The Shorter the Better? Effects of Privacy Policy Length on Online Privacy Decision-Making

Meier, Yannic; Schäwel, Johanna; Krämer, Nicole C.

Media and Communication (ISSN: 2183–2439)
2020, Volume 8, Issue 2, Pages 291–301
DOI: 10.17645/mac.v8i2.2846

Article

The Shorter the Better? Effects of Privacy Policy Length on Online Privacy Decision-Making

Yannic Meier [1,*], Johanna Schäwel [2] and Nicole C. Krämer [1]

[1] Social Psychology: Media and Communication, University of Duisburg-Essen, 47057 Duisburg, Germany;
E-Mails: yannic.meier@uni-due.de (Y.M.), nicole.kraemer@uni-due.de (N.C.K.)
[2] Department of Media Psychology, University of Hohenheim, 70593 Stuttgart, Germany;
E-Mail: johanna.schaewel@uni-hohenheim.de

* Corresponding author

Submitted: 29 January 2020 | Accepted: 1 May 2020 | Published: 23 June 2020

Abstract
Privacy policies provide Internet users with the possibility to inform themselves about websites' usage of their disclosed personal data. Strikingly, however, most people tend not to read privacy policies because they are long and cumbersome, indicating that people do not wish to expend much (cognitive) effort on reading such policies. The present study aimed to examine whether shorter privacy policies can be beneficial in informing users about a social networking site's (SNS) privacy practices, and to investigate associations between variables relevant for privacy decision-making using one theory-based integrative model. In an online experiment, participants ($N = 305$) were asked to create a personal account on an SNS after being given the option to read the privacy policy. Privacy policy length and the SNS's level of privacy were varied, creating a 2 (policy length) × 2 (level of privacy) between-subjects design. The results revealed that participants who saw short policies spent less time on reading but gained higher knowledge about the SNS's privacy practices—due to the fact that they spent more reading time per word. Factual privacy policy knowledge was found to be an indicator for participants' subjective privacy perception. The perception and evaluation of the specific SNS´s privacy level influenced the assessment of privacy costs and benefits. Particularly when benefits were perceived as high, self-disclosure was increased.

Keywords
online privacy; privacy calculus; privacy policy; self-disclosure; social networking site

Issue
This article is part of the issue "The Politics of Privacy: Communication and Media Perspectives in Privacy Research" edited by Johanna E. Möller (Johannes Gutenberg University Mainz, Germany), Jakub Nowak (Maria Curie-Sklodowska University, Poland), Sigrid Kannengießer (University of Bremen, Germany) and Judith E. Möller (University of Amsterdam, The Netherlands).

1. Introduction

To fully enjoy the advantages of the Internet, users often need to disclose personal information to other users or to companies. According to the privacy calculus approach, decisions regarding such disclosure are based on the perception of disclosure benefits and privacy costs (Culnan & Armstrong, 1999), but they are also thought to be dependent on the subjective perception of the current privacy level (Dienlin, 2014). While benefits of sharing personal information often occur immediately and are easy to grasp (because they are the main reason for disclosure), users appear to have difficulties in predicting privacy costs, as they are often abstract and occur with a time delay (if they occur at all). Usually, reading a website's privacy policy is one possibility for Internet users to inform themselves about the privacy costs that might arise from using the respective website. A privacy policy is a written statement about a website's privacy practices (i.e., the extent to which a website collects, uses, and disseminates user data). Since the EU General Data Protection Regulation (GDPR) came into force, website providers have been obligated to use easily understandable language in their privacy policies. However, the length of policies might still be based on companies' primary interest in safeguarding themselves, i.e., by providing the necessary information and thus acting lawfully, rather than on providing the best support for users (i.e., easy-to-read and understandable information). It has been found that only 13% of European Internet users fully read privacy policies, whereas 47% read privacy policies only partially and 37% never read privacy policies (European Commission, 2019). The main reasons stated for reading policies only partially or not at all were that they are too long and too complex (European Commission, 2019), indicating that many users are unwilling to expend much time and cognitive effort on informing themselves about a website's privacy practices.

To address this problem, the first aim of the current article is to focus on the length of privacy policies by investigating whether short policies can be more effective in informing users. The second aim is to test different assumptions relevant for online privacy decision-making that stem from two approaches combined into one integrative model. These approaches are the privacy process model (Dienlin, 2014) and the privacy calculus (Culnan & Armstrong, 1999). The integrative model comprises knowledge about the policy's content, the subjective perception of the privacy level, and the assessment of privacy risk likelihood and disclosure benefits. In the present study, participants were asked to create a personal account on a social networking site (SNS), having been given the option to read one of the SNS's privacy policies beforehand. To gain a better understanding of the link between policy knowledge and the perception of online privacy, we varied not only the length of the privacy policies but also the SNS's actual level of privacy (privacy-intrusive vs. privacy-friendly), thus creating a 2 (policy length) × 2 (level of privacy) between-subjects design.

2. Literature Review

2.1. Privacy Policy Length

According to the limited capacity model of motivated mediated message processing (LC4MP), people have limited available cognitive resources to process messages (Lang, 2000). The amount of available resources to process particular messages depends on the individual. Generally speaking, however, simple messages should lead to a higher likelihood of being processed compared to complex messages, since fewer (cognitive) resources are required and people are thus more easily motivated to engage in message processing (Lang, 2017). This approach can serve as an explanation for why few Internet users fully read privacy policies. Many people believe that privacy policies are too long and elusive (European Commission, 2019), implying that reading and understanding them requires cognitive or time effort. Deriving from this observation, the question arises whether shorter privacy policies that summarize the most relevant points of long policies might be more effective in informing users about the collection, usage, and dissemination of their personal data compared to the usually provided privacy policies. Short privacy policies might be more effective because people anticipate less time and cognitive effort and can more easily extract relevant information. Thus, one aim of the current study is to investigate whether users who are confronted with short policies acquire greater knowledge about the privacy practices of the SNS—potentially because it is less effortful to extract relevant information—than users who see extensive policies. One hint that participants require less cognitive effort would be that they spend less time reading the short policies but spend more time extracting relevant information (i.e., reading time per word). This should in turn result in higher knowledge about the policy's content. Therefore, we propose the following hypotheses:

> Hypothesis 1 (H1): Participants who see a short privacy policy will acquire greater knowledge about the SNS's privacy practices than participants who see a long privacy policy.

> Hypothesis 2 (H2): Participants who see a short privacy policy will have a higher reading time per word than participants who see a long privacy policy.

> Hypothesis 3 (H3): The reading time per word will be positively related to knowledge about the SNS's privacy practices.

2.2. Subjective Privacy Perception

The privacy process model (Dienlin, 2014) postulates that people form a perception of privacy in any situation, both online and offline, meaning that they assess and evaluate every situation in terms of its specific privacy. For instance, being in one's own four walls should lead to a different sense of privacy than being in a public place. Likewise, different privacy perceptions might also occur online, for instance because one website is evaluated to be more private than another. However, a situation's actual level of privacy and people's perception thereof can greatly diverge (Dienlin, 2014), creating a mismatch between actual privacy levels and people's beliefs about how private the situation is (Trepte & Reinecke, 2011). This difficulty in evaluating one's current privacy level seems to be even higher in online situations than offline (Teutsch, Masur, & Trepte, 2018). Apparently, people regularly perceive privacy to be greater than it actually is. As a prominent example of this, Facebook users tend to feel "private" when they are interacting with friends, but forget that the communication is accessible to a larger audience (Vitak, 2012) and to Facebook itself.

To date, studies on how people's perception of online privacy is formed or how it can be conceptualized are scarce. Scholars have primarily focused on concepts such as privacy concerns, attitudes or intentions (e.g., Dienlin & Trepte, 2015), while research on individuals' subjective perception of the privacy level in a specific situation seems to be lacking. While privacy concerns focus on one's negative emotional attitude (Dienlin & Trepte, 2015) towards potential negative effects on one's privacy, the perception of privacy captures one's assessment of the current degree of privacy with a view to a specific application or situation. Classical privacy theories argued that privacy is about freedom and control over the decision of when and to whom to disclose (Altman, 1975; Westin, 1967). This implies that the subjective perception of a given privacy level might involve a sense of control. However, classical theories do not explicitly explain how individuals form a perception of current privacy. Focusing on this issue, a recent qualitative study by Teutsch et al. (2018) found that participants' subjective perception of (online) privacy depends on trust towards the recipient of information and the perception of control over personal information. In the present study, these findings are taken as the basis from which to conceptualize participants' subjective privacy perception. Consequently, perceived privacy is considered as the experience, sense, and evaluation of one's current level of privacy, accompanied by trust towards the information recipient and a perception of control over information. Additionally, we believe that a perception of online privacy includes the perception of how well the information recipient protects personal data.

A realistic perception of online privacy in a given situation should depend on knowledge about the actual level of privacy that is present in that situation (Teutsch et al., 2018). Situational knowledge can either be based on general privacy literacy (e.g., knowledge about how IT processes work) or on being informed about the specific situation (e.g., by reading a website's privacy policy). In the present study, we aim to investigate situational knowledge which is gained by reading the SNS's privacy policy. Following Teutsch et al. (2018), we argue that the more privacy knowledge participants possess, the more accurate their subjective privacy perception will be (i.e., the privacy perception matches the actual privacy level). By varying the actual level of privacy of the SNS, we examine how this association is affected when the SNS is described either as privacy-intrusive or as privacy-friendly:

> Hypothesis 4a (H4a): Higher knowledge about the privacy-intrusive practices will lead to a reduced perception of privacy.

> Hypothesis 4b (H4b): Higher knowledge about the privacy-friendly practices will lead to an increased perception of privacy.

2.3. Privacy Calculus

According to the privacy process model (Dienlin, 2014), people's situational privacy perception directly affects their self-disclosure behavior. In privacy research, however, one approach that has gained a great deal of attention—the privacy calculus (Culnan & Armstrong, 1999; Dinev & Hart, 2006)—assumes that self-disclosure behavior is the result of a cost-benefit analysis. Essentially, according to the privacy calculus, before disclosing information, people weigh privacy costs and disclosure benefits. If users associate higher benefits than costs with information revelation, they are likely to disclose personal data. If the perception of costs outweighs the perception of benefits, self-disclosure is reduced or unlikely. Several studies have found empirical support for the impact of privacy costs and benefits on self-disclosure intentions or technology adoption in a variety of different settings and contexts (e.g., Bol et al., 2018; Dienlin & Metzger, 2016; Krasnova, Kolesnikova, & Guenther, 2009; Princi & Krämer, 2020). These studies examined various kinds of anticipated privacy costs, among them privacy concerns (e.g., Dienlin & Metzger, 2016) or privacy risk beliefs (e.g., Bol et al., 2018). In the present study, participants' assessment of the likelihood of experiencing certain privacy risks will be taken as a measure for privacy costs. This is because reading about a website's privacy practices should primarily impact one's evaluation of how likely certain privacy threats are to occur, and not, for instance, how severe privacy breaches would be.

One point of criticism regarding previous privacy calculus studies is that most did not capture the situational diversity of different disclosure decisions, and instead assessed an accumulated picture of multiple disclosure situations (Masur, 2018). Masur (2018, p. 136) defines a situation as "the entirety of circumstances that affect the behavior of a person at a given time." These circumstances are described as various internal (e.g., goals) and external factors (e.g., walls). Consequently, even visiting the same website at different points in time would result in different situations, since goals or perceptions (or sometimes also external factors like the design of the website) would change. Therefore, the anticipation of privacy costs and disclosure benefits should depend on the given situation or the perception of the circumstances of the situation (e.g., the level of given privacy). This implies that people's subjective experience of the situation's level of privacy should be related to their perception of privacy costs and benefits. In the present study, we assume that participants' assessment of the SNS's privacy level will affect the perception of privacy risk likelihood and the anticipation of benefits of using the SNS. The more one believes a situation to be private, the lower one's assessment of privacy risk likelihood should be. It might also be the case that anticipated benefits are evaluated as even more positive when one perceives a high level of given privacy. However, as we are not aware of any studies that investigated similar issues, these assumptions will be formulated as research questions:

> Research Question 1 (RQ1): Will participants' perception of privacy be negatively related to their perception of privacy risk likelihood?

> Research Question 2 (RQ2): Will participants' perception of privacy be positively related to the anticipated benefits of using the SNS?

Finally, we assume that participants' self-disclosure behavior will be in line with the assumptions of the privacy calculus (Culnan & Armstrong, 1999). To date, the privacy calculus has primarily been investigated in terms of behavioral intentions, and not the actual disclosure behaviors of individuals. A recent study, however, found that persons who had privacy concerns disclosed less information on an online discussion platform, whereas those who perceived disclosure to be beneficial actually disclosed more (Dienlin, Bräunlich, & Trepte, 2019). Hence, we also assume that the privacy calculus notions will hold with respect to actual behavior. This means that participants who perceive benefits from using the SNS should disclose more personal information, whereas those who perceive a high likelihood of experiencing privacy risks should disclose less personal information:

> Hypothesis 5 (H5): The perceived likelihood of privacy risks will be negatively related to the amount of disclosed information.

> Hypothesis 6 (H6): The anticipated benefits of using the SNS will be positively related to the amount of disclosed information.

To provide an overview over the hypothesized relations, we integrated all hypotheses and research questions into one hypothetical model (see Figure 1).

3. Method

3.1. Design and Privacy Policies

The current study comprises a 2 (long vs. short privacy policy) × 2 (privacy-intrusive vs. privacy-friendly SNS) between-subjects design. In accordance with the experimental conditions, four different privacy policies were created. Basically, the short (around 335 words) and the long (around 2000 words) versions provided the same content but differed regarding the level of detail. The short versions summarized the different paragraphs of the long policies with bullet points providing the most important information. In the privacy-intrusive condition, the policies informed about some frequently used privacy practices, for instance, that the SNS automatically collects personal data, disseminates personal data to third parties, uses this data for advertising purposes, and applies user-tracking technologies. In the privacy-friendly condition, participants were told that the SNS mostly refrains from collecting too much personal data, does not disseminate or use this data, and does not apply user-tracking technologies.

3.2. Procedure

Respondents were asked to create a personal account on an SNS which was described as providing users with personalized recommendations for leisure activities in their local area (i.e., events or locations) and to connect with peers. The SNS was introduced as a student network and as being developed by a local start-up company. Before participants created their personal account, one of the four privacy policies was displayed. Participants then had the option—but were not forced or explicitly asked—to read it. To get to the next page, they had to click on a button labeled 'got it.' On the next pages, participants were able to disclose various personal data (see Section 3.4.1) and to choose their preferred privacy setting. After they completed the registration process, they were forwarded to the survey.

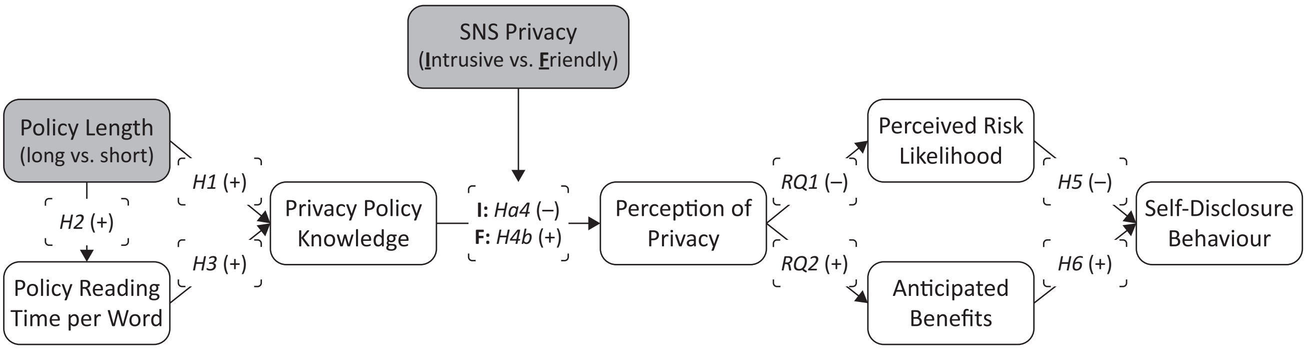

Figure 1. The integrative model including all hypotheses and research questions.

3.3. Sample

In total, 330 persons registered on the SNS and completed the survey. Twenty persons were excluded from the analysis because they answered the questionnaires in an unrealistically fast time (less than two minutes). Another five persons had to be excluded because their account information could not be matched with the respective survey data. Hence, the final sample size consisted of $N = 305$ respondents (213 females, 90 males, 2 did not specify gender) aged 17 to 58 years ($M = 25.68$, $SD = 6.02$). As their highest educational attainment, 43.9% stated having university entrance-level qualifications and 49.05% had a university degree. The majority of participants were students (73.44%), followed by employees (20.33%). The department's ethical committee approved the design of the study. Participants were recruited via Facebook as well as websites for survey sharing (e.g., surveycircle.com) and had the chance to win monetary prizes in a lottery.

3.4. Measures

Below, the measurements are listed in the same order as they appeared in the survey. All items were developed for the purpose of the study. In order to test reliability, confirmatory factor analyses for each construct were performed with SPSS Amos. As can be seen in Table 1, all scales performed well.

3.4.1. Behavioral Data

Different types of behavioral data were assessed while participants interacted with the SNS. First, participants' time spent on the page showing the privacy policy was recorded and taken as a measure for reading time (in seconds). This measure was then divided by the number of words of the respective privacy policy in order to calculate the reading time per word. Self-disclosure behavior was used as dependent variable in the model, which was composed of the number of filled input fields on the SNS. Participants were able to indicate personal information (e.g., name, date of birth, gender), contact information (e.g., e-mail address, telephone number), hobbies, interests (e.g., food and drink, music preferences), information regarding their job or university, as well as religious and political views. Subsequently, respondents had the opportunity to introduce themselves to the other users of the network by writing a short text about themselves. A category that was filled with information was coded as 1 and a blank category was coded as 0. As respondents were able to leave all fields blank, the self-disclosure score ranged from 0–32. Finally, participants were asked to choose their preferred privacy setting (i.e., who can see one's information). The options were: 'only me,' 'only selected friends,' 'my friends,' 'my friends and their friends,' and 'all users.' The score was reverse-coded (1 = 'all users' and 5 = 'only me'). The privacy settings were not part of the model but appear in correlation analyses.

3.4.2. Anticipated Benefits

Participants' perception of the SNS's benefits was assessed using seven items rated on a 7-point Likert scale (ranging from 1 = 'I do not agree at all' to 7 = 'I fully agree'). Items were based on the description of the SNS and consisted of a first part ('I would find it advantageous…') and a varying second part (e.g., '…if the SNS supported me in my leisure planning' or '…to experience new and interesting things using the SNS').

3.4.3. Perceived Privacy

Following Teutsch et al. (2018), eight items were created to capture participants' evaluation of the situation's privacy level using a 7-point Likert scale (ranging from 1 = 'I do not agree at all' to 7 = 'I fully agree'). The scale consisted of items that assessed perceived control over information (e.g., 'The SNS leaves control over my personal data to me'), trust towards the SNS (e.g., 'The SNS is always honest with me about how my personal information is used'), as well as a general perception of privacy (e.g., 'The SNS is a private space') and privacy protection (e.g., 'The SNS protects my data appropriately').

3.4.4. Privacy Policy Knowledge

Participants' knowledge of the SNS's privacy practices that were described in the privacy policies was assessed by nine true/false questions derived from the presented privacy policies. Besides the options 'true' and 'false,' participants were able to state 'I don't know' in order to avoid forcing them to choose an option, which might have led to biased results. A correct answer was coded as 1 and a false answer was coded as 0. 'I don't know' was also coded as 0. Consequently, the score ranged from 0 (only false/no answers) to 9 (only correct answers).

Table 1. Results of the confirmatory factor analyses with fit indices. Internal consistency (Cronbach's α, composite reliability (MacDonald's Ω), and average variance extracted) of the assessed constructs.

	χ^2 (df)	p	CFI	TLI	RMSEA	SRMR	α	Ω	AVE
Anticipated Benefits	33.99 (13)	.001	.99	.98	.07	.02	.93	.93	.66
Perceived Risk Likelihood	1.08 (2)	.582	1.00	1.00	$< .01$	.01	.83	.83	.54
Perceived Privacy	39.82 (19)	.003	.99	.98	.06	.02	.93	.93	.62

3.4.5. Perceived Likelihood of Privacy Risks

Participants assessed the likelihood of negative consequences of using the SNS with a slide bar ranging from 0% to 100%. The seven items were based on the content of the privacy policies and consisted of a first part ('How likely do you think it is…') and a varying second part (e.g., '…that the SNS passes on your personal data to third parties' or '… of being exposed to privacy risks by using the SNS'). Three items were deleted within the confirmatory factor analyses.

4. Results

Data were analyzed with IBM SPSS Statistics 25 and IBM SPSS Amos 25. Table 2 shows descriptive statistics, and Table 3 displays bivariate correlations between the variables.

4.1. Structural Equation Model

The hypotheses and research questions were tested within one structural equation model (SEM) with observed variables and maximum likelihood estimation. Model fit was evaluated in accordance with frequently used fit indices (Browne & Cudeck, 1993; Hu & Bentler, 1999). The model test revealed a good fit: χ^2 (13) = 16.48, p = .224, χ^2/df = 1.27, CFI = .98, TLI = .96, RMSEA = .03 (90% CI: .00, .07), SRMR = .04. The model is shown in Figure 2. H1 expected that participants who read the short privacy policies would have increased knowledge about the SNS's privacy practices compared to participants who read the long versions. Contrary to this assumption, there was no relationship between policy length (coded as 1 = 'long' and 2 = 'short') and policy knowledge (β = .00, p = .997). In H2, we assumed that participants would have a higher reading time per word when confronted with a short privacy policy. This hypothesis was supported, as we found a positive relationship between the two variables (β = .30, $p < .001$). The analysis of H3 found support for the assumption that a higher reading time per word positively contributes to knowledge about the SNS's privacy practices (β = .31, $p < .001$). H4 expected a negative relation between policy knowledge and perceived privacy in the privacy-intrusive condition (H4a), and a positive relation in the privacy-friendly condition (H4b). We used a multigroup analysis to examine whether the relationship behaves equivalently in different subsamples (Kline, 2016). As the model fit of the unconstrained model was not acceptable, an additional path between privacy policy knowledge and risk likelihood had to be drawn based on the modification indices. The adjusted model showed a good data fit: χ^2 (24) = 24.38, p = .440, χ^2/df = 1.02, CFI = 1.00,

Table 2. Descriptive statistics of the assessed constructs and behavioral data.

		Range	
	M (*SD*)	Actual	Potential
Perceived Benefits	4.91 (1.41)	1–7	1–7
Perceived Risk Likelihood	6.06 (2.02)	1–11	1–11
Perceived Privacy	4.03 (1.27)	1–7	1–7
Privacy Policy Knowledge	2.96 (2.34)	0–8	0–9
Policy Reading Time (seconds)	33.32 (68.13)	1–532	∞
Reading Time per Word	0.05 (0.08)	.00–.63	∞
Self-Disclosure (filled fields)	14.93 (6.28)	0–24	0–32
Privacy Setting	3.62 (1.52)	1–5	1–5

Notes: Risk likelihood was assessed with a percentage scale, meaning that a value of 1 equals 0%, 6 equals 50% and 11 equals 100%. Privacy setting was reverse-coded with 1 = 'public' and 5 = 'private.'

Table 3. Bivariate correlations between all assessed constructs and behavioral data.

	1	2	3	4	5	6	7	8
1 Perceived Benefits	—							
2 Perceived Risk Likelihood	−.12 *	—						
3 Perceived Privacy	.24 ***	−.45 ***	—					
Privacy Policy Knowledge								
4 Privacy-Intrusive Website (*n* = 148)	.02	.39 ***	−.29 ***	—				
5 Privacy-Friendly Website (*n* = 157)	.01	−.33 ***	.41 ***	—	—			
6 Policy Reading Time (seconds)	.00	−.12 *	.11	.26 ***	.32 ***	—		
7 Reading Time per Word	.06	−.06	.05	.28 ***	.37 ***	.62 ***	—	
8 Self-Disclosure (answered fields)	.18 **	−.07	.03	.02	.04	.04	−.03	—
9 Privacy Setting	−.16 **	.05	.02	−.20 *	−.01	−.09	−.10	−.25 ***

Note: * $p < .05$, ** $p < .01$, *** $p < .001$.

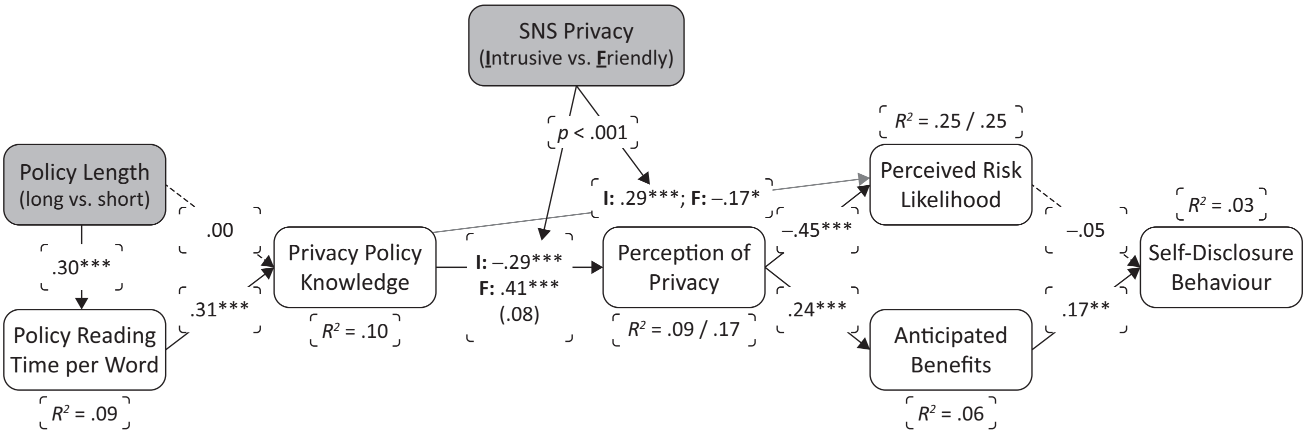

Figure 2. SEM with observed variables. Notes: The gray line was added in the multigroup analysis based on modification indices. Numbers display standardized regression coefficients (β). When two R^2 values are displayed, these are part of the multigroup analyses (privacy-intrusive condition first, privacy-friendly condition second). Numbers in brackets shows the effect size without group effects. Dashed lines indicate non-significant paths. *$p < .05$, **$p < .01$, ***$p < .001$.

TLI = 1.00, RMSEA = .01 (90% CI: .00, .05), SRMR = .06. The multigroup analysis revealed that the paths differed significantly between the two conditions ($\Delta(\chi^2) = 58.61$, $\Delta(p) < .001$).

In accordance with H4, the multigroup analysis revealed that higher knowledge about the privacy practices in the privacy-intrusive condition led to a decreased perception of privacy ($\beta = -.29$, $p < .001$), whereas higher knowledge in the privacy-friendly condition positively affected privacy perception ($\beta = .41$, $p < .001$). The subsequently added path between knowledge and perceived risk likelihood revealed a positive relation in the privacy-intrusive condition ($\beta = .29$, $p < .001$), and a negative relation in the privacy-friendly condition ($\beta = -.17$, $p = .026$). This finding implies that knowledge about the content of privacy policies can lead to a more accurate assessment of the likelihood of privacy risks. Moving onward to the research questions, testing RQ1 revealed that participants' evaluation of the current degree of privacy was negatively related to their assessment of privacy risk likelihood ($\beta = -.45$, $p < .001$). Concerning RQ2, there was a positive relation between privacy perception and the anticipation of self-disclosure benefits ($\beta = .24$, $p < .001$). Thus, the results are in line with the assumptions of both research questions. No support was found for H5, since the perceived likelihood of privacy risks did not show a significant negative relation to the amount of information disclosed on the SNS ($\beta = -.05$, $p = .374$). Finally, the perception of benefits was significantly positively related to the amount of disclosed data, thus supporting H6 ($\beta = .17$, $p = .003$).

4.2. Additional Analysis

To shed more light on the finding that the reading time per word was higher in the short policy condition, we conducted a MANOVA with total reading time and with reading time per word. The results ($F(1, 303) = 7.62$, $p = .006$, $\eta^2 = .025$) showed that the actual reading time was significantly higher in the long policy condition ($M = 44.01$, $SD = 90.01$) compared to the short policy condition ($M = 22.71$, $SD = 30.83$). For reading time per word, the results of the MANOVA ($F(1, 303) = 30.20$, $p < .001$, $\eta^2 = .091$) revealed a lower value in the long condition ($M = .02$, $SD = .05$) in comparison to the short condition ($M = .07$, $SD = .09$). Hence, although the average reading time in the long condition was about twice as high as in the short condition, the reading time per word was more than three times higher in the short condition compared to the long condition. This emphasizes that the short text was more successful in delivering knowledge than the long text, due to the fact that a more effective information extraction was possible.

5. Discussion and Conclusion

The current study pursued two major aims. The first aim was to investigate whether shorter privacy policies can be more beneficial to inform SNS users about potential privacy costs compared to long versions. The second aim was to test assumptions regarding users' privacy decisions stemming from two approaches (i.e., the privacy process model and the privacy calculus) within one integrative model. The results provide insights into the relevance of privacy policy design for individual privacy information acquisition, the importance of knowledge about actual privacy levels, and situational factors underlying self-disclosure. In terms of practical implications, policy makers and politicians may consider our findings for the design of privacy policies and the development of guidelines for such policies.

5.1. Privacy Policy Length

The first three hypotheses focused on whether shorter privacy policies would be more beneficial in informing users about a website's privacy practices than longer versions, and whether participants would have to expend less effort on reading the short versions. Since survey data (e.g., European Commission, 2019) revealed that few users read privacy policies, we argued that for most people, reading privacy policies is associated with (cognitive) effort. Hence, people might be more motivated to read condensed versions due to the lower anticipated cognitive and time effort (cf. Lang, 2017). In the present study, participants were given the option of whether to read the privacy policy of the SNS on which they would subsequently create an account. Although the results did not reveal a direct effect of policy length on knowledge about the content of the policy, we nevertheless found that short privacy policies can indeed be more advantageous than long ones: First, participants who saw a short policy had a higher reading time per word, meaning that they chose to spend more time on understanding the given text. Second, the reading time per word was then positively related to knowledge about the policy's content. This demonstrates that shorter privacy policies indirectly contribute to higher knowledge about their contents compared to the normally applied long versions. However, this effect only exists among persons who actually expend some effort on reading the policies. The effort to extract information from the text, however, was found to be significantly reduced for the short privacy policy, because participants were able to read the text more carefully and understand the text in less time compared to participants who saw the long policy. According to the assumptions of Lang (2017), these findings indicate that people were more willing to engage in reading the shorter policy. Taken together, the results demonstrate that participants were able to absorb more information from the shorter policies and probably had a higher motivation to do so. The GDPR prescribes that policies should be written in comprehensible language to enhance transparency. However, policies of immense length oppose the goal of informing users. Hence, the present findings could be used by politicians to obligate companies to truly inform users by providing short, comprehensible privacy policies instead of allowing companies to provide long and complicated policies which primarily serve the purpose of avoiding lawsuits. While it might be argued that shortening texts brings about a loss of information, we believe that Internet users do not need to be provided with the abundance of information that is written in standard privacy policies at the time when they normally have to give their consent to data processing. Our study findings show that for individuals who wish to register on websites, the provision of less information would be beneficial for informing them about the main privacy practices. For those who wish for more detailed information, the long policies could still be available in addition to the short ones. Nonetheless, the present findings also revealed that shortening privacy policies is not a panacea in itself; the responsibility to inform oneself and protect one's privacy still lies with the user. However, users seem to be more motivated to engage in information-gathering when the privacy policy is short. It must be noted that participants' knowledge of the policies' content was rather low. Thus, providing short informative privacy policies might be a first step toward greater privacy policy knowledge and informed privacy decisions of social media users. However, there is still a great need for research on how to create more transparency to inform users and how to automatically protect users' privacy (e.g., using privacy-by-design approaches or real-time support provided by software). It is becoming increasingly apparent that users might benefit from support in their privacy decisions, given that they are not always able to balance their needs for self-disclosure and privacy protection on their own (Krämer & Schäwel, 2020).

5.2. Privacy Decision-Making

With H4 to H6 and RQ1 and RQ2, we sought to examine how different constructs relevant for online privacy decisions are related. The integrative model was based on parts of the privacy process model (Dienlin, 2014), which assumes that individuals form a privacy perception in any situation, and the privacy calculus (Culnan & Armstrong, 1999), which states that self-disclosure decisions are the result of a cost-benefit analysis. We argued that the subjective perception of the situation's privacy should be based on knowledge about the privacy policy's content (H4). The results supported the assumptions that more knowledge led to a lower perception of privacy in the privacy-intrusive condition and to a higher perception of privacy in the privacy-friendly condition. This finding demonstrates that factual knowledge about the degree of privacy in a situation can advantageously contribute to one's feeling of privacy by resolving potential mismatches between the objective situation and the subjective perception (cf. Trepte & Reinecke, 2011), supporting previous assumptions (Dienlin, 2014; Teutsch et al., 2018). In turn, people who lack knowledge may more easily misperceive actual privacy levels and become victims of privacy breaches, as they might share inappropriate (amounts of) data due to a false perception of situational privacy. Previous research has found that general privacy knowledge (i.e., privacy literacy) can positively contribute to more protective privacy behaviors (e.g., Bartsch & Dienlin, 2016). Together with the results of the present study, it seems that both general knowledge and situational knowledge are important for online privacy perception and behavior. Future studies could also pursue the questions of whether privacy literacy affects the situational feeling of privacy, or how general and situational knowledge are related. It must be noted that the amount of explained variance in privacy perception was rather low in the current study, indicating that situational knowledge is only one of several factors that influence the evaluation of online privacy levels. Without appropriate knowledge, people might rely on heuristics (e.g., triggered by the design of a website) or general feelings or beliefs (e.g., thinking that online privacy is always low or high). Besides our hypotheses, the analysis revealed a direct effect of policy knowledge on the assessment of privacy risk likelihood. In the privacy-intrusive condition, the perceived risk likelihood increased with higher knowledge, whereas in the privacy-friendly condition, knowledge reduced the perceived risk likelihood. Although not part of our hypotheses, it is plausible that people with higher knowledge about a website's privacy practices are better able to estimate the likelihood of potential negative consequences of website usage.

Next, we investigated whether the situational perception of privacy affects the perceived likelihood of privacy risks (RQ1) and the anticipation of benefits of using the SNS (RQ2). The results revealed that the perception of online privacy was indeed related to both risk likelihood appraisal and benefit perception. The more private the situation was perceived to be, the lower respondents assessed the likelihood of negative consequences to be, and the higher they rated the benefits of using the SNS. These results support the assumptions of Masur (2018), who argued that the assessment of privacy costs and disclosure benefits differs for each situation. The present findings show that the perception of privacy risk likelihood and disclosure benefits can vary based on the evaluation of given privacy levels, implying that the weighing of costs and benefits is not stable but rather varies across different situations. While the negative relation between participants' perception of privacy and their assessment of privacy costs is more intuitive (private situations should by definition entail a reduced likelihood of privacy risks), the positive link between privacy perception and benefit perception is an interesting finding. It seems that participants appreciated the privacy-preserving SNS, which led to an increased perception of benefits. Hence, websites that respect user privacy could have an advantage over websites that do not, because people might turn towards the privacy-preserving ones. However, this interpretation is only speculative, and no causal implications can be drawn. Therefore, future studies might consider the role of Internet users' perception of present privacy levels and the antecedents and outcomes thereof.

Finally, hypotheses H5 and H6 focused on the privacy calculus, assuming that participants would disclose less information if they considered privacy risks as likely to happen and would disclose more information if they perceived disclosure to be beneficial. However, only the perception of benefits was significantly positively associated with the amount of disclosed data. Participants who thought that privacy risks were likely did not disclose significantly less personal information. These results are contrary to the basic assumption of the privacy calculus and contradict the findings of a recent study that also collected behavioral data (Dienlin et al., 2019). Although plenty of studies have found support for the basic assumption of the privacy calculus (e.g., Bol et al., 2018; Dienlin & Metzger, 2016; Krasnova et al., 2009; Princi & Krämer, 2020), the approach is not without criticism (Knijnenburg et al., 2017). The vast majority of privacy calculus studies focused on intentions rather than on behavioral data (with the exception of the study by Dienlin et al., 2019). Hence, it may be that the privacy calculus holds in hypothetical decisions but not in concrete disclosure situations. However, we propose some alternative explanations. First, even the positive effect of benefit perception on self-disclosure was comparatively small and the proportion of explained variance in self-disclosure was very low. This implies that the disclosure decision was primarily based on factors other than the perception of benefits, possibly because participants were aware of the artificial experimental situation. This might also be the reason why privacy risk perception did not have any effect on participants' self-disclosure behavior. Second, we did not collect survey data of those persons who decided not to register on the SNS. Thus, it might be the case that the persons who registered were primarily those for whom privacy risks are less important. Third, we are unable to make any statements about whether participants actually weighed risks and benefits, although this is the basic assumption of the privacy calculus. It may be that many participants balanced costs against benefits but came to the conclusion that the benefits were worth the risks (cf. Trepte et al., 2015). Hence, future studies should collect behavioral data on the privacy calculus and investigate different privacy situations in order to better understand the dynamics underlying privacy decision-making.

5.3. Limitations

Some limitations of the present study should be mentioned. For most paths in the model, it is not possible to make causal statements. Moreover, participants did not freely decide to register on the SNS, but were told to do so as part of the study. This created an artificial situation and might have distorted some behavioral data on the SNS. A further limitation pertains to the sample, which mainly consisted of females, students and highly educated persons, and is thus not representative of the general population. Moreover, the items concerning privacy risk likelihood and SNS benefits contained only a limited number of potential negative and positive consequences. It is conceivable that participants anticipated further risks or benefits of using the SNS that were not captured. Since only those who registered for the SNS were also able to participate in the study, future studies should also allow participants to not disclose personal data while still capturing their response behavior. This method could prevent distorted samples and uncover interesting findings. In addition to this point, a further limitation concerns the recruitment, which partially occurred via Facebook and may thus also have distorted the sample. Another issue concerns the measurement of self-disclosure: Some participants disclosed more detailed information than others (e.g., exact date of birth vs. year of birth) and some disclosed false information (real name vs. nickname). However, we did not consider these differences in the analysis but used a simplified self-disclosure score focusing on the amount of disclosure. This approach, however, might be an oversimplification of behavior which might have distorted results in some respects. Finally, with respect to the external validity of the study, since participants disclosed data in one specific SNS, it is unclear whether the same relationships would be found in different situations.

5.4. Conclusions

The present study contributes to our understanding of online privacy in two ways: First, the findings indicate that shorter privacy policies can increase users' reading accuracy (while reading time and probably cognitive effort are decreased) and knowledge. This implies that people might be more willing to read shorter privacy policies about a website's potential privacy costs, which in turn enhances their knowledge. Whereas the GDPR prescribes that policies must be written in an understandable language style, legislators could also think about prescribing shorter versions of privacy policies (possibly in addition to the traditional long ones) since this can support users in terms of information acquisition. Second, an integrative model was tested that was composed of parts of two different approaches and contained factors relevant for online privacy decision-making. Several interesting findings emerged. Factual knowledge about the content of the privacy policies seems to be an important factor for the evaluation of one's current online privacy level as well as the assessment of privacy risk likelihood. The more participants knew about actual levels of privacy, the more realistic their feeling of privacy was. The subjective perception of privacy led to different perceptions of privacy costs and self-disclosure benefits. This suggests that situational perceptions can impact and distort the weights of anticipated negative and positive consequences of disclosure. Finally, participants disclosed more personal information when they perceived higher benefits of using the SNS. Given the importance of factual privacy knowledge, policy makers should seek ways to increase Internet users' situational privacy knowledge, as this is related to other factors underlying privacy decisions. According to the findings of the present study, shortened privacy policies represent one such way to better inform website users about situational privacy issues.

Acknowledgments

This work has been funded by the Federal Ministry for Education and Research of Germany (No. 16KIS0743). We acknowledge support by the Open Access Publication Fund of the University of Duisburg-Essen.

Conflict of Interests

The authors declare no conflict of interests.

References

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

Bartsch, M., & Dienlin, T. (2016). Control your Facebook: An analysis of online privacy literacy. *Computers in Human Behavior*, *56*, 147–154. https://doi.org/10.1016/j.chb.2015.11.022

Bol, N., Dienlin, T., Kruikemeier, S., Sax, M., Boerman, S. C., Strycharz, J., . . . de Vreese, C. H. (2018). Understanding the effects of personalization as a privacy calculus: Analyzing self-disclosure across health, news, and commerce contexts. *Journal of Computer-Mediated Communication*, *23*(6), 370–388. https://doi.org/10.1093/jcmc/zmy020

Browne, M. W., & Cudeck, R. (1993). Alternative ways of assessing model fit. *Sociological Methods & Research*, *21*(2), 136–136. https://doi.org/10.1177%2F0049124192021002005

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

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

Dienlin, T., Bräunlich, K., & Trepte, S. (2019). *How do like and dislike buttons affect communication? A privacy calculus approach to understanding self-disclosure online in a one-week field experiment*. Paper presented at the 69th Annual Conference of the ICA, Washington, DC, USA.

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.

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

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, *17*(1), 61–80. https://doi.org/10.1287/isre.1060.0080

European Commission. (2019). *Special Eurobarometer 487a: The general data protection regulation*. Brussels: European Commission. Retrieved from https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/86886

Hu, L. T., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation*

Modeling: A Multidisciplinary Journal, *6*(1), 1–55. https://doi.org/10.1080/10705519909540118

Kline, R. B. (2016). *Principles and practice of structural equation modeling* (4th ed.). New York, NY: The Guilford Press.

Knijnenburg, B., Raybourn, E., Cherry, D., Wilkinson, D., Sivakumar, S., & Sloan, H. (2017). Death to the privacy calculus? *SSRN Electronic Journal*. Retrieved from https://doi.org/10.2139/ssrn.2923806

Krämer, N. C., & Schäwel, J. (2020). Mastering the challenge of balancing self-disclosure and privacy in social media. *Current Opinion in Psychology*, *31*, 67–71. https://doi.org/10.1016/j.copsyc.2019.08.003

Krasnova, H., Kolesnikova, E., & Guenther, O. (2009). "It won't happen to me!": Self-disclosure in online social networks. In *Proceedings of the 15th Americas Conference on Information Systems* (pp. 1–9). Atlanta, GA: AIS/ICIS. Retrieved from http://aisel.aisnet.org/amcis2009/343

Lang, A. (2000). The limited capacity model of mediated message processing. *Journal of Communication*, *50*(1), 46–70. https://doi.org/10.1111/j.1460-2466.2000.tb02833.x

Lang, A. (2017). Limited capacity model of motivated mediated message processing (LC4MP). In P. Rössler, C. A. Hoffner, & L. van Zoonen (Eds.), *The international encyclopedia of media effects* (pp. 1–9). Hoboken, NJ: John Wiley & Sons. https://doi.org/10.1002/9781118783764.wbieme0077

Masur, P. K. (2018). *Situational privacy and self-disclosure: Communication processes in online environments*. Cham: Springer. https://doi.org/10.1007/978-3-319-78884-5

Princi, E., & Krämer, N. (2020). I spy with my little sensor eye: Effect of data-tracking and convenience on the intention to use smart technology. In *Proceedings of the 53rd Hawaii International Conference on System Sciences* (pp. 1391–1400). Maui, HI: University of Hawaii, Manoa. https://doi.org/10.24251/HICSS.2020.171

Teutsch, D., Masur, P. K., & Trepte, S. (2018). Privacy in mediated and nonmediated interpersonal communication: How subjective concepts and situational perceptions influence behaviors. *Social Media + Society*, *4*(2), 2056305118767134. https://doi.org/10.1177%2F2056305118767134

Trepte, S., & Reinecke, L. (2011). The social web as a shelter for privacy and authentic living. In S. Trepte & L. Reinecke (Eds.), *Privacy online* (pp. 47–60). Heidelberg: Springer.

Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., & Lind, F. (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: Springer. http://dx.doi.org/10.1007/978-94-017-9385-8

Vitak, J. (2012). The impact of context collapse and privacy on social network site disclosures. *Journal of Broadcasting & Electronic Media*, *56*(4), 451–470. https://doi.org/10.1080/08838151.2012.732140

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

About the Authors

Yannic Meier is a PhD Candidate and Research Associate in the Team Social Psychology: Media and Communication at the University of Duisburg-Essen, Germany. He is a Member of the research project 'Forum Privacy' that works on an interdisciplinary understanding of the role of privacy. In his dissertation, he studies mechanisms of online privacy decision-making and supportive means for online privacy protection. His research interests include online privacy, online self-disclosure, and entertainment research.

Johanna Schäwel is a Postdoctoral Researcher in the field of media psychology and communication at the University of Hohenheim in Germany. She finished her PhD in 2018 at the University of Duisburg-Essen, Germany, in the field of social psychology and media psychology. In her dissertation, she focused on online privacy protection and psychological factors that influence the acceptance of technical privacy support. Her research focuses on online privacy, self-disclosure and self-presentation on social networking sites, and persuasive processes of communication.

Nicole C. Krämer is Full Professor of Social Psychology, Media and Communication at the University of Duisburg-Essen, Germany. She completed her PhD in Psychology at the University of Cologne, Germany, in 2001, and received the *venia legendi* for psychology in 2006. Dr. Krämer's research focuses on social psychological aspects of human-machine-interaction (social effects of robots and virtual agents) and computer-mediated-communication. She investigates processes of information selection, opinion building, and relationship maintenance of people communicating via Internet, especially via social media.