literacy affects this relation by a mediation or even a suppression. As a result, we pose the following four research questions:

Research Questions: After controlling for privacy literacy, what is the association between (1) the time spent on SNSs and online social privacy behaviors, (2) the time spent on SNSs and perceived privacy safety on SNSs, (3) the experience with privacy regulations and online social privacy behaviors, (4) the experience with privacy regulations and perceived privacy safety on SNSs?

For an overview of the final research model, all hypotheses and the research questions see Fig. 1.

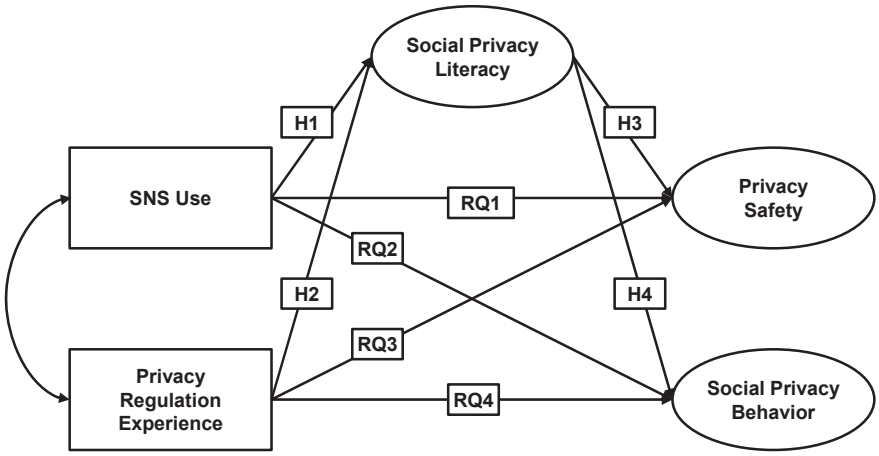

Fig. 1. The structural equation model that was tested.

4. Method

4.1. Participants and procedure

630 respondents participated in an online questionnaire that took place in Germany in October and November of 2012 (74% female, $M_{age} = 24$ years, $Range_{age} = 18–63$ years). Participation in the study was voluntary, and in order to avoid substantial dropout respondents did not need to answer all items in order to proceed with the questionnaire. Students who took part were able to receive course credits. Altogether, 424 (67.3%) students participated. The link to the study was also shared publicly, for example on SNSs such as Facebook or Twitter. As a result, the sample was self-selective and non-representative. Data of respondents below the age of 18 were deleted—privacy settings of minors are by default different compared to those of adults. Also, data of respondents without a Facebook account were deleted. As suggested by Subrahmanyam, Reich, Waechter, and Espinoza (2008), participants were asked to log into their Facebook account while answering the questionnaire, thus having the chance to look up information with the aim to improve data quality.

4.2. Measures

All items are listed in the Appendix, Table A1. For each variable's mean, standard deviation, skewness, and curtosis see Table 1. In order to test the scales for construct validity, we ran confirmatory factorial analyses (CFA), and in order to test reliability, we estimated the McDonald's composite reliability within the final model (see Table 1). Regarding composite reliability, values above $\omega = 0.6$ imply good fit (Bagozzi & Yi, 1988)—which was the case for all variables. Hence, results showed that reliability was adequate for all variables. As Cronbach's alpha should not be used to estimate reliability for non essentially tau-equivalent items (Raykov, 2001), we reported it only for reasons of conventionality (Table 1).

4.2.1. SNS use

SNS use measured the time respondents typically spent each week on Facebook. We measured SNSs use in minutes with one single item. The scale's mean was $M = 347$ min and the standard deviation $SD = 662$ min. For the analyses, the log of the variables was used to normalize the distribution ($M = 4.91$, $SD = 1.81$).

4.2.2. Privacy regulation experience

Privacy regulation experience captured how often respondents had already changed their privacy settings on Facebook. We used a single-item measure with answers ranging on an ordinal scale from 1 = *never*, 2 = *1–3 times*, 3 = *4–6 times*, 4 = *7–9 times*, 5 = *10–12 times*, 6 = *13–15 times*, to 7 = *more than 15 times*. In addition, we provided the option *I do not know*, which we coded as missing value. The scale's mean was $M = 2.98$ and the standard deviation $SD = 1.23$.

4.2.3. Social privacy literacy

Social privacy literacy measured perceived skill to regulate privacy settings on Facebook. One example item was "I know how to restrict access to profile information such as hobbies or interests." On six items, respondents indicated their agreement on a scale ranging from 1 = *I absolutely do not know how to do this* to 5 = *I completely know how to do this*. The scale's mean was $M = 3.77$, the standard deviation $SD = 0.91$. A CFA showed that construct validity was only moderate ($\chi^2 = 37.17$, $df = 9$, $p < .01$, CFI = 0.97, TLI = 0.96, RMSEA = 0.08, 90% CI [0.05, 0.10]), which is why we deleted two malfunctioning items. The updated scale showed good construct validity ($\chi^2 = 0.75$, $df = 2$, $p = .69$, CFI = 1, TLI = 1, RMSEA < 0.01, 90% CI [<0.01, 0.06]).

4.2.4. Social privacy behavior

Social privacy behaviors captured the accessibility of respondents' Facebook profiles. One example item was: "Who can see your status updates on your Facebook profile?" Respondents

Table 1
Psychometric properties.

Variable	M	SD	Skew	Curt	Reliability		Factorial validity		
					α	ω	AVE	MSV	ASV
SNS use	4.91	1.81	−1.17	1.33	–	–	–	–	–
Privacy regulation experience	2.98	1.23	1.32	2.01	–	–	–	–	–
Social privacy literacy	3.77	0.91	−0.70	0.38	0.84	0.84	0.58	0.06	<0.01
Social privacy behavior	3.18	0.72	−0.02	0.99	0.90	0.92	0.83	0.07	<0.01
Privacy safety	2.63	0.89	0.26	−0.27	0.73	0.74	0.49	0.07	<0.01

answered 15 items on an ordinal scale ranging from 1 = *only me*, 2 = *some of my friends/particular friends lists only*, 3 = *all of my friends*, 4 = *my friends and their friends*, to 5 = *everybody (public)*. Also, the option *I do not know* was provided and coded as missing value. Items were reverse coded, such that higher values indicated stricter privacy behaviors. As the scale was lengthy and consisted of ordinal items, we computed two item parcels by using the odd-even procedure (Yang, Nay, & Hoyle, 2010). The scale's mean was $M = 3.18$, the standard deviation $SD = 0.72$.

4.2.5. Privacy safety

Privacy safety measured perceived safety with regard to the three aspects of online privacy: informational, social, and psychological privacy (Burgoon, 1982). For example, the informational privacy safety item was: "On Facebook, I feel safe regarding my personal data." The scale's mean was $M = 2.63$, the standard deviation $SD = 0.89$. Construct validity was good ($\chi^2 = 0.01$, $df = 1$, $p = .93$, CFI = 1, TLI = 1.01, RMSEA < 0.01, 90% CI [<0.01, 0.04]).

4.3. Data analysis

We analyzed the hypotheses with structural equation modeling (SEM). SEM cannot operate with missing values, which is why either missing values need to be estimated based on the existing date or, instead, cases with missing data need to be deleted altogether. As mentioned above, answering the items was voluntary in this study. Consequently, participants answered only 77% of all the items that we included in the final model, which implies a comparatively high number of missing values. As conclusion, we decided to estimate missing values based on the full information maximum likelihood approach (Arbuckle, 1996)—instead of deleting participants that did not provide complete data, which probably would have increased the chance of a systematic dropout. Next, SEM has the assumption that all items follow a multivariate normal distribution. We thus first looked at the distribution of the individual items, which showed that items for the privacy literacy variable were somewhat skewed (e.g., see Table 1). In addition, we conducted a multivariate Shapiro-Wilk normality test, which also showed a violation of multivariate normality ($W = 0.96$, $p \leq .001$). Hence, we used a robust maximum likelihood estimation with robust (Huber-White) standard errors and a scaled test statistic that is (asymptotically) equal to the Yuan-Bentler test statistic (Rosseel, 2015). We tested our hypotheses with a two-tailed 5% level of significance. To estimate effect sizes, the correlation coefficient r was used (Field, Miles, & Field, 2012). Values exceeding $r = 0.1$ were regarded as small effects, $r = 0.3$ as medium-sized effects, and $r = 0.5$ as strong effects. The data were analyzed with the Software R, version 3.2.2 (R Core Team, 2015) and the SEMs were calculated with the package lavaan, version 0.5–18 (Rosseel, 2012).[2]

5. Results

5.1. Model fit and factorial validity

The analyses showed that the model fit the data well ($\chi^2 = 31.92$, $df = 36$, $p = .66$, CFI = 1.00, TLI = 1.00, RMSEA < 0.01, 90% CI [0.00, 0.02]), as all recommended thresholds were met (Hu & Bentler, 1999). To check for factorial validity, we computed the average variance extracted (AVE), the maximum shared variance (MSV), and the average shared variance (ASV). As benchmarks, values above AVE = 0.5 signify good factorial validity (Fornell & Larcker, 1981; see Table 4), and both MSV and ASV need to be below the AVE. With the exception of privacy safety, which was marginally below the recommended threshold (AVE = 0.49), all variables met the recommended thresholds, implying good factorial validity.

5.2. Analyses of hypotheses and research questions

Hypothesis 1 stated that users who spent more time on SNSs would show higher levels of online privacy literacy. The data confirmed Hypothesis 1: Users who spent more time online also reported higher levels of online privacy literacy ($b = 0.07$, $\beta = 0.16$, $p = .002$, $SE = 0.02$). Hypothesis 2 suggested that users who have changed their privacy settings more frequently would also report higher levels of online privacy literacy. The data confirmed Hypothesis 2: Users who had changed their privacy settings more frequently also reported higher levels of online privacy literacy ($b = 0.17$, $\beta = 0.28$, $p < .001$, $SE = 0.03$). Hypothesis 3 suggested that users who report more social privacy literacy would also show more social privacy behaviors. The data confirmed Hypothesis 3: Users who reported higher levels of privacy literacy also restricted the access to their SNS profiles more strongly ($b = 0.13$, $\beta = 0.14$, $p = .050$, $SE = 0.07$). Hypothesis 4 suggested that users who report more privacy control would also report more perceived safety with regard to their online privacy. The data also confirmed Hypothesis 4: Participants who reported more privacy control also reported more perceived privacy safety ($b = 0.25$, $\beta = 0.26$, $p < .001$, $SE = 0.06$). In terms of effect sizes, all effects that we found were small.

The research questions analyzed the effects of time spent on SNSs and prior privacy regulations on social privacy behaviors and privacy safety, when controlling for the influence of online privacy literacy. Regarding RQ1, we found a negative association between the time spent on SNSs and online social privacy behaviors ($b = -0.08$, $\beta = -0.20$, $p < .001$, $SE = 0.02$). With regard to RQ2, we found a positive relation between the time spent on SNSs and perceived privacy safety on SNSs ($b = 0.05$, $\beta = 0.14$, $p = .004$, $SE = 0.02$). Regarding RQ3, we found a positive relation between experience with privacy regulations and online social privacy behaviors ($b = 0.11$, $\beta = 0.19$, $p < .001$, $SE = 0.03$). With regard to RQ4, we found a negative relation between experience with privacy regulations and perceived privacy safety on SNSs ($b = -0.07$, $\beta = -0.13$, $p = .029$, $SE = 0.03$). Taken together, the results for the research questions showed that after we controlled for the influence of online privacy literacy, people who spend more time on Facebook still felt safer but also showed less privacy behaviors—the latter being a suppression effect. Similarly, after we controlled for the influence of online privacy literacy, people who had more experience with privacy regulations still used more privacy behaviors but, at the same time, felt less secure on SNSs—with the latter, again, being a suppression effect. Therefore, even though both antecedents related to online privacy literacy in a positive direction, we found this positive direction for only two direct effects. The two other negative direct effects implied a suppression effect, which underscores the importance to include privacy literacy as a mediator.

For an overview of all results, see Fig. 2.

6. Discussion

To date, online privacy literacy is still a comparatively new strand of research, with only a few studies that analyzed its basic premises in an empirical approach. Thus, the main purpose of this study was to increase the understanding of online privacy literacy. It is the first study that analyzed both potential antecedents and

[2] We uploaded the data, the analyses, an R Studio project file, and a PDF with the documentation of the results in the following online repository: https://osf.io/5z9vw/?view_only=09985747a4dc43d69e8f8734138eff41.

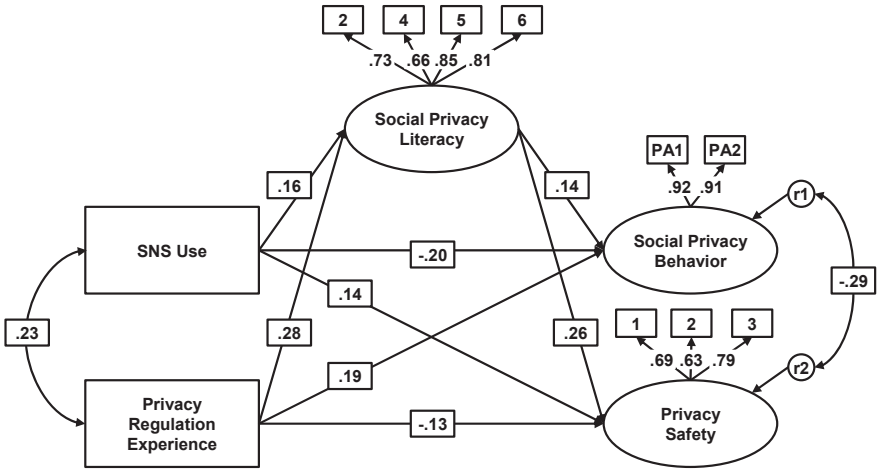

Fig. 2. Results of the model. *Note*: All paths were significant based on a 5% significance level. Social privacy behavior consisted of 15 items that we measured in two parcels. Social privacy literacy initially consisted of 6 items, of which we dropped items 1 and 3.

outcomes of online privacy literacy in one single SEM.

Regarding the antecedents, we found that time spent on SNSs and frequency of changing privacy settings positively related to online privacy literacy (Hypothesis 1 and 2). This is in line with extant literature: Park (2013), for example, showed that Internet experience contributed to the perceived control over private information. Likewise, Park and Jang (2014) reported that frequency of Internet access would positively relate to privacy knowledge. As a result, it seems worthwhile to encourage users to make themselves more familiar with their privacy settings, and to change some privacy settings occasionally—with a good chance that this will increase their online privacy literacy.

Furthermore, we suggest that fostering online privacy literacy is actually relevant and important. We illustrated this in the second part of our study, in which we analyzed potential outcomes of online privacy literacy. First, we found that respondents with higher levels of social privacy literacy also showed more social privacy regulation behaviors (Hypothesis 3). This implies that online privacy literacy contributes to a more cautious SNS activity. That is, online privacy literacy might help to reduce potential threats to privacy online. For example, taking part in SNSs necessitates the disclosure of personal information (Burke, Marlow, & Lento, 2009), which makes users vulnerable to privacy violations (Petronio, 2002). Hence, users need to enact social privacy behaviors—for example, by restricting access to their profiles—so that others cannot abuse disclosed information. With this study, we showed that social privacy literacy might foster these social privacy behaviors, which we suggest is a potentially desirable behavior. Secondly, we found that social privacy literacy was associated with higher levels of perceived privacy safety on SNSs. We can now add to this notion that higher levels of social privacy literacy are related to privacy control. This finding seems relevant because of two reasons: First, perceived control over one's private information is necessary when it comes to feeling comfortable sharing personal information online. Second, and arguably more important, privacy control is necessary when it comes to protecting oneself from potential privacy threats, such as online identity theft, fraud, or bullying.

Second, as another potential outcome of online privacy literacy, we found that people who had more online privacy literacy also felt safer when using SNSs (Hypothesis 4). No studies exist that have already tested this hypothesis; however, our results seem in line with similar studies: For example, boyd (2008) and Dinev and Hart (2006) suggested a negative relation between Internet literacy and privacy concern. As one can argue that privacy concerns are somewhat like the opposite of privacy safety, also extant literature supports the plausibility of our findings. Likewise, Livingstone et al. (2011) stated that children who are more digitally literate have smaller chances of experiencing harm when being online. Similarly, Litt and Hargittai (2014) surveyed 547 young adults and found that respondents who were more literate were also less likely to encounter negative experiences online. Taken together, our finding that online privacy literacy leverages perceived privacy safety on SNSs stresses the importance and relevance of online privacy literacy.

In four research questions, we analyzed the potential effect of time spent on SNSs and past privacy regulations on social privacy behaviors and privacy safety, after controlling for online privacy literacy. Interestingly, we found two suppressor effects: First, the time spent on SNSs negatively related to social privacy behaviors (Research Question 1). One could explain this by the fact that we used cross-sectional data. That is, people who use SNSs less frequently might, in general, be more cautious online and thus use more social privacy behaviors. However, in the end, only longitudinal data can answer this question effectively. Second, we found that prior privacy regulations negatively related to perceived safety (Research Question 4), which is, again, a suppressor effect. Likewise, one could explain this finding be the fact that people who, in general, do not feel safe on SNSs change their privacy settings more frequently. However, this does not rule out that changing privacy settings results in more privacy safety—again, only longitudinal data can explain the potential causality, as cross-sectional relations do not imply causal effects. In addition, we found that people who spent more time on SNSs also feel safer on SNSs (Research Question 2), and that people who have changed their privacy settings more often in the past also restricted access to their profiles more strongly (Research Question 3). In conclusion, the research questions revealed that it is important to control for online privacy literacy, as it offers a better picture of the relation between the variables presented here.

6.1. Limitations and future perspective

Regarding the sample, one can rise several points of criticism. First, the data was not representative of the German population, as 67% of all respondents were students. Second, for all items that we used for the SEM, we had 23% missing values, which was because answering of all items was not mandatory but optional. Third, the

data was cross-sectional. Thus, we cannot prove the direction of effects with a statistical method. In this study, we determined the direction of effects based on deductive reasoning only. For example, one can suggest that increased online privacy literacy itself makes people change their privacy settings more often. Therefore, in order to analyze the directions of effects as suggested in this paper longitudinal data are necessary. However, these three problems are inherent to most questionnaire-based designs. Next, it might be that a third external common factor explained the shared variance of online privacy literacy and privacy safety. For example, this common third factor might be self-confidence or self-determination, potentially accounting for the variables' shared variance.

For future research, the following considerations seem worthwhile: In this study, we analyzed online privacy literacy that is horizontal. In other words, we measured the self-perceived skills of the respondents regarding preventing access for their peers or friends. For future research, it might be interesting to analyze vertical online privacy literacy also. That is, how good are users at regulating access to their data for governments, providers, and institutions? Moreover, we measured online privacy literacy based on self-ratings. However, Li (2008) showed that people are too optimistic regarding their own Internet skills. In order to avoid this so-called optimism bias, future research might use objective tests of online privacy literacy, such as the online privacy literacy scale (Masur, Teutsch, & Trepte, 2015). Next, we used variables such as SNS use and privacy regulation experience as antecedents for online privacy literacy. For future research, it would be interesting to include concrete interventions as potential antecedents. This could answer the question if it might be possible to proactively leverage online privacy literacy—for example, by doing computer courses in schools.

6.2. Conclusion

This study highlighted the importance of leveraging privacy literacy: First, privacy literacy relates to more social privacy behaviors. Second, privacy literacy is associated with more perceived safety on SNSs—which is an important need, considering that 1.49 billion people use Facebook on a monthly basis. Taken together, online privacy literacy is not only important to feel safe but also to be safe. Online threats can endanger most if not all areas of our offline life, and thus an appropriate online behavior is equally important as locking doors, closing curtains, and lowering voices. In conclusion, we suggest that when SNS users want to improve their privacy online and when they want to feel safer on SNSs, they should aim to increase their online privacy literacy.

Acknowledgments

We would like to express our gratitude to Fiona Dwinger, Philipp Masur, and Michael Scharkow who provided valuable advice during the process of writing the paper.

Appendix

Table A1
Items used in the study.

Variable	Item
SNS use	How many hours a week do you typically spend on Facebook?
Privacy regulation experience	How often have you already changed your privacy settings on Facebook?
Online privacy literacy	
SPL1	- I know how to delete or deactivate my account
SPL2	- I know how to restrict access to profile information such as hobbies, interests
SPL3	- I know how to make my profile not accessible via Google
SPL4	- I know how to control if others tag my name on pictures
SPL5	- I know how to restrict access to my postings
SPL6	- I know how to restrict access to my contact information (e.g. name, address)
Privacy safety	
	On Facebook, I feel safe regarding
SPS1	- My personal data
SPS2	- Who can contact me
SPS3	- The personal exchange of thoughts and feelings
Social privacy behavior	
	Who can see the following things on your Facebook profile?
SPB1	Contact information such as e-mail or phone
SPB2	Date of birth
SPB3	Age
SPB4	Relationship status
SPB5	Religion
SPB6	Current school/university/employer
SPB7	Residential address
SPB8	Sexual orientation
SPB9	Interests (music, sports, hobbies)
SPB10	Status updates/activity feeds
SPB11	List of friends
SPB12	Photos
SPB13	Political orientation
SPB14	Current location
SPB15	Who can see what others post on your profile?

References

Acquisti, A., & Gross, R. (2006). *Imagined communities: Awareness, information sharing, and privacy on the Facebook*. Paper presented at the 6th workshop on privacy enhancing technologies, Cambridge, UK. http://dx.doi.org/10.1007/11957454_3.

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: a phishing threat avoidance perspective. *Computers in Human Behavior, 38*, 304–312. http://dx.doi.org/10.1016/j.chb.2014.05.046.

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.
Baek, Y. M. (2014). Solving the privacy paradox: a counter-argument experimental approach. *Computers in Human Behavior, 38*, 33–42. http://dx.doi.org/10.1016/j.chb.2014.05.006.
Bagozzi, R. P., & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science, 16*, 74–94. http://dx.doi.org/10.1007/BF02723327.
Barnes, S. B. (2006). A privacy paradox: social networking in the United States. *First Monday, 11*(9). http://dx.doi.org/10.5210/fm.v11i9.1394.
boyd, d. (2008). *Taken out of context: American teen sociality in networked publics*. Ph.D. dissertation. University of California at Berkeley www.danah.org/papers/TakenOutOfContext.pdf. Retrieved 19.02.15.
boyd, d., & Hargittai, E. (2010). Facebook privacy settings: who cares? *First Monday, 15*(8). http://dx.doi.org/10.5210/fm.v15i8.3086.
Burgoon, J. K. (1982). Privacy and communication. In M. Burgoon (Ed.), *Communication yearbook 6*, (pp. 206–249). Beverly Hills, CA: Sage.
Burke, M., Marlow, C., & Lento, T. (2009, April 4–9). *Feed me: Motivating newcomer contribution in social network sites*. Paper presented at the Proceedings of the 27th International conference on human factors in computing systems.
Christofides, E., Muise, A., & Desmarais, S. (2012). Hey mom, what's on your Facebook? Comparing Facebook disclosure and privacy in adolescents and adults. *Social Psychological and Personality Science, 3*, 48–54. http://dx.doi.org/10.1177/1948550611408619.
Debatin, B. (2011). Ethics, privacy, and self-restraint in social networking. In S. Trepte, & L. Reinecke (Eds.), *Privacy online: Perspectives on privacy and self-disclosure in the social web* (pp. 47–60). Berlin, Germany: Springer. http://dx.doi.org/10.1007/978-3-642-21521-6_5.
Debatin, B., Lovejoy, J. P., Horn, A. K., & Hughes, B. N. (2009). Facebook and online privacy: attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication, 15*, 83–108. http://dx.doi.org/10.1111/j.1083-6101.2009.01494.x.
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. http://dx.doi.org/10.1002/ejsp.2049.
Dinev, T., & Hart, P. (2006). Internet privacy concerns and social awareness as determinants of intention to transact. *International Journal of Electronic Commerce, 10*, 7–29. http://dx.doi.org/10.2753/JEC1086-4415100201.
Dwyer, D. J., & Ganster, D. C. (1991). The effects of job demands and control on employee attendance and satisfaction. *Journal of Organizational Behavior, 12*, 595–608. http://dx.doi.org/10.1002/job.4030120704.
Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The benefits of Facebook "friends": social capital and college students' use of online social network sites. *Journal of Computer-Mediated Communication, 12*, 1143–1168. http://dx.doi.org/10.1111/j.1083-6101.2007.00367.x.
Eurobarometer. (2010). *Attitudes on data protection and electronic identity in the European Union*. Brussels: European Commission. http://ec.europa.eu/public_opinion/archives/ebs/ebs_335_en.pdf. Retrieved 19.02.15.
Facebook. (2015). *Statistics*. http://newsroom.fb.com/company-info/. Retrieved 13.02.15.
Field, A. P., Miles, J., & Field, Z. (2012). *Discovering statistics using R*. Thousand Oaks, CA: Sage.
Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*, 39–50. http://dx.doi.org/10.2307/3151312.
Frees, B., & Koch, W. (2015). Internetnutzung: Frequenz und Vielfalt nehmen in allen Altersgruppen zu [Internet use: frequency and variety increase for all age groups]. *Media Perspektiven, 9*, 366–377. http://www.ard-zdf-onlinestudie.de/index.php?id=540. Retrieved 13.10.15.
Hong, W., & Thong, J. Y. (2013). Internet privacy concerns: an integrated conceptualization and four empirical studies. *MIS Quarterly, 37*, 275–298. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2229627. Retrieved 19.02.15.
Hoofnagle, C. J., King, J., Li, S., & Turow, J. (2010). *How different are young adults from older adults when it comes to information privacy attitudes and policies?*. Available at SSRN 1589864. http://dx.doi.org/10.2139/ssrn.1589864.
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*, 1–55. http://dx.doi.org/10.1080/10705519909540118.
Kobsa, A., Patil, S., & Meyer, B. (2012). Privacy in instant messaging: an impression management model. *Behaviour & Information Technology, 31*, 355–370. http://dx.doi.org/10.1080/01449291003611326.
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. 127–142). Berlin, Germany: Springer. http://dx.doi.org/10.1007/978-3-642-21521-6_10.
LaRose, R., Rifon, N., Liu, S., & Lee, D. (2005, May). *Understanding online safety behavior: a multivariate model. Paper presented at the International communication association*. New York, NY: Communication and Technology Division.
Lewis, K., Kaufman, J., & Christakis, N. (2008). The taste for privacy: an analysis of college student privacy settings in an online social network. *Journal of Computer-Mediated Communication, 14*, 79–100. http://dx.doi.org/10.1111/j.1083-6101.2008.01432.x.
Li. (2008). Third-person effect, optimistic bias, and sufficiency resource in internet use. *Journal of Communication, 58*, 568–587. http://dx.doi.org/10.1111/j.1460-2466.2008.00400.x.
Lin, K. M. (2015, July 6–9). *Understanding undergraduates' information literacy from their Facebook usage*. Paper presented at the 2015 IEEE 15th International conference on advanced learning technologies (ICALT), Hualien County, Taiwan.
Litt, E. (2013). Understanding social network site users' privacy tool use. *Computers in Human Behavior, 29*, 1649–1656. http://dx.doi.org/10.1016/j.chb.2013.01.049.
Litt, E., & Hargittai, E. (2014). A bumpy ride on the information superhighway: exploring turbulence online. *Computers in Human Behavior, 36*, 520–529. http://dx.doi.org/10.1016/j.chb.2014.04.027.
Livingstone, S. (2008). Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression. *New Media & Society, 10*, 393–411. http://dx.doi.org/10.1177/1461444808089415.
Livingstone, S., Bober, M., & Helsper, E. (2005). *Internet literacy among children and young people: Findings from the UK Children Go Online Project*. London, UK: LSE. http://eprints.lse.ac.uk/397/. Retrieved 19.02.15.
Livingstone, S., Haddon, L., Görzig, A., & Ólafsson, K. (2011). *EU kids online final report: EU Kids online*. London, UK: London School of Economics & Political Science. http://eprints.lse.ac.uk/39351/. Retrieved 19.02.15.
Maslow, A. H., & Mittelmann, B. (1941). *Principles of abnormal psychology*. New York, NY: Harper & Brothers.
Masur, P. K., Teutsch, D., & Trepte. (2015, May 21–25). *How skilled are internet users when it comes to online privacy and data protection? Development and validation of the online privacy literacy scale (OPLIS)*. Paper presented at the 65th annual conference of the International Communication Association, San Juan (Puerto Rico).
Maurice, P., Lavoie, M., Laflamme, L., Svanström, L., Romer, C., & Anderson, R. (2001). Safety and safety promotion: definitions for operational developments. *Injury Control and Safety Promotion, 8*, 237–240. http://dx.doi.org/10.1076/icsp.8.4.237.3331.
Park, Y. J. (2013). Digital literacy and privacy behavior online. *Communication Research, 40*, 215–236. http://dx.doi.org/10.1177/0093650211418338.
Park, Y. J., & Jang, S. M. (2014). Understanding privacy knowledge and skill in mobile communication. *Computers in Human Behavior, 38*, 296–303. http://dx.doi.org/10.1016/j.chb.2014.05.041.
Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. Albany, NY: State University of New York Press.
R Core Team. (2015). *Software R, version 3.0.1*. http://www.r-project.org/. Retrieved 19.02.15.
Raykov, T. (2001). Estimation of congeneric scale reliability using covariance structure analysis with nonlinear constraints. *British Journal of Mathematical and Statistical Psychology, 54*, 315–323.
Rosenbaum, J. E., Johnson, B. K., Stepman, P. A., & Nuijten, K. C. (2010, April). *Just being themselves? Goals and strategies for self-presentation on Facebook*. Paper presented at the 80th annual conference of the Southern States Communication Association, Memphis, TN http://www.benjaminkjohnson.com/wp-content/uploads/2010/09/Just_Being_Themselves_Final.pdf. Retrieved 19.02.15.
Rosseel, Y. (2012). lavaan: an R package for structural equation modeling. *Journal of Statistical Software, 48*, 1–36. http://www.jstatsoft.org/v48/i02/. Retrieved 19.02.15.
Rosseel, Y. (2015). *Estimators*. Retrieved from http://lavaan.ugent.be/tutorial/est.html.
Subrahmanyam, K., Reich, S. M., Waechter, N., & Espinoza, G. (2008). Online and offline social networks: use of social networking sites by emerging adults. *Journal of Applied Developmental Psychology, 29*, 420–433. http://dx.doi.org/10.1016/j.appdev.2008.07.003.
Taddicken, M. (2011). Selbstoffenbarung im social web [Self-disclosure on the social web]. *Publizistik, 56*, 281–303. http://dx.doi.org/10.1007/s11616-011-0123-8.
Taddicken, M. (2014). The 'privacy paradox' in the social web: the impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *Journal of Computer-Mediated Communication, 19*, 248–273. http://dx.doi.org/10.1111/jcc4.12052.
Taddicken, M., & Jers, C. (2011). The uses of privacy online: trading a loss of privacy for social web gratifications? In S. Trepte, & L. Reinecke (Eds.), *Privacy online: Perspectives on privacy and self-disclosure in the social web* (pp. 143–154). Berlin, Germany: Springer. http://dx.doi.org/10.1007/978-3-642-21521-6_11.
Trepte, S., & Reinecke, L. (2011). The social web as a 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. 61–73). Berlin, Germany: Springer. http://dx.doi.org/10.1007/978-3-642-21521-6_6.
Trepte, S., & Reinecke, L. (2013). The reciprocal effects of social network site use and the disposition for self-disclosure: a longitudinal study. *Computers in Human Behavior, 29*, 1102–1112. http://dx.doi.org/10.1016/j.chb.2012.10.002.
Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., et al. (2015). Do people know about privacy and data protection strategies? Towards the "online privacy literacy scale" (OPLIS). In S. Gutwirth, R. Leenes, & P. de Hert (Eds.), *Reforming European data protection law* (pp. 333–365). Heidelberg, Germany: Springer. http://dx.doi.org/10.1007/978-94-017-9385-8.
Westin, A. F. (1967). *Privacy and freedom*. New York, NY: Atheneum.
Yang, C., Nay, S., & Hoyle, R. H. (2010). Three approaches to using lengthy ordinal scales in structural equation models: parceling, latent scoring, and shortening scales. *Applied Psychological Measurement, 34*, 122–142. http://dx.doi.org/10.1177/0146621609338592.
Young, A. L., & Quan-Haase, A. (2013). Privacy protection strategies on Facebook. *Information, Communication & Society, 16*, 479–500. http://dx.doi.org/10.1080/1369118X.2013.777757.