SCM
Studies in Communication and Media

FULL PAPER

Between protection and disclosure: applying the privacy calculus to investigate the intended use of privacy-protecting tools and self-disclosure on different websites

Zwischen Schutz und Preisgabe: die Anwendung des Privacy Calculus zur Untersuchung der beabsichtigten Nutzung von privatheitsschützenden Tools und der Datenpreisgabe auf verschiedenen Websites

Yannic Meier, Johanna Schäwel & Nicole C. Krämer

Yannic Meier (Dr.), University of Duisburg-Essen, Social Psychology: Media and Communication, Forsthausweg 2, 47057 Duisburg, Germany. Contact: yannic.meier(at)uni-due.de. ORCID: https://orcid.org/0000-0002-5726-3229

Johanna Schäwel (Dr.), University of Hohenheim, Department of Media Psychology, (540 F), 70593 Stuttgart, Germany. Contact: johanna.schaewel(at)uni-hohenheim.de. ORCID: https://orcid.org/0000-0002-2038-2443

Nicole C. Krämer (Prof. Dr.), University of Duisburg-Essen, Social Psychology: Media and Communication, Forsthausweg 2, 47057 Duisburg, Germany. nicole.kraemer(at)uni-due.de. ORCID: https://orcid.org/0000-0001-7535-870X

FULL PAPER

Between protection and disclosure: applying the privacy calculus to investigate the intended use of privacy-protecting tools and self-disclosure on different websites

Zwischen Schutz und Preisgabe: die Anwendung des Privacy Calculus zur Untersuchung der beabsichtigten Nutzung von privatheitsschützenden Tools und der Datenpreisgabe auf verschiedenen Websites

Yannic Meier, Johanna Schäwel & Nicole C. Krämer

Abstract: Using privacy-protecting tools and reducing self-disclosure can decrease the likelihood of experiencing privacy violations. Whereas previous studies found people's online self-disclosure being the result of privacy risk and benefit perceptions, the present study extended this so-called privacy calculus approach by additionally focusing on privacy protection by means of a tool. Furthermore, it is important to understand contextual differences in privacy behaviors as well as characteristics of privacy-protecting tools that may affect usage intention. Results of an online experiment (N = 511) supported the basic notion of the privacy calculus and revealed that perceived privacy risks were strongly related to participants' desired privacy protection which, in turn, was positively related to the willingness to use a privacy-protecting tool. Self-disclosure was found to be context dependent, whereas privacy protection was not. Moreover, participants would rather forgo using a tool that records their data, although this was described to enhance privacy protection.

Keywords: Privacy Calculus, Desire for Privacy Protection, Privacy-Protecting Tool, Privacy Contexts, Online Self-Disclosure

Zusammenfassung: Die Verwendung von privatheitsschützenden Tools und die Verringerung der Selbstoffenbarung können die Wahrscheinlichkeit des Auftretens von Privatheitsverletzungen verringern. Während bisherige Studien herausfanden, dass die Online-Selbstoffenbarung das Ergebnis der Wahrnehmung von Privatheitsrisiken und Gratifikationen ist, erweitert die vorliegende Studie diesen sogenannten Privacy Calculus-Ansatz, indem sie zusätzlich den Schutz der Privatsphäre durch ein Tool in den Mittelpunkt stellt. Darüber hinaus ist es wichtig, kontextuelle Unterschiede im Privatsphäre-Verhalten sowie Charakteristika von Privatsphäre-schützenden Tools zu verstehen, die die Nutzungsabsicht beeinflussen können. Die Ergebnisse eines Online-Experiments (N = 511) unterstützten den Grundgedanken des Privacy Calculus und zeigten, dass wahrgenommene Risiken für die Privatsphäre stark mit dem gewünschten Schutz der Privatsphäre der Teilnehmer:innen zusammenhingen, was wiederum positiv mit der Bereitschaft der Nutzung eines privatheitsschützenden Tools verbunden war. Es zeigte sich, dass die Selbstoffenbarung kontextabhängig war, während der Schutz der Privatsphäre nicht kontextuell geprägt war. Da-

rüber hinaus würden die Teilnehmer:innen eher darauf verzichten, ein Tool zu verwenden, das ihre Daten erfasst, obwohl dies eine Verbesserung des Schutzes der Privatsphäre hervorgebracht hätte.

Schlagwörter: Privacy Calculus, Wunsch nach Privatheitsschutz, Privatheitsschützendes Tool, Privatheitskontexte, Online Informationspreisgabe

1. Introduction

The application of privacy-protective strategies has become an issue of high importance in a digitalized world in which many Internet companies make great efforts to access the maximal amount of Internet users' personal data. Individuals' personal information has become a currency people have to trade off in exchange for the ability to use certain web-services (Papacharissi, 2010). Once collected, personal information may be used for purposes other than those initially agreed upon and may be disseminated to third parties which can lead to privacy invasions and harm users' self-determination (Solove, 2008). A prominent example is the usage of private data to target people with personalized commercial or political advertisements posing not only individual but also societal threats (Zuiderveen Borgesius et al., 2018). Although online privacy risks cannot be completely avoided today, users can at least reduce the hazards to a possible minimum. Researchers argue that it is crucial to support Internet users in their privacy protection efforts, for instance, by technical means such as privacy tools (Krämer & Schäwel, 2020). Such tools can inform users about potential privacy risks in order to enable them to make more privacy-aware choices (e.g., *Lightbeam;* Mozilla, 2019), automatically provide privacy protection, for instance, by blocking user-tracking mechanisms (e.g., *TrackMeOrNot;* Meng et al., 2016), or they can do both simultaneously (e.g., *Ghostery*). The current study takes a closer look on participants' intention to use a privacy-protecting tool applying an extended privacy calculus framework. The privacy calculus originally focused on information revelation but also seems to be applicable for privacy protective behaviors (cf. Dienlin & Metzger, 2016). It assumes that peoples' self-disclosure decisions are driven by the perception of privacy risks and disclosure benefits (e.g., Culnan & Armstrong, 1999). Since people engage in privacy regulative behaviors when they sense to have less privacy than they desire (Dienlin, 2014), we argue that Internet users who perceive high online privacy risks experience a lack of privacy, and, as a consequence, have a high desire for privacy protection. This desired privacy protection should be related to privacy regulation in form of the willingness to apply a privacy-protective tool. Finally, it will be examined whether self-disclosure, the desire for protection, and the intention to protect oneself by using a tool will be different among three kinds of websites (i.e., contexts) and whether different features of tools affect usage intentions. All hypotheses and research questions are investigated within one integrative model.

2. Literature review

The literature review is structured as follows. After a general description of privacy-protective behaviors, the privacy calculus framework is introduced and extended by trust and perceived control. Subsequently, Internet users' desire for privacy protection is going to be derived from the literature. Finally, the advantages of a contextual perspective on self-disclosure and privacy protection as well as potential effects of the characteristics of a privacy-protecting tool are outlined.

2.1 Online privacy protection

Online, privacy risks can arise when someone either actively shares private information to other parties (e.g., companies or other users) or when another party automatically collects personal information (e.g., visited websites or search queries) about someone (Bujlow et al., 2017). However, Internet users can engage in various strategies to decrease potential privacy threats such as disclosing false information about oneself, deleting cookies and browser history, or using protective software (Boerman et al., 2018). Generally, privacy-protective behaviors can be divided into passive and active forms (Matzner et al., 2016). Passive forms of privacy protection refer to the decision to disclose or not disclose personal data, whereas active forms refer to the decision to use software or to request the deletion of one's personal data. The current study focuses on self-disclosure and the willingness to use a privacy-protecting tool to investigate both passive as well as active privacy protection strategies. Empirical findings indicate that users engage in both passive and active forms of data protection, however, especially the usage of protective software and browser tools is rather modest (Boerman et al., 2018; Matzner et al., 2016). Hence, the question arises which factors particularly affect Internet users' willingness to use privacy-protective tools. The current study pursues the questions whether people who desire more privacy online are willing to protect themselves both passively (i.e., decreased self-disclosure) and actively (i.e., adopt a privacy-protecting tool) and what factors are related to an increased or decreased desire for privacy protection. The assumptions are derived from an extended privacy calculus framework that will be presented in the following.

2.2 The privacy calculus

Many studies that focus on online self-disclosure (i.e., the revelation of personal information to websites, companies, or other persons) apply the *privacy calculus* approach. Originating from the calculus of behavior (Laufer & Wolfe, 1977), the privacy calculus assumes that people weigh costs and benefits of disclosure before deciding to reveal personal information (Culnan & Armstrong, 1999; Dinev & Hart, 2006). Consequently, a person is more likely to disclose information when they perceive greater benefits than costs of disclosure and they less likely disclose information when higher costs than advantages are associated with disclosure. The costs associated with information revelation can, for example, be the perception of privacy risks (Bol et al., 2018). Benefit perceptions comprise social incen-

tives, such as social support or positive feedback, but also convenience or enjoyment (Krasnova et al., 2010). Several studies empirically showed that Internet users' privacy risk and benefit perceptions impact their intention to disclose personal information in various online contexts such as on social networking sites (Dienlin & Metzger, 2016; Meier, Schäwel, Kyewski, & Krämer, 2020), health contexts (Dinev et al., 2016) or e-commerce contexts (Culnan & Armstrong, 1999; Dinev & Hart, 2006).

However, self-disclosure decisions do not only depend on risk and benefit perceptions but are also affected by other factors like trust in the receiver of information and the perception of control over one's data (Culnan & Armstrong, 1999; Dinev & Hart, 2006). In recent research, trust and perceived control are also considered when it comes to conceptualize the situational perception of online privacy (Meier, Schäwel, & Krämer, 2020; Teutsch et al., 2018). Hence, in the current study, the privacy calculus framework is expanded by trust and a control perception. These variables are described in the following section.

2.3 Trust and perceived control

The concepts of trust and control are rooted in (research of) interpersonal relationships. Trust has been described as the degree of uncertainty about possible control one can exert in a relationship (Heath & Bryant, 2013). In this respect, trust and control have a complementary character. Consequently, trust is the expectation that the conduct of another party will not be harmful (Bhattacharya et al., 1998) without having the chance to actually control the other party's conduct. In the area of online privacy, trust towards the receiver of information (e.g., a website or other person) has been found to be positively related to self-disclosure (e.g., Metzger, 2006) and to the general perception of online privacy (Teutsch et al., 2018). This implies that people are willing to disclose personal information to another party when they do not expect any harmful actions from that party. In the current study, trust is operationalized as the expectation that a website is transparent regarding the usage of personal information and that personal information is kept confidentially. Besides trust, a sense of control is important for the perception of online privacy (Teutsch et al., 2018). Whereas people have actual control possibilities in interpersonal relations (Heath & Bryant, 2013), these possibilities are usually very limited among online self-disclosure. Still, people can have the impression of being able to control their own data. In general, the perception of control is associated with a reduced risk perception (Weinstein, 1984). Krasnova and colleagues (2010) confirmed this assumption by showing that a control perception had a negative effect on perceived privacy risks resulting in an increased self-disclosure intention. Moreover, a direct link between perceived control and self-disclosure was found: individuals who perceived control over the dissemination of revealed information, disclosed more personal data than persons who did not have that perception of control (Brandimarte et al., 2012).

The presented previous empirical evidence on the privacy calculus, trust, and perceived control shows that these variables play a significant role for people's

self-disclosure intention and will be integrated into one model in the present study. Hence, the following hypotheses are derived:

Hypothesis 1 (H1): Perceived privacy risks will be negatively related to the intention to disclose personal information.

Hypothesis 2 (H2): (a) Trust towards the website, (b) perceived control over information as well as (c) perceived benefits of self-disclosure will be positively related to the intention to disclose personal information.

2.4 A desire for privacy protection

Every person has an individual optimal level of privacy (Altman, 1975) depending on the extent of one's need for privacy (Trepte & Masur, 2020). When one's current privacy level deviates from one's desired privacy level, people adjust their privacy behaviors both offline and online (Dienlin, 2014). Hence, a person may reduce their self-disclosure or may engage in privacy-protective behaviors when they perceive to have little privacy online. Based on empirical findings revealing that Internet users are quite concerned about their privacy and have high privacy risk perceptions (e.g., Bol et al., 2018; Meier, Schäwel, Kyewski, & Krämer, 2020), it can be assumed that many Internet users' perceived levels of privacy are not satisfying which should induce a desire for a higher privacy level. We define this desire for more privacy protection as a general wish that websites and companies keep user data safe from misuse, treat and store them confidentially, and do not disseminate them to third parties for purposes other than the originally intended ones. People who desire more online privacy protection should be more likely to engage in privacy regulation efforts (Dienlin, 2014) to restore their optimal privacy level (Altman, 1975). Online, people can either engage in passive regulation strategies (e.g., reducing self-disclosure) or in active regulation strategies (e.g., usage of privacy tools; Matzner et al., 2016). Thus, the following hypotheses are derived:

Hypothesis 3 (H3): Participants' desire for privacy protection will be negatively related to the intention to disclose personal information.

Hypothesis 4 (H4): Participants' desire for privacy protection will be positively related to the willingness to use the privacy-protective tool.

Above, it has been described that self-disclosure is the result of risk and benefit perceptions, trust, and a sense of control. Similarly, it is conceivable that the factors associated with people's intention to disclose, are related to the desire for more privacy protection, too. Dienlin and Metzger (2016) applied a privacy calculus framework to examine people's self-disclosure and self-withdrawal behaviors on Facebook. They found that people's privacy concerns were positively related to their self-withdrawal intention. This indicates that the privacy calculus is applicable to investigate both information revelation and privacy protection. When people perceive high risks to their privacy online, their current privacy level is likely to fall below their desired level (Altman, 1975; Dienlin, 2014).

Hence, people who perceive high privacy threats should have a high desire for privacy protection. Conversely, trust and perceived control may be negatively related to one's desire for protection. Someone who trusts another party does not expect the other party to behave in a detrimental way (Bhattacharya et al., 1998). Therefore, when someone does not expect privacy violations, their desire for more privacy should be rather low. In the same vein, people who think that they can control how a company treats their personal information may perceive reduced privacy risks (Krasnova et al., 2010). Or stated differently: people who think that websites do not give them any control options may develop a wish to regain control over personal information (in this case a desire for protection). Hence, people who trust a website and perceive to have control over their personal information seem to have an enhanced feeling of privacy (Meier, Schäwel, & Krämer, 2020; Teutsch et al., 2018) and would therefore be less likely to desire more privacy protection. Finally, perceiving high self-disclosure benefits may be negatively related to one's desire for privacy protection. According to the privacy calculus, people weigh perceived risks and benefits (Dinev & Hart, 2006). Primarily anticipating benefits with disclosure may override the perception of privacy costs (Trepte et al., 2015). Consequently, when the salience of privacy costs is reduced, people should also have a lower protection desire. Based on these assumptions, the following hypotheses are derived:

> *Hypothesis 5 (H5): Perceived privacy risks will be positively related to participants' desire for privacy protection.*
>
> *Hypothesis 6 (H6): (a) Trust, (b) perceived control over information and (c) perceived benefits of self-disclosure will be negatively related to participants' desire for privacy protection.*

So far, the basic framework of the integrative theoretical model was described. This study, however, further investigates whether this baseline framework will be stable across different contexts and whether people's intention to adopt privacy protection depends on software characteristics. These factors will be described in the following.

2.5 Privacy context

Privacy behaviors are thought to be context dependent (e.g., Nissenbaum, 2010). In her work on contextual integrity, Nissenbaum (2010) describes contexts as structured settings that are characterized by differing actors, activities, roles, relationships, and norms but also intra-individual factors like goals and purposes of disclosure. This means that in each context people have certain expectations on how information is treated, and which information is appropriate to share. Whereas there are few studies that investigated self-disclosure in different contexts (i.e., different websites; Bol et al., 2018; Xu et al., 2008), there is an apparent lack of contextual studies and privacy protection. In the current work, a context is conceptualized as a specific form of website (i.e., social networking site, e-health website, e-commerce website). When people have a certain expectation

how personal information is treated in one context (Nissenbaum, 2010), their intention to self-disclose, their desire for protection, and their intention to protect their privacy might also be context dependent. So far, empirical findings regarding privacy (protection behavior) in different contexts are scarce. Whereas Xu and colleagues (2008) found that different websites unequally affected privacy-related perceptions, Bol and colleagues (2018) found the general privacy calculus notions to be stable across different websites. This means that privacy risk and benefit perceptions affect self-disclosure regardless of the specific context. However, it may be that a certain context elicits a specific feeling of privacy that leads to a higher or lower desire for protection and subsequently results in an increased or decreased privacy protection intention. Because of limited research findings we formulate the following research question:

> *Research Question 1 (RQ1): Will different contexts (i.e., social, health, and commerce) impact the relationships between perceived risks, trust, control, and benefits and (a) self-disclosure intention, (b) desire for protection, and (c) the relationship between the desire for protection and the willingness to use the privacy-protective tool?*

2.6 Privacy-protecting tools

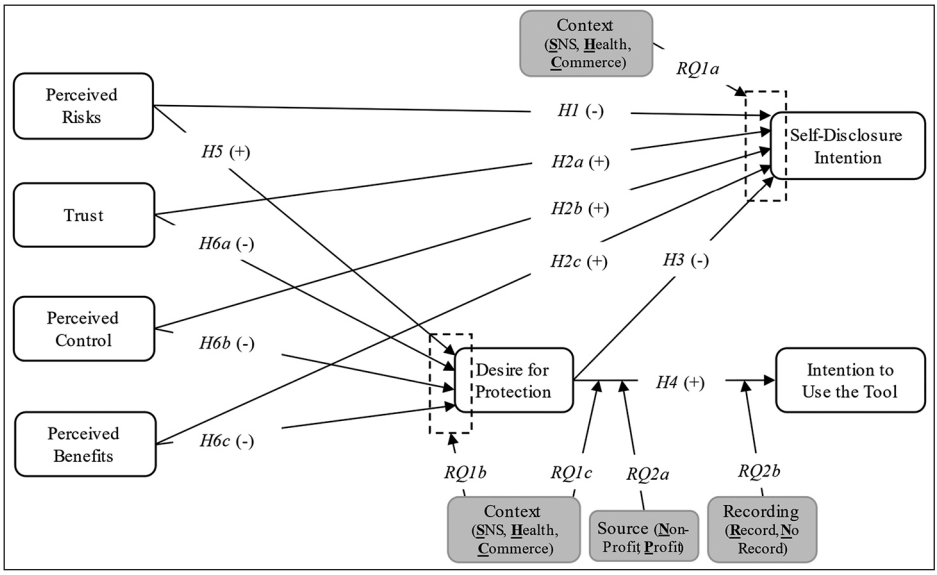
Tools for privacy enhancement can automatically prevent privacy risks stemming from user-tracking mechanisms and they can increase users' knowledge of websites' data processing (Meng et al., 2016; Mozilla, 2019). Thus, it seems that using such tools has primarily positive effects by increasing online privacy and equipping users with knowledge. However, special characteristics could determine whether a tool is accepted or rejected by users. Privacy-protecting technologies can be offered by different developers like data-protectionists or by profit-oriented companies that aim to sell their product. These different developers, however, could elicit different perceptions of the intentions behind offering such a tool. Profit-oriented companies may be associated with data-tracking mechanisms themselves and people may mistrust these developers.

Some privacy tools need access to one's personal data to provide personalized protection or transparency. For instance, Mozilla's transparency enhancing tool *Lightbeam* requests access to a user's information on visited websites (Mozilla, 2019). However, users who primarily desire better privacy protection may be deterred by the fact that a privacy-protecting tool can theoretically invade one's privacy itself. This raises the question whether Internet users will be motivated to use privacy tools that collect and process user data to provide optimal privacy protection and personalized recommendations. Because we are not aware of any former studies addressing these issues, we state the following research question:

> *Research Question 2 (RQ2): Will the relationship between the desire for protection and the willingness to use the privacy-protective tool be affected by (a) the source of the tool and (b) the tools' ability to record user data?*

As can be seen in Figure 1, all hypotheses and research questions will be integrated into one hypothetical model.

Figure 1. Integrative model comprising all hypotheses and research questions



Note. Gray boxes represent the experimental conditions.

3. Method

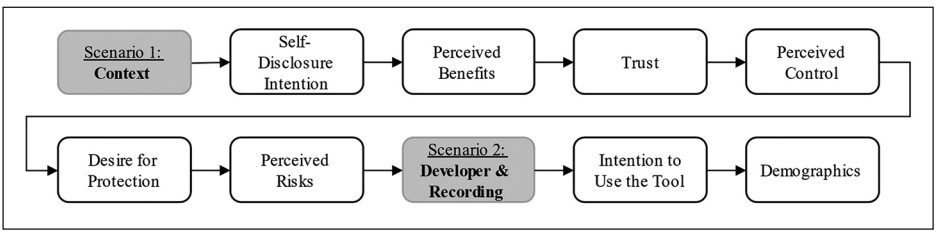
The present study features online supplementary material (OSM) including the dataset, additional stimulus material, the items of the study, and additional analyses. The OSM can be accessed via: https://osf.io/5ym97/

3.1 Procedure and scenarios

The present experimental online study comprised a 3 (context) x 2 (source) x 2 (data-record) between-subjects design. Each participant was confronted with two scenarios, one in the beginning and one towards the end of the survey. Figure 2 shows the order of the scenarios and questionnaires. In the first scenario, respondents should imagine having registered on either a (1) social networking site, (2) an e-health, or (3) an e-commerce website which manipulated the context. Afterwards, they were asked to indicate their self-disclosure intention, perceived benefits, trust towards the respective website, control over personal information, desire for protection, and perceived privacy risks. Afterwards, the second scenario was presented. In the second scenario, participants should imagine visiting the same website as described in the first scenario while having the option to use a privacy-protecting tool. The descriptions were accompanied by a mockup of the tool's appearance (see OSM). The tool was described to provide both transpar-

ency (display potential privacy risks of the used website) and privacy protection (blocking user-tracking mechanisms). The tool developers were described to be either (1) researchers and data protectionists or (2) a profit-oriented company (source). Finally, participants were told that the tool either (1) collects their data in order to provide them with personalized advice messages that could lead to a better privacy protection or (2) that it does not collect user data respecting the privacy of users (data-record). After the second scenario, participants were asked to indicate their willingness to use the presented privacy-protecting tool.

Figure 2. Study procedure



Note. Chronological sequence of the scenarios (gray boxes) and the scales (white boxes). In scenario 1 the context was manipulated and in scenario 2 the characteristics of the privacy-protecting tool were manipulated.

3.2 Sample

Five hundred and thirty-two participants were recruited online via social media channels for survey distribution and different websites on which persons voluntarily participate in surveys. Twenty individuals were excluded from the sample due to too little participation times (significantly less than 4 minutes) and one person was excluded because he/she was an extreme outlier. The final sample included 511 participants (367 females, 139 males, 5 did not specify gender), aged 15 to 65 (M = 27.14, SD = 8.22). Most participants stated to have a university degree (52.25%) followed by high school graduates (37.77%). The majority of participants were university students (69.67%) followed by employees (18.20%). The design of the study was approved by an ethics committee. Participation was incentivized by the raffle of monetary prizes (200€ in total).

3.3 Measurements

The following questionnaires were presented on a seven-point Likert-scale (if not specified differently) from 1 = *I do not agree at all* to 7 = *I fully agree*. Scales were analyzed in confirmatory factor analyses (CFA) to test for one-dimensionality and reliability. Among some scales, items had to be deleted (see OSM). Ultimately, all constructs showed good reliability (see Table 1).

Table 1. Results of the confirmatory factor analyses of all independent and dependent variables and reliabilities (Cronbach's α, McDonald's Ω, and Average Variance Extracted)

	χ^2 (df)	*p*	CFI	TLI	RMSEA	SRMR	α	Ω	AVE
Perceived benefits	35.39 (13)	.001	.99	.98	.06	.03	.88	.88	.50
Perceived risks	25.18 (4)	< .001	.98	.96	.10	.03	.85	.84	.52
Trust	4.18 (2)	.124	1.00	1.00	.05	.01	.90	.91	.71
Perceived control	3.65 (2)	.162	1.00	1.00	.04	.01	.87	.88	.64
Desire for protection	1.11 (1)	.293	1.00	1.00	.01	.01	.88	.89	.67
Self-disclosure intention	28.79 (6)	< .001	.99	.97	.09	.03	.88	.86	.53
Intention to use the tool	2.72 (2)	.256	1.00	1.00	.03	.01	.92	.92	.75

Perceived benefits. Perceived benefits of self-disclosure were assessed by 12 items used in previous studies by Dienlin and Metzger (2016) and by Bol and colleagues (2018). The items covered a social dimension (e.g., "Sharing personal information on the website would help me feeling more connected to others") and a non-social dimension (e.g., "Sharing personal information on the website would help me finding information faster"). Five items were deleted within CFA.

Perceived privacy risks. Perceived privacy risks were assessed by 12 items that covered risks by other users (horizontal privacy risks) and risks by governments or companies (vertical privacy risks; see Debatin, 2011). Six items covering the vertical dimension (e.g., "I think that the websites would collect information about my online search behavior") were taken from the study by Bol and colleagues (2018), and another six items were developed to fit the horizontal dimension (e.g., "I find it problematic when other persons know things about me that I have disclosed on the website"). Seven items had to be deleted based on CFA results.

Trust. Trust in the respective website was measured by four items developed by Bol and colleagues (2018), for instance, "I think that the website would protect my personal information".

Perceived control. Four items by Dinev et al. (2013) were used to capture perceived control over personal information (e.g., "I believe I can control my personal information provided to the website").

Self-disclosure intention. Participants' self-disclosure intention was measured by nine items developed by Dienlin and Trepte (2015) for example: "How much identifying information do you currently want to provide on the website?".

Desire for privacy protection. Six self-developed items captured participants' general desire for more protection of their personal data on the Internet (e.g., "I wish that website owners collect fewer personal data from me"). Two items were deleted within CFA.

Intention to use the tool. After the presentation of the scenarios that were described above, participants' intention to use the tool was assessed by four items

adapted from Moon and Kim (2001) (e.g., "I would use the software on a regular basis").

4. Results

Statistical analyses were performed using IBM SPSS Statistics 25 and IBM SPSS Amos 25. The structural equation model (SEM) was analyzed using the mean scores of the scales and maximum likelihood estimation. Observed variables were chosen to decrease model complexity compared to a latent factor solution. Bivariate correlations of the independent and dependent variables can be seen in Table 2.

Table 2. Means, standard deviations and bivariate correlations of all independent and dependent variables as well as sex and age

	M (*SD*)	1	2	3	4	5	6	7	8
1 Perceived benefits	3.34 (1.33)	-							
2 Perceived risks	5.90 (1.10)	- .19***	-						
3 Trust	2.92 (1.34)	.33***	- .24***	-					
4 Perceived control	2.65 (1.29)	.29***	-.32***	.57***	-				
5 Desire for protection	6.10 (1.06)	- .14**	.63***	- .28***	-.34***	-			
6 Self-disclosure intention	2.60 (1.12)	.39***	-.31***	.31***	.36***	-.29***	-		
7 Intention to use the tool	4.99 (1.55)	.12**	.15**	-.00	-.01	.15**	.06	-	
8 Sex (1 = f, 2 = m)[a]	1.27 (.45)	-.01	-.19**	.07	.03	-.13**	.06	-.13**	-
9 Age	27.17 (8.25)	-.06	.14**	-.09*	-.04	.11*	-.05	-.08	.11*

Note: [a]persons who did not specify gender (n = 5) were excluded from the correlations with sex; *p < .05, **p < .01, ***p < .001

4.1 Descriptive values

The descriptive values of the main constructs (see Table 2) revealed that participants perceived high privacy risks (M = 5.90, SD = 1.10), had a high desire for privacy protection (M = 6.10, SD = 1.06) and a relatively high intention to use the privacy-protecting tool (M = 4.99, SD = 1.55). Perceived control (M = 2.65, SD = 1.29), perceived trust (M = 2.92, SD = 1.34), perceived benefits (M = 3.34, SD = 1.33) as well as self-disclosure intention (M = 2.60, SD = 1.12) were rather low.

4.2 Structural equation model

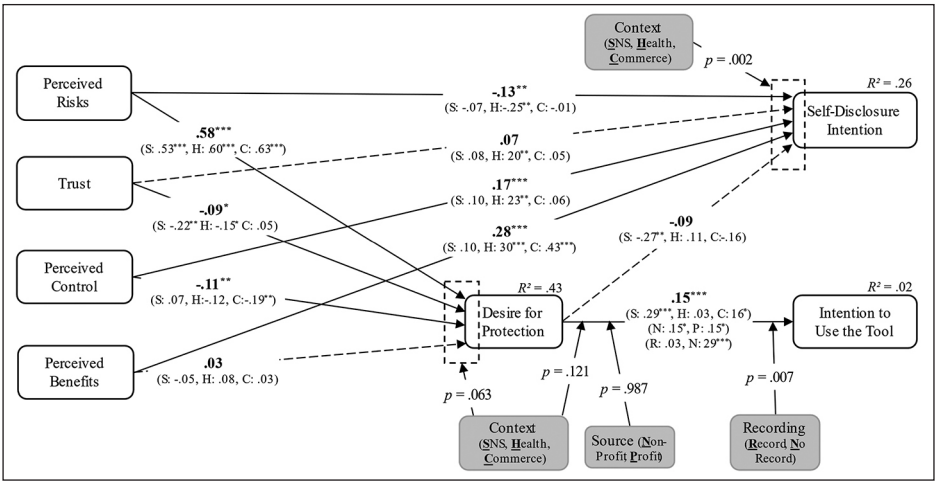
Testing the hypothesized relationships within an SEM revealed a well-fitting model: χ^2 (5) = 17.75, p = .003, χ^2/df = 3.55, CFI = .98, TLI = .93, RMSEA = .07 (90% CI: .04, .11), SRMR = .04. Additional information about the model fit criteria can be found in Table 3. Although the TLI was slightly below the proposed cut-off criterion of .95, combinational rules find CFI and TLI values of .90 to be still acceptable, provided that the SRMR does not exceed a value of .06 (Hu & Bentler, 1999). The whole model can be seen in Figure 3. First, the privacy calculus assumptions extended by trust and perceived control were examined. The data showed that perceived privacy risks were negatively related to self-disclosure intention (β = -.13, p = .010) supporting *H1*. Regarding the second hypothesis, only *H2a* and *H2b* were found to be supported by the data, but not *H2c*. Both perceived benefits (β = .28, p < .001) and perceived control (β = .17, p < .001) were positively related to self-disclosure intention. However, there was no significant relationship between trust and self-disclosure intention (β = .07, p = .178). Second, the predicted relation between participants' desire for protection and passive as well as active protection strategies was investigated. *H3* was not supported by the data as the desire for protection was not significantly negatively related to self-disclosure intention (β = -.09, p = .066). Twenty-six percent of variance of self-disclosure intention were explained (R^2 = .26). In contrast, *H4* was supported revealing a positive relationship between the desire for protection and the intention to use the tool (β = .15, p = .001). Two percent of variance of participants' willingness to use the tool were explained (R^2 =.02). Third, it was investigated whether the variables of the extended privacy calculus framework would be related to participants' desire for protection. Results supported *H5* showing that perceived privacy risks and the desire for protection were positively related to each other (β = .58, p < .001). In accordance with *H6a* and *H6b*, trust towards the website (β = -.09, p = .032) and perceived control (β = -.11, p = .008) were negatively related to participants' desire for protection. However, perceived benefits and desired protection were not significantly related to each other (β = .03, p = .415) not supporting *H6c*. Together, the variables explained 43% of the variance among the desire for protection (R^2 = .43).

Table 3. *Model fit indices for the four analyses.*

Parameter	Criteria	Overall model	Multigroup Analyses		
			Contexts	Developer	Data Record
χ^2		17.75	33.45	25.62	19.60
df		5	15	10	10
χ^2/df	< 5[a]	3.55	2.23	2.56	1.96
CFI	≥ .95[b]	.98	.98	.98	.99
TLI	≥ .95[b]	.93*	.91*	.92*	.95
RMSEA (90% CI)	< .08[c]	.07 (.04, .11)	.05 (.03, .07)	.06 (.03, .08)	.04 (.01, .07)
SRMR	< .08[b]	.04	.04	.03	.05

Note: [a]Marsh & Hocevar (1985), [b]Hu & Bentler (1999), [c]Browne & Cudeck (1993), *CFI and TLI values of > .90 acceptable provided that SRMR ≤ .06 (Hu & Bentler, 1999)

Figure 3. Structural equation model



Note. Bold numbers represent standardized effect sizes of the main model. Gray boxes represent the experimental conditions that were analyzed as multigroup analyses. Numbers in parentheses represent the standardized effect sizes of the multigroup analyses. Dashed lines indicate that the effect in the main model was not significant.
$^{*}p < .05$, $^{**}p < .01$, $^{***}p < .001$

4.3 Multigroup analyses

In order to analyze *RQ1* and *RQ2*, multigroup analyses were performed. In a multigroup analysis the components of the model are tested for measurement invariance, which means that the analysis tests whether the relations between the variables are performing equivalent between different sub-samples (Byrne, 2010). To do so, five different constrained models (*RQ1a – RQ2b*) were tested against the unconstrained model to detect measurement invariance (see Byrne, 2010). By this means a potential influence of experimental conditions on the model paths can be detected. *RQ1* followed the question whether the three different contexts would lead to structural differences in the paths leading to self-disclosure, the desire for privacy protection, and the intention to use the tool. *RQ2* focused on the tool characteristics pursuing the question whether different tool developer or the tool's ability to record user data would impact the relationship between the desire for protection and tool usage intention. Prior to testing structural invariance, metric invariance was tested in order to determine whether the items measure the same latent factor across different groups (Putnick & Bornstein, 2016). Assumptions of metric invariance were not violated implying that the factor loadings of the latent factors were comparable across conditions (see OSM).

4.3.1 Contexts

In the first multigroup analysis, the fit of the unconstrained model was good: χ^2 (15) = 33.45, p = .004, χ^2/df = 2.23, CFI = .98, TLI = .91, RMSEA = .05 (90% CI: .03, .07), SRMR = .04. Comparing the first constrained to the unconstrained model (*RQ1a*) did produce a significant decrease in model fit ($\Delta(\chi^2)$ = 27.23, $\Delta(p)$ = .002) implying that the three different contexts did have an impact on the effects in this model (see Figure 3). Specifically, in the SNS context, neither perceived risks, nor perceived control nor anticipated benefits were significantly related to self-disclosure intention. Instead, participants' desire for privacy protection was negatively related to self-disclosure intention. In the health context, trust was positively related to the intention to disclose and in the e-commerce context, neither perceived privacy risks nor perceived control were related to self-disclosure intention.

Turning towards the next analysis (*RQ1b*), results indicated that the effects on desire for protection were not context dependent as model fit did not decrease significantly ($\Delta(\chi^2)$ = 14.82, $\Delta(p)$ = .063). Finally, the last context analysis (*RQ1c*) pointed to a context-independency of the relation between desire for protection and the intention to use the tool ($\Delta(\chi^2)$ = 4.22, $\Delta(p)$ = .121).

4.3.2 Tool developer and record of user data

Next, two separate analyses were performed to examine whether the other two conditions (source and data-record) had an impact on the relationship between participants' desire for protection and the intention to use the tool (*RQ2*). The first analysis (*RQ2a*) investigated the impact of the source of the tool and revealed a well-fitting model: χ^2 (10) = 25.62, p = .004, χ^2/df = 2.56, CFI = .98, TLI = .92, RMSEA = .06 (90% CI: .03, .08), SRMR = .03. However, results indicated that there was no difference in the relationship between desire for protection and the intention to use the tool dependent on the developer ($\Delta(\chi^2)$ = 0.40, $\Delta(p)$ = .942). The analysis of *RQ2b* also revealed a good model fit: χ^2 (10) = 19.60, p = .033, χ^2/df = 1.96, CFI = .99, TLI = .95, RMSEA = .04 (90% CI: .01, .07), SRMR = .05. Since the model fit of the constrained model decreased significantly ($\Delta(\chi^2)$ = 7.18, $\Delta(p)$ = .007), there was a difference among the relationship between desire for protection and the intention to use the tool depending on whether the tool collects data or not. Looking at the effects revealed that the desire for protection was not significantly related to the willingness to use the tool when participants were told that it collects their personal data but only when they were told that it does not collect user data (see Figure 3).

5. Discussion

The current study applied an extended privacy calculus framework to investigate internet users' desire for privacy protection, their self-disclosure intention, and their willingness to adopt a privacy-protective tool across different contexts. The findings of this study tie in with results of previous studies and expand the under-

standing of internal and external factors important to online privacy behavioral intentions, particularly to Internet users' willingness to protect their privacy by using privacy protective tools.

5.1 Privacy calculus

The overall findings of the present study support the general privacy calculus assumptions that perceiving privacy risks is associated with a decrease in self-disclosure intentions and perceiving benefits of information sharing is positively related to disclosure intentions (Culnan & Armstrong, 1999; Dinev & Hart, 2006). Like in previous studies (e.g., Dienlin & Metzger, 2016; Meier, Schäwel, Kyewski, & Krämer, 2020) the association between perceived benefits and self-disclosure was highest. The size of the relation between perceived risks and disclosure was comparably smaller. One explanation for this pattern is that the perception of rewards that are typically certain, immediate, and more tangible than privacy risks impact people's behavioral intentions and behaviors more than the perception of (abstract and uncertain) privacy risks (cf. Trepte et al., 2015). Besides these findings, a positive relationship between information control and self-disclosure intention was found replicating previous results (Brandimarte et al., 2012). However, contrary to prior studies (Bol et al., 2018; Metzger, 2006) people who trusted a website were not willing to reveal more information. Hence, participants who had the feeling of being in control of what will happen to their data but not those who believed in a website's honesty and confidentially were more intended to disclose information. Looking at bivariate correlations, however, reveals that trust and perceived control were highly related to each other. This might be a further indication that trust and perceived control are not completely independent factors but that they contribute to a general feeling of privacy (Meier, Schäwel, & Krämer, 2020; Teutsch et al., 2018).

5.2 The desire for more privacy protection

One major aim of the current study was to examine whether the components of the privacy calculus would also be related to Internet users' desire for online privacy protection. Results supported the idea that perceiving privacy risks is highly related to a desire for better privacy protection. This implies that the awareness of Internet privacy risks is an indicator of perceiving one's current privacy level below one's desired optimum (Altman, 1975; Dienlin, 2014). In contrast, trust towards a website and the perception of control over personal data were negatively associated with the desire for protection. Hence, persons who think that websites handle their personal data confidentially and believe that they can decide what will happen to their personal information after disclosure, appear to have a weakened wish for privacy protection. This corresponds to the idea that trust and control perceptions are related to a situational privacy feeling (Teutsch et al., 2018). Nevertheless, the effect sizes of both trust and perceived control were very small. Contrary to our assumptions that primarily perceiving the self-disclosure benefits would replace risk awareness resulting in a reduced desire for protection,

results did not reveal such a relation between benefit perception and the protection desire. Thus, it seems that an anticipation of benefits and privacy protection (or the desire thereof) are rather independent (cf. Dienlin & Metzger, 2016). A general observation was that participants' desire that their personal data are better protected online was extremely high. Hence, many people seem to be unsatisfied thinking that companies do not really care about their online privacy.

Based on the assumption that people who desire more privacy online engage in privacy regulation (Dienlin, 2014), it was investigated whether those who desired more protection would be less willing to reveal personal information and more intended to use the privacy tool. Whereas the assumption that participants' desire for privacy protection would be negatively related to their self-disclosure intention was not supported, individuals who had a higher desire for protection were found to have a higher willingness to use the tool. Hence, it seems that passive privacy protection by reducing self-disclosure was not considered as effective as applying an active strategy, that is the usage of the protective tool (cf. Matzner et al., 2016). Remarkably, the size of the relationship between the desire for privacy protection and the willingness to use the tool was rather small. Thus, using privacy tools appears to be not the best strategy to restore a desired privacy level and participants might consider other protection strategies as more useful. Moreover, people could passively demand protection from the legal or technical site, but do not perceive themselves to be in the position to achieve the desired state. However, past studies showed that privacy protection is a rather complex behavior and that numerous factors predict people's motivation to protect their privacy. For instance, people need to believe that protection actually leads to increased privacy (Boerman et al., 2018) and people require relatively high Internet skills to engage in protection (Büchi et al., 2016). Finally, it may also be that Internet users – although many seem to desire more online privacy – show no change in privacy behaviors (known as the privacy paradox[1]; Barnes, 2006) or they may have resigned to engage in protective attempts (Hoffmann et al., 2016). Importantly, the experimental manipulation (data collection of the tool) affected the relation. Hence, the effect size might have been decreased due to certain tool characteristics (see below).

5.3 Privacy in different contexts

Unlike at the general level, the privacy calculus notions were not replicated, on a contextual level. This means that participants' perceptions of privacy risks and benefits were not related to their self-disclosure intentions in each context. For instance, in the social context, neither perceived privacy risks nor perceived benefits were significantly related to self-disclosure which contradicts previous findings (Dienlin & Metzger, 2016; Krasnova et al., 2010; Meier, Schäwel, Kyewski,

1 There are numerous explanations for why researchers initially found people's privacy attitudes and privacy behaviors to be inconsistent, for instance, privacy literacy (Trepte et al., 2015), privacy cynicism (Hoffmann et al., 2016), and the privacy calculus (Culnan & Armstrong, 1999). Hence, the privacy paradox is mainly viewed as a "relic" today (cf. Dienlin & Trepte, 2015).

& Krämer, 2020). This may be explained by the fact that the scales were not suitable for every context (e.g., most social benefit items were deleted in the CFA; see OSM). This understanding of the findings would not refute the general logic of the privacy calculus, but would rather strengthen contextual ideas (e.g., Nissenbaum, 2010), which means that context-specific privacy risks and benefits are associated with self-disclosure in different contexts. In addition, this logic is also supported by the study of Bol and colleagues (2018) who found the general privacy calculus being stable across three website types. An alternative explanation might relate to the analytical method: because multigroup analyses use subsamples, statistical power was reduced which may have led to not finding effects of a certain size.

Turning towards privacy protection and contextual notions, the findings revealed that both participants' desire for privacy protection and their willingness to use the tool were independent of the three contexts. This indicates a positive relation between privacy risk perceptions and the protection desire and negative relations between trust and perceived control and the desire for protection regardless of specific websites. Likewise, participants who desired more privacy had a higher willingness to use the privacy-protecting tool independent of a particular website. Thus, it seems that disclosing information is driven by context-specific perceptions and expectations, but privacy protection processes are rather cross-contextual. Consequently, the current study combines a contextual perspective (self-disclosure) and a cross-contextual perspective (privacy protection). One's desire for privacy protection may represent a general feeling that is rather independent of single contexts but in fact based on knowledge and experience. Therefore, the causal implications of the model should be interpreted with particular caution because it might well be that the general feeling of the desire for protection impacts contextual perceptions.

5.4 Characteristics of privacy tools

Finally, two of the tool's characteristics were varied to learn more about external factors impacting participants' willingness to adopt privacy tools. First, the tool was described as being either developed by a profit organization or by a non-profit organization. However, results did not reveal an impact of the tool developer on the relation between desire for protection and participants' willingness to use the tool. This shows that the mere fact that a tool is provided by a private company is not a reason to not use it. Second, the tool was described as either recording user data to better protect their privacy or to refrain from recording personal data. In contrast to the developer, the tool's ability to record user data had an impact on the relationship. Participants whose desire for protection was high were only willing to use the tool, when it did not collect their personal information. This means that Internet users who desire privacy protection would probably forego using protection tools that can record their data which might, however, result in being exposed to higher privacy risks by websites. Moreover, tools that offer personalized privacy protection (e.g., recommendations) might be more effective compared to general ones. This seems to be a somewhat paradoxi-

cal finding because users who renounce the usage of privacy-protecting technologies would probably automatically reveal more personal data to websites than users who use such software. This phenomenon should be investigated in more detail since the tool description was rather superficial. Hence, the effect might vanish when the reasons for data recording and its subsequent usage are explained to them in more detail.

5.5 Limitations and future directions

The current study entails some limitations. First, the cross-sectional nature of the investigation does not allow drawing any causal conclusions from the relationships in the model. This might especially be an issue among the effects on desire for protection as it could be that there are reversed causalities or reciprocal relationships. Second, the study used a scenario-based design. This leads to an increase in internal validity and has the further advantage of applying easily controllable manipulations, but at the same time external validity is low. Hence, in the future, participants may be asked to use existing privacy and transparency enhancing technologies while visiting actual websites to eliminate the artificial nature of a scenario-based design. A third issue is that no real behavior but only participants' intentions to self-disclose and to use the tool were assessed. Thus, technical skills and time efforts to adopt such a tool could play significant roles for real usage behavior. In future studies, it would thus be beneficial to examine the actual behavior of persons who interact with a privacy-protecting technology. Fourth, the results of the multigroup-analyses are based on subsamples, which means that its power is lower compared to the total sample. Hence, its results must be handled carefully. Fifth, the convenience sample that was gathered for the present study imposes limitations in terms of age, gender, and education levels. Correlations indicate that privacy risk perceptions may be skewed because there were more women than men (30:70) and the sample was quite young. Moreover, the sample was highly educated implying that knowledge about the application of privacy protection may have been high. Future studies could use representative samples to detect unbiased effect sizes.

5.6 Conclusion and implications

Although billions of people around the globe use Internet technologies which threaten their personal privacy, their online privacy behaviors are still not fully understood. The current study has added to the knowledge of psychological factors related to both online self-disclosure and privacy protection by protective tools in three different contexts. The results showed that the privacy calculus is stable on a general but not on a contextual level. This implies that context-specific risk and benefit perceptions drive self-disclosure. Contrary, people's desire for privacy protection and their intention to adopt a privacy-protecting tool were context independent. This indicates that people who desire more privacy than a current situation provides engage in attempts to restore privacy irrespective of specific contexts. Trust in websites and the perception of control over information

seem to contribute to a feeling of privacy which can lead to increased disclosure and decreased protection efforts. On a practical level, it was found that people who desire to have more online privacy may forgo privacy-protecting tools that collect personal data themselves. Hence, they might perceive the tool itself as a possible source of privacy invasion. Summed up, the present study found that the privacy calculus framework can be used to investigate both self-disclosure and privacy protection in different contexts. Whereas participants who desired to have more online privacy were more willing to protect their privacy by using a tool (that does not collect user data itself), they seem to still need (legal or technical) assistance in shielding privacy threats.

References

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

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday, 11*(9). https://doi.org/10.5210/fm.v11i9.1394

Bhattacharya, R., Devinney, T. M., & Pillutla, M. M. (1998). A formal model of trust based on outcomes. *Academy of Management Review*, *23*(3), 459–472. https://doi.org/10.5465/amr.1998.926621

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

Bol, N., Dienlin, T., Kruikemeier, S., Sax, M., Boerman, S. C., Strycharz, J., Helberger, N., & 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

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2012). Misplaced confidences: Privacy and the control paradox. *Social Psychological and Personality Science*, *4*(3), 340–347. https://doi.org/10.1177/1948550612455931

Browne, M. W., & Cudeck, R. (1993). Alternative ways of assessing model fit. In K. A. Bollen & J. S. Long (Eds.), *Testing structural equation models* (pp. 136–163). SAGE Publications.

Büchi, M., Just, N., & Latzer, M. (2016). Caring is not enough: the importance of Internet skills for online privacy protection. *Information, Communication & Society, 20*(8), 1261–1278. https://doi.org/10.1080/1369118X.2016.1229001

Bujlow, T., Carela-Español, V., Sole-Pareta, J., & Barlet-Ros, P. (2017). A survey on web tracking: Mechanisms, implications, and defenses. *Proceedings of the IEEE, 105*(8),1476–1510. https://doi.org/10.1109/JPROC.2016.2637878

Byrne, B. (2010). *Structural equation modeling with AMOS. Basic Concepts, Applications and Programming*. Routledge Taylor & Francis Group.

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

Debatin, B. (2011). Ethics, privacy, and self-restraint in social networking. In S. Trepte & L. Reinecke (Eds.), *Privacy online* (pp. 47–60). Springer. https://doi.org/10.1007/978-3-642-21521-6_5

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). Karl Stutz Verlag.

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

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology, 45*(3), 285–297. https://doi.org/10.1002/ejsp.2049

Dinev, T., Albano, V., Xu, H., D'Atri, A., & Hart, P. (2016). Individuals' attitudes towards electronic health records: A privacy calculus perspective. In A. Gupta, V. L. Patel, & R. A. Greenes (Eds.), *Annals of information systems: Vol. 19. Advances in healthcare informatics and analytics* (pp. 19–50). Springer. https://doi.org/10.1007/978-3-319-23294-2_2

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

Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates: An empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems*, *22*(3), 295–316. https://doi.org/10.1057/ejis.2012.23

Heath, R. L., & Bryant, J. (2013). *Human communication theory and research: Concepts, contexts, and challenges*. Routledge Taylor & Francis Group.

Hoffmann, C. P., Lutz, C., & Ranzini, G. (2016). Privacy cynicism: A new approach to the privacy paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 10*(4), Article 7. https://doi.org/10.5817/CP2016-4-7

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

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

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

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

Matzner, T., Masur, P. K., Ochs, C., & von Pape, T. (2016). Do-it-yourself data protection -empowerment or burden? In S. Gutwirth, R. Leenes, & P. De Hert (Eds.), *Law, governance and technology series, Vol. 24. Data protection on the move* (pp. 277– 305). Springer. https://doi.org/10.1007/978-94-017-7376-8_11

Meier, Y., Schäwel, J., & Krämer, N. C. (2020). The shorter the better? Effects of privacy policy length on online privacy decision-making. *Media and Communication*, *8*(2), 291–301. https://doi.org/10.17645/mac.v8i2.2846

Meier, Y., Schäwel, J., Kyewski, E., & Krämer, N. C. (2020). Applying protection motivation theory to predict Facebook users' withdrawal and disclosure intentions. In A. Gruzd, P. Mai, R. Recuero, Á. Hernández-García, C. S. Lee, J. Cook, J. Hodson, B. McEwan, & J. Hopke (Eds.), *SMSociety'20: International conference on social media and society* (pp. 21–29). Association for Computing Machinery https://doi.org/10.1145/3400806.3400810

Meng, W., Lee, B., Xing, X., & Lee, W. (2016). TrackMeOrNot: Enabling flexible control on web tracking. In J. Bourdeau, J. A. Hendler, R. Nkambou Nkambou, I. Horrocks, & B. Y. Zhao (Eds.), *WWW '16: Proceedings of the 25th international conference on World Wide Web* (pp. 99–109). Republic and Canton of Geneva, Switzerland: International World Wide Web Conferences Steering Committee. http://doi.org/10.1145/2872427.2883034

Metzger, M. J. (2006). Effects of site, vendor, and consumer characteristics on web site trust and disclosure. *Communication Research*, *33*(3), 155–179. https://doi.org/10.1177/0093650206287076

Moon, J. W., & Kim, Y. G. (2001). Extending the TAM for a World-Wide-Web context. *Information & Management, 38*(4), 217–230. https://doi.org/10.1016/S0378-7206(00)00061-6

Mozilla. (2019, November 10). Lightbeam 3.0. Retrieved from https://addons.mozilla.org/de/firefox/addon/lightbeam-3-0/

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

Papacharissi, Z. (2010). Privacy as a luxury commodity. *First Monday, 15*(8). https://doi.org/10.5210/fm.v15i8.3075

Putnick, D. L., & Bornstein, M. H. (2016). Measurement invariance conventions and reporting: The state of the art and future directions for psychological research. *Developmental Review*, *41*, 71–90. https://doi.org/10.1016/j.dr.2016.06.004

Solove, D. (2008). *Understanding privacy*. Harvard University Press.

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), 1–14. https://doi.org/10.1177/2056305118767134

Trepte, S., & Masur, P. (2020). Need for privacy. In V. Zeigler-Hill & T. Shackelford (Eds.), *Encyclopedia of personality and individual differences*. Springer. https://doi.org/10.1007/978-3-319-24612-3_540

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.), *Law, governance and technology series: Vol. 20. Reforming European data protection law* (pp. 333–365). Springer. https://doi.org/10.1007/978-94-017-9385-8_14

Weinstein, N. D. (1984). Why it won't happen to me: Perceptions of risk factors and susceptibility. *Health Psychology, 3*(5), 431–457. https://doi.org/10.1037/0278-6133.3.5.431

Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2008). Examining the formation of individual's privacy concerns: Toward an integrative view. *ICIS 2008 Proceedings*, *6*. https://aisel.aisnet.org/icis2008/6/

Zuiderveen Borgesius, F. J., Möller, J., Kruikemeier, S., Ó Fathaigh, R., Irion, K., Dobber, T., Bodo, B., & de Vreese, C. (2018). Online political microtargeting: Promises and threats for democracy. *Utrecht Law Review*, *14*(1), 82–96. https://doi.org/10.18352/ulr.420