Proceedings of the 54th Hawaii International Conference on System Sciences | 2021

The Dark Side of Privacy Nudging – An Experimental Study in the Context of a Digital Work Environment

Torben Jan Barev
University of Kassel
torben.barev@uni-kassel.de

Melanie Schwede
University of Kassel
melanie.schwede@wi-kassel.de

Andreas Janson
University of St.Gallen
andreas.janson@unisg.ch

Abstract

In digital environments, individuals tend to share disproportionally more information than in face-to-face communication. Critically, disclosing personal information can yield risks such as unwanted monitoring or discrimination. Privacy nudging is a promising approach to get users to disclose less personal information. In this work, we tested two nudges corresponding to the issue of personal privacy. A framing nudge conveys an intensive message, and a social nudge provides social cues. To empirically test these nudges, we evaluated an experiment with 223 participants. The results indicate that privacy nudges negatively influence information disclosure behavior. The social nudge was perceived as a threat. The framing nudge directly affected negative emotions and the social nudge indirectly. Perceived threat and negative emotions have a significant negative effect on information disclosure intention. With this research, we contribute to the discussion of what drives privacy nudge effectiveness and influences information disclosure behavior in digital work environments.

1. Introduction

Information and communication technology tools accompany almost every form of occupation. Companies use more forms of digital work systems, such as Slack, MS Teams, or company-internal intranets that are similar to social networks. Individuals use these tools to interact, work, or communicate with each other. This is associated with opportunities for employees and employers, for example, through more flexible working models, such as home office or crowdsourcing. On the flip side, these systems enable the possibility to electronically acquire information about work activities as well as personal sensitive data of individuals [36]. Personal user information is generated, for example, when creating a user profile or uploading personal documents. The issue arising is that people value their privacy while they do not always protect it [5]. A risk arises of employees becoming transparent and vulnerable to unwanted monitoring or discrimination. Economists assume that this tendency will continue to grow as companies will benefit from the advancing digitalization [36].

According to a survey by IDG Research Services, 38.4% of the interviewed German employees are concerned about being spied on at work by new technologies [20]. Furthermore, Sherif and Jewisimi (2018) conclude that the monitoring aspects of the technologies have negative effects on employees, such as increasing fluctuation, performance decrease, lack of acceptance of the technology, occupation dissatisfaction, and demotivation [22; 36]. This emphasizes that organizations should protect the privacy of their employees.

Moreover, multiple studies provide evidence that digital environments generally lead to increased self-disclosure compared to direct face-to-face communication [24, 41]. In digital environments, individuals tend to share disproportionally more information. The increased willingness for self-disclosure is attributed, among other things, to the fact that individuals feel a stronger sense of anonymity [24]. social cues are weaker in comparison to face-to-face situations, and the communication situation is perceived to a greater extent as controllable [34]. Thus, digital work environments that support users for privacy-friendly decision-making are needed.

A promising method to strengthen users' privacy-friendly decisions is digital nudging [1]. The concept of nudging comes from behavioral economics and is a mechanism to influence decision and individuals' behavior. Privacy nudges use biases and heuristics to influence users to make privacy-friendly decisions without removing any decision option [40]. If the digital work platform communicates the issue of personal privacy, this will cause privacy awareness, which is an antecedent that in turn affects privacy concerns [38]. Hence, we test two privacy nudges that specifically communicate this kind of message. First, a framing nudge, which conveys a clear and intensive privacy warning message (Figure 3). Second, a social nudge,

URI: https://hdl.handle.net/10125/71117
978-0-9981331-4-0

which mitigates the deficit of social cues in digital environments (Figure 4). Furthermore, in our study we selected nudges that are promising in raising emotional and cognitive components in individuals, as they are considered strong triggers for an individual’s behavior.

Accordingly, a more privacy-conscious working environment should have a positive impact on employees and organizations.

However, research calls for more insights about the design of nudges [4], as some developed nudges emerge to have little impact on actual behavior or even trigger unintended mechanisms [33, 39].

The aim of this research project is to better understand information disclosure behavior in digital work environments with the implementation of digital privacy nudges. Therefore, the guiding research question (RQ) for our study is as follows:

RQ: How do privacy framing nudges and privacy social nudges influence information disclosure behavior in digital work environments?

With this research, we expect a twofold contribution. From a theoretical perspective, we are contributing to the discussion of what drives privacy nudge effectiveness and influences information disclosure behavior in digital work environments. For practitioners, we offer evaluated digital nudges in digital work environments to promote information privacy.

2. Theoretical Background

2.1. Digital Nudging

Thaler and Sunstein define a *nudge* as "any aspect of the choice architecture that alters individual’s behavior in a predictable way without forbidding any options or significantly changing their economic incentives" [40, p. 6]. Nudges can be integrated into the presentation of a decision situation through small design modifications that influence individuals to make certain decisions [40]. The approach of soft or libertarian paternalism is the basis of nudging. Therefore, nudges are used to influence individuals to make decisions that are beneficial for society but also in the individual’s long-term interest, without forbidding them the choice between possible options and decisions [1].

In *digital nudging*, this concept is transferred to the digital space, and corresponding design elements in the user interface are used to influence behavior in digital decision environments [46]. Digital decision environments are user interfaces that require people to make judgments or decisions, such as purchasing decisions in an online store.

In the field of security and privacy, the basic idea behind the use of nudges is to “nudge people towards more thoughtful and informed privacy-related decisions” [44, p. 2367]. These *privacy nudges* are about preserving the informational self-determination of individuals and empowering them to make decisions that effectively protect their data security and privacy.

2.2. Privacy & Decision-Making

Westin defines the term *privacy* “as the claim of an individual to determine what information about himself or herself should be known to others” [47, p. 431]. In the digital context, the term *information privacy* is often used. Rai defines information privacy as “the ability of the individual to personally control information about one’s self” [13].

Individuals disclose personal information so that fellows know who they are. This can have several reasons and depends on the purpose and context in which individuals share personal information [24]. For example, individuals might disclose information about themselves on internal digital employee platforms because they hope that this will strengthen the relationship with colleagues at work [24]. Individuals perceive online platforms as a kind of private space in which individuals reduce their uncertainty and are motivated to disclose more data about themselves [25].

Online behavior research defines the phenomenon of the *privacy paradox*, which means the discrepancy between the attitude and actual behavior of users regarding their privacy [5]. The privacy paradox shows that individuals are concerned about the protection of their privacy. Yet, they often do not act accordingly, e.g., by disclosing personal information [5].

To show why individuals disclose information, the general decision-making process is introduced. The *general decision-making process* commences with a situation that demands a decision or behavior. Individuals first assess this situation cognitively. In this process, individuals form opinions, obtain conclusions, and critically evaluate events or individuals [35]. Depending on how individuals evaluate a situation cognitively, it triggers different emotions (positive, negative, or neutral) [2]. Both the cognitive evaluation and feelings can influence the decision, in which case individuals choose between alternatives. The decision-making process is linked to concrete behavior patterns and actions [35].

In security and privacy research, the explanatory approach of the *privacy calculus* prevails. This calculus is based on the fact that individuals try to weight the benefits against the costs [1]. Depending on whether individuals attribute higher benefits or costs to a situation, they decide for or against a certain behavior. According to the privacy paradox, individuals therefore receive more benefits than costs in disclosing their personal information. However, researchers describe human decision-making behavior as a process of limited rationality [1]. Influencing factors such as time pressure or cognitive complexity do not make purely objective decisions possible [1].

2.3. Emotional Components

Affect comprises the two terms emotions and mood. As a generic term, it encompasses a wide range of feelings that people experience. Emotions are intense feelings, which are triggered by a contextual stimulus, e.g., an interpretation of a specific event. Depending on the relevance for the person themself, emotions can lead to certain reactions and corresponding behaviors [2].

Emotions are multidimensional constructs and consist of four components: physiology, cognition, expression, and motivation [7]. In this paper, the focus is on the motivational component that triggers behavior. Mees assumes that whenever individuals perform an action, an emotion is its direct or indirect cause [30]. Therefore, individual's hope to experience positive emotions and the avoidance of feeling negative emotions influence specific behavior.

Prospect theory developed by Kahneman and Tversky states that individuals fear losses more than they welcome profits [26]. Hence, in this paper and the context of privacy nudges, we focus on negative emotions. *Negative emotions* such as fear, hostility, and upset could convince individuals to change their behavior due to reasons of conformity [29]. If individuals perceive a situation as threatening to their own person, it will trigger negative emotions because they find the situation unpleasant [48]. According to affect heuristics by Slovic et al., individuals perceive negative emotions as a feeling of risk, which leads individuals to want to avoid this risk by, for example, disclosing less personal information [37]. This is where the avoidance strategy that triggers negative emotions in individuals comes in. According to this strategy, emotions can influence the perception in decision-making situations [14]. If the perception already signals a higher risk or cost than benefits based on cognitive evaluation, then the triggered negative effects will further strengthen this assessment [27]. Hence, individuals are willing to avoid or actively control this situation and the decision-making process is affected [28]. Individuals adjust their behavior according to the perceived stimulus.

3. Hypotheses Development

According to Caraban et al., the two privacy nudges "social nudge" and "framing nudge" are categorized as transparent nudges [9]. The privacy nudges are therefore visually visible to individuals. They perceive them and understand the intention behind them [9]. On the one hand, the transparent use of privacy nudges can inform individuals about privacy, make them aware of it, and improve their privacy management [49] and, on the other hand, the transparent use of privacy nudges guarantees openness and fairness towards individuals.

3.1. Influence of Privacy Nudges

In social psychology, studies have already demonstrated that individuals act differently through social influence [12, 43]. Social influence includes changes in opinions, attitudes, or behavior that other individuals or groups trigger [43]. The concept of conformity is the basis of social influence. Conformity is defined as "the act of changing one's behavior to match the responses of others" [12]. Individuals therefore change their behavior due to the real or supposed influence of others. We assume that the new work system from our experiment represents a situation when individuals are not sure how to behave and how much data to disclose. Thus, individuals observe the behavior of other individuals to identify socially acceptable behavior. Based on the privacy nudge, individuals are adjusting their behavior. Therefore, we hypothesize:

H1: Providing a privacy social nudge in a digital work environment positively supports reducing users' intention to disclose personal information.

If the respondents assume, through the social nudge, that society accepts and performs a certain behavior (kind of social norm), and if they feel capable of implementing this behavior, it will be more likely that individuals perform a certain behavior. The social nudge can lead to a certain behavior but may also be perceived as a threat because at the same time the nudge subconsciously states alternatives that are risky and harmful. Therefore, we hypothesize:

H2: Providing a privacy social nudge in a digital work environment positively influences users' perceived threat (vulnerability and severity).

When individuals sense a threat, it may also spark negative emotions, as an individual may feel forced into a specific behavior. Hence, we hypothesize:

H3: Providing a privacy social nudge in a digital work environment influences the negative emotions of individuals.

The term framing describes something that "refers to a controlled presentation of a decision problem considering different framing methods regarding one decision problem" [31]. The framing nudge concentrates principally on the emphasis, orientation, and presentation of decision problems [31]. Framing effects include the wording of decision problems. For wording, researchers often point out the prospect theory [1]. This theory states that positive framing weighs the gains higher than the possible losses and negative framing emphasizes the losses more than the gains. Negative framing refers to loss aversion [1]. We assume that the implemented privacy framing nudge increases the risk perception (low privacy control) of individuals. Thus, individuals disclose less information. We therefore hypothesize:

H4: Providing a privacy framing nudge in a digital work environment positively supports reducing users' intention to disclose personal information.

We assume that the negative framing nudge in our experiment increases an individual's perception of the threat and risk of revealing personal information. Framings in the form of red colors, flashing boxes, or pictorial warnings seem promising, as they can be processed cognitively easily by individuals. In situations where respondents do not know the risk or underestimate it, the implemented privacy framing nudge can trigger the loss aversion bias [1], which changes the perceived risk (higher risks; lower benefits) and individuals tend to disclose less information. We therefore hypothesize:

H5: Providing a privacy framing nudge in a digital work environment positively influences users' perceived threat (vulnerability and severity).

Furthermore, we assume that the implemented privacy framing nudge conveys visibly and textually a personal message of loss. Messages of loss are generally unpleasant to receive and cognitively closely linked to negative emotions. Yet, individuals who are exposed to this stimulus may be affected in their emotional state. Individuals exposed to the privacy nudge in the experiment may feel upset, irritable or even hostile. This leads to the following hypotheses:

H6: Providing a privacy framing nudge in a digital work environment influences negative emotions of individuals.

3.2. Role of Emotions and Threat on Information Disclosure

Negative emotions can signal to individuals that a certain threat or risk exists in a situation. As a result, individuals are willing to avoid or actively control this situation [28]. Neurological research shows that negative emotions have a direct connection with brain structures [19]. When individuals feel negative emotions, their attention changes from being goal directed to being stimulus driven; the stimulus receives the human's full attention [19]. *Attentional control theory* (ACT) explains that when the processing capacity of the working memory is reduced, individuals can no longer control their attention. However, they are concentrating principally on the stimuli that trigger negative emotions. ACT shows that negative emotions reduce attentional control [19]. With the implemented privacy nudges, individuals perceive a higher risk of their own safety. Yet, individuals react accordingly by avoiding the potential negative consequences and disclose less information. Therefore, we hypothesize:

H7: Users' negative emotions negatively influence users' intention to disclose personal information.

The construct *threat* includes perceived threat severity and vulnerability. The perceived threat severity determines how serious the threat is to individuals and the perceived threat vulnerability determines how susceptible individuals are to the threat [21, 23]. If users perceive their privacy as threatened by the implemented privacy nudges, the risk factor increases (see privacy calculus). Thus, this promotes concerns about the misuse of the private information on the working platform as well as hindering the intention to disclose personal information. Thus, we hypothesize the following:

H8: Users' perceived threat (vulnerability and severity) negatively influences users` intention to disclose personal information.

Furthermore, we believe that perceived threat triggers negative emotions in individuals because they perceive the situation as personally dangerous and unpleasant. Individuals usually change their attentiveness to the stimuli that trigger negative emotions (ACT; [19]). The stimulus is therefore the privacy social or framing nudge that warns against revealing too much personal information. Therefore, we hypothesize:

H9: Users' perceived threat of privacy (vulnerability and severity) positively influences users' negative emotions.

The motivation of individuals to show a certain action depends on situational incentives, personal preferences, and their interaction [35]. The motivational tendency leads to a behavioral intention (character of an intention to act). The behavioral intention is thus a transition from the motivation phase of consideration to the volition phase of planning and action [35]. The intention to act, according to the action motivation, is a prerequisite for individuals to implement a certain action or decision. In the conducted experiment we assume that a positive relation between behavioral intention and actual behavior exists. Thus, we hypothesize the following:

H10: Users' intention to disclose personal information positively influences users' behavior to disclose personal information.

The research model in Figure 1 summarizes the deduced hypotheses.

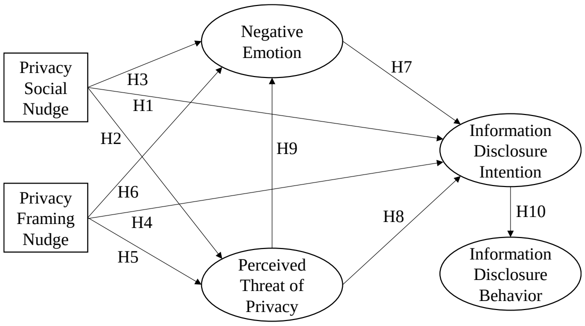

Negative Emotion
Privacy Social Nudge
H3
H1
H7
H2
H9
Information Disclosure Intention
H6
Privacy Framing Nudge
H4
H8
H10
H5
Perceived Threat of Privacy
Information Disclosure Behavior

Figure 1. Research Model

4. Research Design and Method

As we investigate the information disclosure behavior of individuals, the research method of an experiment is appropriate to show the cause–effect relationships. In addition to direct behavior, we explored the cognitive and emotional variables through an individual self-report by collecting data on the latent variables described in the research model.

4.1. Online Experiment Design

The online experiment is based on a multi-factor 2x2 *between-subject design*. This experiment contains two independent manipulation variables. A privacy nudge in the form of a social nudge and a framing nudge. The control group (CG) did not receive either of the two privacy nudges in the experiment. The treatment group 1 (TG1) received the social nudge and treatment group 2 (TG2) the framing nudge. Treatment group 3 (TG3) was exposed to the social as well as the framing nudge. We implemented three *pretest phases*. In each of them, we verified whether the online experiment and the survey fulfill the quality criteria and manipulation requirements.

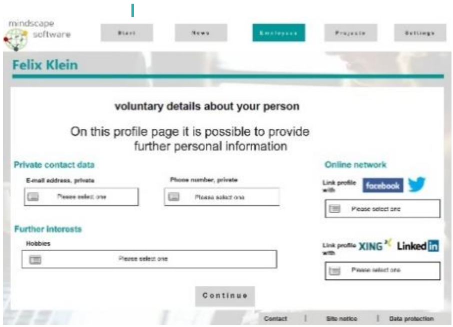
4.2. Participants

In total, the sample consists of 223 participants. With regard to gender, the sample comprises 145 female and 75 male participants. Two individuals answered divers to the question of gender and one participant did not want to answer this question. In the study, the majority of respondents (175 in total) were aged between 21 and 30. The youngest participant in the online study was 17 years old and the oldest 66 years old. With regard to the current profession, 113 respondents stated that they were students and 87 respondents indicated that they were employees. The sample essentially comprises the highly educated female generation Y (20-30 years old) who are students or employed. This generation has grown up with the technical innovations and has digital know-how. In addition, the growing digital work life and challenges of informational disclosure concerns them [6].

4.3. Experimental Procedure

The procedure of the online experiment looks as follows: On the welcome page we informed the respondents about the study initiator, the overall purpose, topic, and anonymity assurance. Next, we introduced the participants to the content of the online study in detail. The respondents were told to imagine that they are employees of the company "Kleimberg", which wants to use a new digital work system to improve communication, networking, and project work. We enquired the respondents to test the registration process of the digital work platform and to create their own employee profile. During the whole online experiment, the respondents act as the employee Felix Klein. They should fill out the employee profile as if it was their own. However, for ethical reasons we did not take personal data from the participants. Instead they used the data of Felix Klein. On the next two pages the participants had to generate a new account and saw visually and with short explanations the purpose of the platform.

Afterwards, the respondents created their employee profile. First, they provide business information like their business contact details and skills. Second, depending on which experimental group the software assigned the respondents to, they saw a privacy nudge, both or none of them. Third, the respondents could enter further and more personal as well as sensitive information about themselves, e.g., their private e-mail address, telephone number, and links to privately used online networks. After the respondents decided to (not) disclose voluntary information, we informed the respondents that they had successfully completed the process of the employee profile. We asked them to complete the online survey in the next step. Figure 2 presents a screenshot of the digital work system Mindscape.



Felix Klein

voluntary details about your person

On this profile page it is possible to provide further personal information

Private contact data

E-mail address, private: Please select one

Phone number, private: Please select one

Further interests

Hobbies: Please select one

Online network

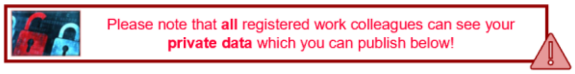
Link profile with facebook / Twitter: Please select one

Link profile with XING / LinkedIn: Please select one

Figure 2. Screenshot of Mindscape

4.4. Design of the Experimental Manipulation

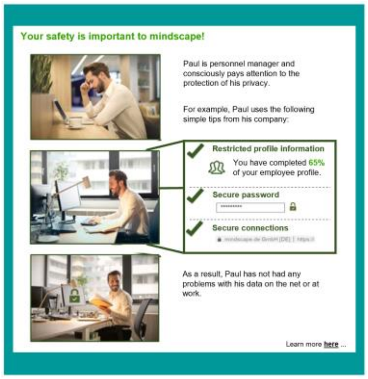
The framing nudge contained a statement (Figure 3). We formulated the statement in such a way that participants understood it as an indication of threat and loss of their privacy by disclosing personal information. Therefore, it adopts an emotional character and addresses the heuristic of loss aversion. We highlighted expressive words such as “all” and “private data” in bold to strengthen the perceived threat. The use of red colors, a flashing box and a pictorial warning should make the respondents unambiguously aware that the information they obtain to read is important and threatening. Referring to the definition of framing, the framing nudge in the experiment represents a negative frame in both visual and textual design.



Please note that **all** registered work colleagues can see your **private data** which you can publish below!

Figure 3. Privacy Framing Nudge

The social nudge explains and shows how to protect personal information and to behave securely (Figure 4). The respondents should learn what methods they could use to protect their own privacy on a digital work platform and that these methods are simple, successful, and easy to implement. In order to make the social nudge as convincing and effective as possible, we additionally used three principles of the psychology of persuasion according to Cialdini [11]. We used the principle of liking, authority, and social proof [11]. Furthermore, we paid attention to a professional and realistic visual presentation and provided textually strengthening and confident messages.



Your safety is important to mindscape!

Paul is personnel manager and consciously pays attention to the protection of his privacy.

For example, Paul uses the following simple tips from his company:

✓ Restricted profile information

You have completed 65% of your employee profile.

✓ Secure password

✓ Secure connections

As a result, Paul has not had any problems with his data on the net or at work.

Learn more here ...

Figure 4. Privacy Social Nudge

4.5. Common Method Variances

Common method variances that are caused by the measurement method rather than the construct measures were also taken into account [32]. To control these biases, we made several procedural remedies. To ensure a psychological separation of measurement, we did not reveal the purpose of the survey and provided a cover story [32]. In order to control socially desirable responses, we assured that there were no wrong answers and that the respondents answered questions as honestly as possible [32]. Regarding the statistical remedies, we conducted the Harmann’s Single Factor Test [32]. We performed an exploratory factor analysis with all model indicators and examined the unrotated factor solution. Since more than one factor emerged, the first factor does not account for the majority of covariance among the measures. We assume that these kinds of method errors play a rather minor role in the results of the online study [32].

4.6. Instrument Development

For the collection of the cognitive and emotion variables from the research model, we created an online survey. The survey comprises three sections. In the first section, we enquired four questions about the online experiment. We were able to test whether the respondents had carried out the online experiment conscientiously and attentively. In the second section of the online survey, we collected the single questionnaire constructs from the research model (Table 3). We measured the individuals’ perception of emotions when they were asked to disclose personal information in the online experiment. For this evaluation, we used the negative emotion items of the measuring instrument PANAS, which comprises the specific affect hostility according to PANAS-X [45]. The three items hostile, irritable, and upset were used for our negative emotions in the paper. Furthermore, we took well-established questionnaire constructs from the IS literature in the context of information security behavior and digital/privacy nudging.

Table 3. Latent Constructs and Sources

Latent Construct	Literature Source	Latent Construct Type	Sub-Construct	Sub-Construct Type
Information Disclosure Intention	Wakefield (2013)	Reflective		
Perceived Threat of Privacy	Johnston and Warkentin (2010)	Formative	Threat Vulnerability	Reflective
			Threat Severity	Reflective
Negative Emotions	Breyer and Bluemke (2016)	Reflective		

In the third and last section of the online survey, we enquired sociodemographic data as well as questions on the use of digital work systems and the usual willingness to provide personal information.

4.7. Statistical Analysis Methods

To evaluate the proposed research model, we used structural equation modeling (SEM) with the variance-based partial least squares (PLS) approach [10]. PLS-SEM is a causal modeling approach aimed at maximizing the explained variance of the dependent latent constructs and is a suitable method for research objectives aimed at predicting target constructs and theory development. SmartPLS 3.28 was used as an analysis tool [16] as well as SPSS 25 statistics.

5. Results

5.1. Analysis of Variance

A two-factorial analysis of variance (ANOVA) was used to examine whether the nudges influence information disclosure behavior. As Levene's F-test revealed that the homogeneity of variance assumption was not met (p = 0.001), we used Welch's F-test. An alpha level of 0.05 was used for all subsequent analysis. Post hoc comparisons, using the Games–Howell post hoc procedure, were conducted to determine which nudges' means differed significantly. As manipulation checks, we performed independent samples t-tests, indicating that both nudges affected participants' perceptions and behavior.

The results in Table 4 indicate that both nudges influence the information disclosure behavior of individuals. The privacy framing nudge (M = 1.81, SD = 1.18) had a significantly higher effect in reducing information disclosure than the privacy social nudge (M = 2.03, SD = 1.64). Both nudges together showed the highest effect (M = 1.79, SD = 1.36).

Table 4. ANOVA and Post Hoc Comparison Results

		Group Size	**Information Disclosure**	**Post Hoc Comparisons** Mean Differences ($X_i – X_j$)		
Group	**Treatment**	**N**	**Mean (SD)**	**TG1**	**TG2**	**TG3**
CG	--	54	2.53 (1.71)	0.50	0.72*	0.74*
TG 1	Privacy Social Nudge	55	2.03 (1.64)		0.22	0.24
TG 2	Privacy Framing Nudge	59	1.81 (1.18)			0.02
TG 3	Both Nudges	54	1.79 (1.36)			

Note: ANOVA; F (3; 138.99) = 3.14, p = 0.027; * p<0.05.

5.2. Measurement Models

The evaluation of the model followed a two-step process [16, 17]. First, we evaluated the measurement models. Second, we evaluated the inner model and the structural relationships [18].

Table 5. Quality Criteria of Constructs

Construct Information	**Indicator**	**Loading**	**Composite Reliability**	**Average Variance Extracted**
Information Disclosure Intention	Intent1	0.958	0.977	0.913
	Intent2	0.974		
	Intent3	0.943		
	Intent4	0.947		
Threat Severity	Sev1	0.923	0.954	0.873
	Sev2	0.947		
	Sev3	0.933		
Threat Vulnerability	Vul1	0.930	0.933	0.822
	Vul2	0.908		
	Vul3	0.881		
Negative Emotions	NE_upset	0.905	0.875	0.701
	NE_hostile	0.772		
	NE_irritable	0.830		

The quality criteria of the outer model are reported in Table 5. We measured indicator reliability with the standardized indicator loadings. All indicators load above the minimum value of 0.70. Internal consistency of the latent variables was indicated by the composite reliability of all constructs [17]. Values above the threshold of 0.70 show that the composite reliability is acceptable and thus substantiates the internal consistency of the latent variables [3]. We measured convergent validity using the average variance extracted, indicating the variance of a latent construct that is explained by the related indicators [3].

In the following, we assessed the discriminant validity with the Fornell–Larcker Criterion [15] as well as with the heterotrait–monotrait ratio (HTMT) and the heterotrait–monotrait inference criteria ($\text{HTMT}_{\text{inference}}$; [19]). The analysis in Table 6 shows that discriminant validity through consideration of the Fornell–Larcker Criterion and the conservative HTMT_{85} measure (indicated through all HTMT measures under 0.85) is established. Also, $\text{HTMT}_{\text{inference}}$ values are all significantly below the threshold of 1.

Moreover, the results of the cross-loadings indicate that all indicators load the highest on their own [10]. Thus, the evaluation of the measurement models shows that they fulfill the desired quality criteria.

Table 6. Discriminant Validity of Constructs*

Construct	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Framing Nudge (1)	1.000						
Information Disclosure Behavior (2)	-0.109 (0.109)	1.000					
Information Disclosure Intention (3)	0.006 (0.008)	0.514 (0.522)	0.955				
Threat Severity (4)	0.053 (0.056)	-0.175 (0.181)	-0.426 (0.450)	0.934			
Threat Vulnerability (5)	0.081 0.086	-0.263 0.280	-0.424 0.456	0.787 0.863	0.906		
Negative Emotions (6)	0.164 (0.179)	-0.161 (0.176)	-0.243 (0.276)	0.216 (0.248)	0.229 (0.267)	0.837	
Social Nudge (7)	-0.027 (0.027)	-0.065 (0.065)	-0.130 (0.132)	0.203 (0.210)	0.101 (0.106)	0.124 (0.135)	1.000

* Values on the diagonal represent the square root of the average variance captured and all other elements represent the correlations with the latent variables. The calculation was omitted for the manifest and binary-coded variables of the experimental manipulations (NA). Values in brackets indicate the HTMT criterion, where 0.85 is the conservative limit. Therefore, the HTMT_{85} criterion is fulfilled to satisfaction and confirms the discriminant validity.

The results of the key indicators in Table 7 show that the key guidelines are fulfilled.

Table 7. Quality Criteria of Formative Construct

Construct	Indicator	VIF	Factor Weights	t-value	Factor Loadings
Perceived Threat of Privacy	Threat Severity	2.626	0.639	2.871	0.966
	Threat Vulnerability	2.626	0.419	1.787	0.919

Although the indicator of threat vulnerability was not significant and showed a factor loading below 0.5, we did not drop the indicator because of the well-grounded theory of perceived threat [23].

5.3. Structural Model

The results of the structural model consist of path coefficients, the explained variance, significance levels, the effect sizes, and the predictive relevance [17]. We applied the path weighting scheme PLS algorithm with 300 iterations to the model evaluation, and we used the bootstrapping procedure with 5000 samples to determine the significance levels. The respective results of the structural model are depicted in Figure 5.

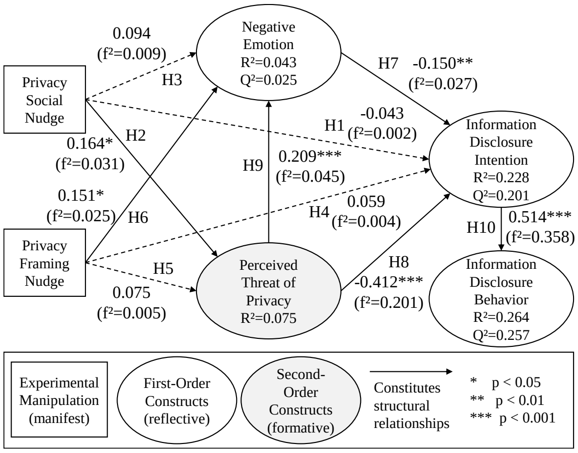

Privacy Social Nudge
Privacy Framing Nudge
Negative Emotion R^2=0.043 Q^2=0.025
Perceived Threat of Privacy R^2=0.075
Information Disclosure Intention R^2=0.228 Q^2=0.201
Information Disclosure Behavior R^2=0.264 Q^2=0.257
0.094 (f^2=0.009) H3
H2 0.164* (f^2=0.031)
0.151* (f^2=0.025) H6
H5 0.075 (f^2=0.005)
H1 -0.043 (f^2=0.002)
H4 0.059 (f^2=0.004)
H7 -0.150** (f^2=0.027)
H9 0.209*** (f^2=0.045)
H8 -0.412*** (f^2=0.201)
H10 0.514*** (f^2=0.358)
Experimental Manipulation (manifest)
First-Order Constructs (reflective)
Second-Order Constructs (formative)
Constitutes structural relationships
* p < 0.05
** p < 0.01
*** p < 0.001

Figure 5. Results of Research Model

The results of the model indicate that the privacy social nudge does not directly influence the intention to disclose personal information (H1, $\beta = -0.043$, $p > 0.05$) and negative emotions (H3, $\beta = 0.094$, $p > 0.05$). Yet, the privacy social nudge shows a significant effect on perceived threat (H2, $\beta = 0.164$, $p < 0.05$). The privacy framing nudge shows no direct effect on information disclosure intention (H4, $\beta = 0.059$, $p > 0.05$) and on perceived threat (H5, $\beta = 0.075$, $p > 0.05$). However, the privacy framing nudge shows a positive significant effect on negative emotions (H6, $\beta = 0.151$, $p < 0.05$). The relationships between the construct's negative emotions (H7, $\beta = -0.150$, $p < 0.001$), perceived threat of privacy (H8, $\beta = -0.412$, $p < 0.001$; H9, $\beta = 0.209$, $p < 0.001$), and information disclosure intention are significant. Furthermore, information disclosure intention has a positive and highly significant effect on information disclosure behavior (H10, $\beta = 0.514$, $p < 0.001$).

Regarding the explained variance (R^2), the constructs information disclosure behavior ($R^2 = 0.264$) and information disclosure intention ($R^2 = 0.228$) show a small proportion of explained variance. The two constructs negative emotions ($R^2 = 0.043$) and perceived threat ($R^2 = 0.075$) with R^2 below 0.19 show only a small proportion of explained variance.

The measurement of the prognosis relevance Q^2 determines the prognostic capability of the model. Since Q^2 is above the threshold value of 0 for all endogenous reflective constructs, the predictive relevance of this structural model is given. The results show a moderate predictive relevance for the constructs information disclosure behavior ($Q^2 = 0.257$) and information disclosure intention ($Q^2 = 0.201$). The construct negative emotions ($Q^2 = 0.025$) shows a small predictive relevance.

6. Discussion and Contributions

The results of the experiment indicate that both privacy nudges influence information disclosure behavior and individuals disclose less personal information. Even though the results are weak, we can see an influence of nudges as subtle mechanisms. In the future, more sensible designs of nudges can increase the effects. However, all treatment groups provided less personal information than the control group.

Both privacy nudges show no direct effect on information disclosure intention. Rather, indirect effects are identified. The factors driving privacy nudges are the perceived threat to individuals' privacy and negative emotions. Triggering these constructs through privacy nudges can drive disclosure behavior. The social nudge affected threat severity and vulnerability, which in turn trigger negative emotions. Consequently, individuals felt upset, hostile, and irritable.

Emotions have a disruptive character and influence the perception in decision-making situations. In regards to *attentional control theory* (ACT), individuals generally concentrate on the stimuli that trigger negative emotions [19]. ACT shows that negative emotions reduce attentional control. In security and privacy-related decisions, a rational evaluation of the *privacy calculus* can be negatively affected by negative emotions. Thus, privacy nudges can reduce individual's information disclosure but also minimize the informational self-determination, exposing the dark side of the implemented privacy nudges.

With this research we are enriching the discussion about what drives privacy nudge effectiveness in digital work environments, what is being perceived as a threat to privacy, and negative emotions that influence information disclosure behavior.

7. Limitations and Future Research

Empirical studies suffer from certain limitations. In the experiment, we transferred the respondents to a digital work environment that was as realistic as possible in the form of a digital work platform. They were supposed to imagine themselves in a particular role and situation (vignette), to act accordingly, and to make decisions. These types of experiments show limitations in external validity. Thus, a field study should test to what extent the findings of our study can be transferred to other or real situations in digital work environments.

The goal of our study was to understand how privacy framing nudges and privacy social nudges influence information disclosure behavior in digital work environments. The results of our experiment indicate that the implemented privacy nudges influence negative emotions and perceived threat, thus reducing the intention to disclose information. Overall, more research should focus on privacy nudge designs that do not spark negative emotions and ensure its effectiveness in protecting individuals' privacy in digital work environments.

8. Acknowledgements

The research presented in this paper was funded by the German Federal Ministry of Education and Research in the context of the project Nudger (www.nudger.de), Grant No. 16KIS0890K.

9. References

[1] Acquisti, A., Sleeper, M., Wang, Y., Wilson, S., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., Leon, P. G., Sadeh, N., and Schaub, F. 2017. Nudges for Privacy and Security. *ACM Computing Surveys* 50, 3, 44:1 - 44:41.

[2] Bagozzi, R. P., Gopinath, M., and Nyer, P. U. 1999. The Role of Emotions in Marketing. *Journal of the Academy of Marketing Science* 27, 2, 184–206.

[3] Bagozzi, R. P. and Yi, Y. 1988. On the evaluation of structural equation models. *Journal of the Academy of Marketing Science* 16, 1, 74–94.

[4] Barev, T. J. and Janson, A., Eds. 2019. *Towards an Integrative Understanding of Privacy Nudging – Systematic Review and Research Agenda*. *Pre-ICIS Workshop on HCI Research in MIS*, Munich. Germany.

[5] Barth, S. and Jong, M. D.T. de. 2017. The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics* 34, 7, 1038–1058.

[6] Bencsik, A., Juhász, T., Horváth-Csikós, G., Széchenyi István University in Győr, and Szent István University in Gödöllő. 2016. Y and Z Generations at Workplaces. Journal of Competitiveness, 6, 3, 90-106.

[7] Bradley, M. M. and Lang, P. J. 2007. Emotion and Motivation. In *Handbook of psychophysiology*, J. T. Cacioppo, L. G. Tassinary and G. G. Berntson, Eds. Cambridge University Press, Cambridge [England], New York, 581–607.

[8] Breyer, B. and Bluemke, M. 2016. *Deutsche Version der Positive and Negative Affect Schedule PANAS (GESIS Panel)*.

[19] Caraban, A., Karapanos, E., Gonçalves, D., and Campos, P. 2019. 23 Ways to Nudge. *Proceedings of the 2019 CHI Conference*. ACM Press, New York, New York, USA, 1–15.

[10] Chin, W. W. 1998. Commentary: Issues and Opinion on Structural Equation Modeling. *MIS Quarterly* 22, 1, 7–16.

[11] Cialdini, R. B. 2011. *Influence. The Psychology of Persuasion*. Collins, New York, NY.

[12] Cialdini, R. B. and Goldstein, N. J. 2004. Social influence: compliance and conformity. *Annual review of psychology* 55, 591–621.

[13] Collier, C. A. 2018. Nudge Theory in Information Systems Research A Comprehensive Systematic Review of the Literature. *Academy of Management Proceedings* 2018, 1, 18642:1 - 18642:40.

[14] Finucane, M. L., Alhakami, A., Slovic, P., and Johnson, S. M. 2000. The affect heuristic in judgments of risks and benefits. *Journal of Behavioral Decision Making* 13, 1, 1–17.

[15] Fornell, C. and Larcker, D. F. 1981. Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research* 18, 1, 39–50.

[16] Hair, J. F., Ringle, C. M., and Sarstedt, M. 2011. PLS-SEM: Indeed a Silver Bullet. *Journal of Marketing Theory and Practice* 19, 2, 139–152.

[17] Hair, J. F., Sarstedt, M., Ringle, C. M., and Mena, J. A. 2012. An assessment of the use of partial least squares structural equation modeling in marketing research. *Journal of the Academy of Marketing Science* 40, 3, 414–433.

[18] Henseler, J., Ringle, C. M., and Sarstedt, M. 2015. A new criterion for assessing discriminant validity in variance-based structural equation modeling. *JAMS* 43, 1, 115–135.

[19] Hibbeln, M., Jenkins, J. L., Schneider, C., Valacich, J. S., and Weinmann, M. 2017. How Is Your User Feeling? Inferring Emotion Through Human-Computer interaction Devices. *MIS Quarterly* 41, 1, 1–21.

[20] IDG Research Services. 2018. *Welche Risiken und Nachteile bergen die neuen Arbeitsplatz- und Mobilitätskonzepte für Sie als Arbeitnehmer?*

[21] Ifinedo, P. 2012. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security* 31, 1, 83–95.

[22] Jiang, H.; Siponen, M. and Tsohou, A. 2019. A field experiment for understanding the unintended impact of internet monitoring on employees: policy satisfaction, organizational citizenship behavior and work motivation. *Proceedings of the 27th ECIS*, Stockholm & Uppsala, Sweden, June 8-14, 2019.

[23] Johnston, A. C. and Warkentin, M. 2010. Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly* 34, 3, 549–566.

[24] Joinson, A. N. 2001. Self-disclosure in computer-mediated communication: The role of self-awareness and visual anonymity. *Eur. J. Soc. Psychol.* 31, 2, 177–192.

[25] Joinson, A. N. and Paine, C. B. 2009. Self-disclosure, privacy and the Internet. In *The Oxford handbook of Internet psychology*, A. N. Joinson, K. Y. A. MacKenna, T. Postmes and U.-D. Reips, Eds. Oxford University Press, New York, 237–525.

[26] Kahneman, D. and Tversky, A. 1979. Prospect Theory: An Analysis of Decision under Risk. *Econometrica* 47, 2, 263.

[27] Li, H., Sarathy, R., and Xu, H. 2011. The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. *Decision Support Systems* 51, 3, 434–445.

[28] Li, H., Sarathy, R., and Zhang, J. 2008. The Role of Emotions in Shaping Consumers' Privacy Beliefs about Unfamiliar Online Vendors. *Journal of Information Privacy and Security* 4, 3, 36–62.

[29] Lupton, D. 2013. Risk and emotion: towards an alternative theoretical perspective. *Health, Risk & Society* 15, 8, 634–647.

[30] Mees, U. 2006. Zum Forschungsstand der Emotionspsychologie - eine Skizze. In *Emotionen und Sozialtheorie. Disziplinäre Ansätze*, R. Schützeichel, Ed. Campus-Verl., Frankfurt/Main, 104–123.

[31] Mirsch, T., Lehrer, C., and Jung, R. 2017. Digital Nudging: Altering User Behavior in Digital Environments. *13th International Conference on Wirtschaftsinformatik,*, St. Gallen, 634–648.

[32] Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., and Podsakoff, N. P. 2003. Common method biases in behavioral research: a critical review of the literature and recommended remedies. *The Journal of applied psychology* 88, 5, 879–903.

[33] Schöbel, S., Barev, Torben Jan, Janson, A., Hupfeld, F., and Leimeister, J. M. 2020. Understanding User Preferences of Digital Privacy Nudges – A Best-Worst Scaling Approach. In *Hawaii International Conference on System Sciences Proceedings (HICSS)*.

[34] Schouten, A. P., Valkenburg, P. M., and Peter, J. 2007. Precursors and Underlying Processes of Adolescents' Online Self-Disclosure: Developing and Testing an "Internet-Attribute-Perception" Model. *Media Psychology* 10, 2, 292–315.

[35] Schwarzer, R. 2008. Modeling Health Behavior Change: How to Predict and Modify the Adoption and Maintenance of Health Behaviors. *Applied Psychology* 57, 1, 1–29.

[36] Sherif, K. and Jewisimi, O. (2018): Electronic Performance Monitoring Friend or Foe: Empowering Employees through Data Analytics. *AMCIS 2018 Proceedings*.

[37] Slovic, P., Finucane, M. L., Peters, E., and MacGregor, D. G. 2004. Risk as analysis and risk as feelings: some thoughts about affect, reason, risk, and rationality. *Risk analysis : an official publication of the Society for Risk Analysis* 24, 2, 311–322.

[38] Smith, Dinev, and Xu. 2011. Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly* 35, 4, 989–1016.

[39] Sunstein, C. R. 2017. Nudges that fail. *Behav. Public Policy* 1, 1, 4–25.

[40] Thaler, R. H. and Sunstein, C. R. 2009. *Nudge - Improving decisions about health, wealth and happiness*. Penguin Books, London.

[41] Tidwell, L. C. and Walther, J. B. 2002. Computer-Mediated Communication Effects on Disclosure, Impressions, and Interpersonal EvaluationsGetting to Know One Another a Bit at a Time. *Hum Commun Res* 28, 3, 317–348.

[42] Wakefield, R. 2013. The influence of user affect in online information disclosure. *The Journal of Strategic Information Systems* 22, 2, 157–174.

[43] Wang, C., Zhang, X., and Hann, I.-H. 2018. Socially Nudged: A Quasi-Experimental Study of Friends' Social Influence in Online Product Ratings. *Information Systems Research* 29, 3, 641–655.

[44] Wang, Y., Leon, P. G., Acquisti, A., Cranor, L. F., Forget, A., and Sadeh, N. 2014. A field trial of privacy nudges for facebook. *Proceedings of the 32nd annual*, Toronto, ON, Canada, 2367–2376.

[45] Watson, D. and Clark, L. A. 1994. *The PANAS-X: Manual for the Positive and Negative Affect Schedule - Expanded Form*, The University of Iowa.

[46] Weinmann, M., Schneider, C., and Vom Brocke, J. 2016. Digital Nudging. *Business & Information Systems Engineering* 58, 6, 433–436.

[47] Westin, A. F. 2003. Social and Political Dimensions of Privacy. *Journal of Social Issues* 59, 2, 431–453.

[48] Wirth, J., Maier, C., Laumer, S., and Weitzel, T. 2007. Understanding Privacy Threat Appraisal and Coping Appraisal Through Mindfulness. In *ICIS 2007 Proceedings*, South Korea, 1–11.

[49] Zhang, B. and Xu, H. 2016. Privacy Nudges for Mobile Applications: Effects on the Creepiness Emotion and Privacy Attitudes. In *Proceedings of the 19th ACM CSCW '16*. ACM Press, New York, New York, USA, 1674–1688.