Privacy Protection Behaviors from a New Angle: Exploratory Analysis on a Russian Sample

Denis Obrezkov
denis.obrezkov@tib.eu
TIB – Leibniz Information Centre for Science and Technology
Hannover, Germany

ABSTRACT

To understand why people engage in privacy protection behaviors on the Internet, multiple researchers tried to reveal the underlying factors of the phenomenon. The results were ambiguous. Identifying privacy concerns as a mediating construct, some researchers were able to establish its influence on protection behaviors, others were not. In addition, the structure of hypothesized factors affecting privacy concerns differed from work to work. This paper aims to shed light on the inconsistencies in the previous research. To achieve this, we perform an exploratory analysis of factors affecting privacy protection behavior on the Internet. We conduct a survey on a Russian sample ($N = 228$) and perform the analysis using a technique of structural equation modeling. Our results suggest the following: (a) privacy protection behavior is a multidimensional construct, with each behavior type being affected by its own set of factors; (b) privacy concerns might have a dynamic structure, that is dependent on the context and the environment of the target population. Given these findings, we conclude that future research should consider a specific type of protection behavior together with characteristics of the target population and to refrain from generalization of the results from other domains or protection behavior types.

1 INTRODUCTION

Individuals always seek a balance when they interact with others. The pushing need for social communication makes them disclose personal information. At the same time, to avoid the threat of being manipulated by those who know their secrets, a person aims to control the amount of information shared by them [4, 49]. While this type of control is often referred to as privacy [4], the Internet exhibits the phenomenon in a new light, posing unexpected challenges to researchers.

The extensive use of digitized personal data in the modern economies led to the need to rethink privacy [33]. On the one side, users started to utilize a variety of online services, such as e-commerce, banking, or gaming [21]. Often, those services required users to provide them with personal information. On the other side, companies started to collect more personal data to make better business decisions. Time has shown that the data could be made available to third parties without individuals' consent [11, 25]. Unsurprisingly, these trends made some users concerned about sharing data in the Internet [17].

To obtain the understanding of why individuals share information in the Internet, researchers designed a number of hypotheses on factors affecting the disclosure and protection behaviors. Among others it was suggested that individuals' privacy concerns are the antecedents of the behaviors of interest [17]. Surprisingly, that was not always the case. Researchers faced what is known as the *privacy paradox*, a situation when users' stated privacy concerns do not sufficiently explain their privacy protection behavior [40]. However, the evidence on the aforementioned phenomenon is manifold (see [15] for the overview).

The privacy paradox can be viewed as a manifestation of *privacy calculus*. The latter refers to the individuals making a decision on information disclosure based on the assessment of the corresponding risks and benefits [13]. In that case privacy concerns can be viewed as an operationalization of costs, while rewards from the information disclosure might be considered as an operationalization of benefits [46]. Thereby, in the light of privacy calculus the "paradoxical" behavior is viewed as a result of cost-benefit assessment. In a similar fashion, Baruh et al. point to a moderate or small effect of privacy concerns on resulting behaviors and intentions in their meta-review [7]. Interestingly, the authors also observed different correlations between privacy concerns and behaviors in different domains (e.g., revealing the privacy paradox only in the context of social networks). Given that, we conclude that there is a certain gap in the understanding of different privacy behaviors and their antecedents.

One way to deeper understand the problem is to investigate it in different contexts. For instance, existing research on privacy behaviors examined the phenomenon in different nations, revealing new insights from distinct populations [37, 38]. In our study we followed a similar approach and chose a specific population for the investigation: adult Russian Internet users. This choice is motivated by two factors. First, the Russian population is relatively underrepresented in privacy studies. Previous research investigated samples from North America [19, 29, 34], Western Europe [26, 37, 55], and some Asian countries [3, 38], while little research was done on samples from Eastern Europe. Second, the Russian government is known for a wide range of established censorship and surveillance measures [20, 53]. Additionally, the Russian population experiences risks of the conscription and mobilization due to the ongoing war with Ukraine. Thereby, the Russian population might be exposed to different threats and might bring new light on the phenomenon of privacy behavior.

Proceedings on Privacy Enhancing Technologies 2024(4), 1–13

https://doi.org/10.56553/popets-2024-0001

RQ: "What factors do underlie privacy protection behaviors in the population of Russian Internet users?"

This paper is structured as follows. In the next section we identify the gaps and inconsistencies in the literature on privacy concerns and privacy protection behaviors. In section 3, we describe how we approached the problem by detailing our method. Section 4 presents descriptive statistics and the results of our analysis. Section 5 discusses the limitations of our work and embeds our findings into the existing research. Finally, we conclude our paper with a summary of the obtained results.

2 BACKGROUND

In this section we review several constructs related to the perception of privacy. We discuss how existing works investigate them and identify the gaps in the domain knowledge.

Privacy protection behavior. The notion of privacy protection is closely associated with the protection behavior. Altman suggests that people utilize a number of behavioral mechanisms to achieve their desired level of privacy [4]. The author points to the dynamic nature of this process: a person adjusts boundaries to their self and pays physical and psychological costs.

The protection behavior is investigated from several perspectives. Roger's Protection Motivation Theory (PMT) posits that the intention to adopt a protection behavior is influenced by thee factors: probability of threat occurrence, response efficacy, and outcome severity [42]. In addition, the revised PMT introduces an additional factor of self-efficacy [32]. The latter is adopted from Bandura's work [5] and represents a person's beliefs on their ability to successfully perform actions necessary to achieve a certain goal.

Utilizing protection technologies is not the only type of protection behavior. Liang and Xue provides researchers with another perspective and introduce Technology Threat Avoidance Theory (TTAT)[30]. The authors state that the threat avoidance behavior is influenced by two factors: threat appraisal and coping appraisal. The former is referred to the assessment of the threat possibility by a person, and the latter reflects the person's evaluation of their threat mitigation capabilities. Additionally, the theory accounts for emotion-focused coping. The latter is likely to be induced when users feel that they have limited control over a situation.

In addition to the diversity of theoretical approaches, a variety of methods exist to measure privacy behavior. First, some researchers ask participants to indicate the degree of specific privacy protection technologies. Weinberger et al. asked respondents to agree or disagree with statements on the use of specific privacy protection measures [48]. Boerman et al. presented respondents with scales about the frequency of use of privacy protection technologies [8]. A binary scale was used by Mohamed and Ahmad to find out whether survey participants use any privacy measures [38]. Second, other researchers construct scales to measure privacy protection behavior. Youn constructed scales for three types of behavior: refusing to use a website, falsifying or providing incomplete information about themselves, seeking help of more experienced agents [54]. A number of similar factors constituted privacy behavior scales utilized by Adhikari and Panda [3]. Thereby, while some researchers measured the behavior as a single construct, others distinguished several types of protection behaviors.

H1. *Privacy protection behavior is a multidimensional construct.*

Privacy concerns. Privacy concerns are shown to be a prominent factor affecting protection behavior. Dinev and Hart explore the link between privacy concerns and an attitude to share personal information [18]. In a similar manner, Malhotra et al. investigate the influence of privacy concerns on the behavioral intention to share the information [34]. A number of empirical studies reveal the connection between privacy concerns and actual reported behaviors [3, 38, 55].

There are a number of works that investigate what constitutes privacy concerns. Smith et al. consider four contributing factors: collection, errors, unauthorized secondary use, and improper access [45]. The first factor represents the feeling of the overwhelming amount of collected data. The second refers to the lack of protection from deliberate and accidental errors in processed data. The third represents the concern of data utilization for secondary purposes without provided permission. The last factor refers to the access to collected data by unauthorized parties. Based on these hypotheses, Smith et al. develop and validate the Concern for Information Privacy (CFIP) scale [45] in the context of a protection behavior. Another approach is utilized by Xu et al. Avoiding privacy-protection behavior context, the authors investigate the formation of privacy concerns [52]. They find an empirical evidence of three constituents of privacy concerns: perception of instruction, perceived privacy risk, and perceived privacy control.

A certain discrepancy can be found in existing works that measure privacy concerns. First, there are different hypothesized structures of privacy concerns and their underlying factors. Zeissig et al. investigate the relation between privacy concerns and awareness and experience, while self-efficacy is considered in a direct relation with the resulting protection behavior [55]. In the work of Mohamed and Ahmad the factors of awareness and experience are not considered, while self-efficacy is investigated as an antecedent of privacy concerns [38]. Being structurally different, the proposed models demonstrate good fit to data. Second, the majority of works rely on similar theories (e.g. TTAT and TPB), rarely exploring additional possibilities. That results in a large part of a phenomenon being not investigated.

H2. *Privacy concerns are positively related to privacy protection behavior.*

Self-efficacy. The term self-efficacy refers to a human's belief in their ability to successfully perform a task [5]. According to Bandura, there are four sources of efficacy information: performance accomplishments, vicarious experience, verbal persuasion, emotional arousal [5]. An interesting phenomenon arises in the field of privacy protection. If a user experiences a privacy breach, thereby obtaining the evidence of their poor privacy protection performance, will the user exhibit a more prominent protection behavior, or will the experience lead to a lower self-efficacy inhibiting the behavior? Or, does the experience lead to higher privacy concerns as it is observed by Zeissig et al. [55]?

H3. *Previous privacy violation experience is positively related to privacy protection behavior.*

H4. *Previous privacy violation experience is negatively related to self-efficacy.*

H5. *Previous privacy violation experience is positively related to privacy concerns.*

Self-efficacy is often considered in privacy behavior research. It was found that self-efficacy was an influential factor in many types of protection behaviors. Crossler investigates the phenomenon with regard to the behavior of making back-ups [12]. Privacy behavior of older adults is considered in the work of Zeissig et al [55]. Woon et al. consider self-efficacy in the context of wireless security [51]. While the aforementioned works provide researchers with some evidence on the relationship between self-efficacy and protection behavior, it is not always the case. Larose and Rifon investigated the phenomenon in the context of personal information disclosures [27]. The authors were not able to find a direct link between self-efficacy and the disclosure behavior.

H6. *Self-efficacy is positively related to privacy protection behavior.*

It should be noted that the place of self-efficacy is not clear in privacy research. On the one hand, self-efficacy is often viewed as a factor affecting privacy behaviors indirectly, via privacy concerns as a mediating construct [3, 38]. On the other hand, a number of researchers consider self-efficacy a direct antecedent of protection behavior [12, 55]. Additionally, the link between the two constructs is not always found to be significant. This inconsistency leads us to the following hypothesis.

H7. *Self-efficacy is positively related to privacy concerns.*

Severity. According to PMT, severity is an important factor of the threat appraisal [42]. Perceived severity can be defined as individuals' belief in the seriousness of the threat if it succeeds [36]. The factor is shown to have a direct effect on both privacy behavior [8, 51] and privacy concerns [3]. At the same time, there is evidence on insignificance of the perceived severity on privacy behavior intention [28, 56].

H8. *Severity is positively related to privacy concerns.*

Vulnerability. PMT distinguishes vulnerability as another factor that positively affects threat appraisal process [42]. Perceived vulnerability refers to an individual's assessment of the probability of the threatening event occurrence [12]. As noted by Rogers there is an effect of the vulnerability on protection intentions [43]. The evidence from privacy behavior studies is not so unambiguous. Some researchers revealed a significant effect of vulnerability on privacy concerns [3] or protection behavior [28]. Others pointed to the absence of significant influence of the perceived probability of the event occurrence on protection behavior [8, 54] or behavioral intentions [56]. In addition, Crossler revealed a negative influence of perceived vulnerability on making-backups behavior [12].

H9. *Vulnerability is positively related to privacy concerns.*

Response efficacy. Response efficacy is defined as "an individual's confidence that a recommended behavior will prevent or mitigate the threatening security event" [12]. PMT considers it to be a part of coping appraisal [42]. The evidence on the relationship of the construct with security behavior is inconsistent. It was shown that response efficacy has a positive significant effect on password protection intentions [56] and on wireless network protection behavior [51]. The opposite is true for privacy concerns: the significant relation was missing in the context of social networks [3, 38].

H10. *Response efficacy is positively related to privacy concerns.*

H11. *Response efficacy is positively related to privacy protection behavior.*

Rewards. In the frame of PMT, rewards can be defined as expected benefits resulting from a behavior, associated with maladaptive response to the threat [43]. With regard to privacy, rewards are generally associated with the benefits from personal data disclosure [26, 54]. In addition, rewards are the cornerstone of "privacy calculus" — an assumption that consumers seek a tradeoff of costs and benefits of information disclosure during their decision making [19]. Existing research exhibits a certain degree of inconsistency. Youn reveals a significant relationship between perceived benefits and privacy concerns among young adolescents in social networks [54]. At the same time Adhikari and Panda find no influence from rewards on privacy concerns among Indian students in the same context of social networks [3]. Nevertheless the same factor was found to have a significant negative relationship with disclosure behaviors [26] and behavioral intentions [29].

H12. *Rewards are negatively related to privacy concerns.*

H13. *Rewards are negatively related to privacy protection behavior.*

Trust. Trust is shown to be a significant predictor of the information disclosure behavior in such domains as e-commerce [35] and health information management [6]. At the same time, the evidence on this relationship is not consistent. Norberg et al. find no significant influence of trust on consumers' disclosure behavior [40]. Dinev and Hart reveal a significant negative relationship between trust and the information disclosure attitude in the context of e-commerce [18]. Similarly, Zeissig et al. found a significant connection between trust and protection behavior on the Internet [55].

H14. *Trust is negatively related to privacy protection behavior.*

3 METHOD

Our exploratory work aims to address inconsistencies found in the existing research. To investigate them, we have formulated a number of hypotheses and designed a questionnaire. The questionnaire items were adopted from multiple sources. To filter out low effort responses we added four attention questions. The structural model was created to assess the hypotheses.

The study included two phases. First, we ran a pre-test with 23 participants to ensure a good quality of the questions. Second, we conducted a study on the crowdsourcing website Toloka[1] in

[1] https://toloka.ai

October-November 2023. We used the following criteria for participants: they should be among top 10% of the platform users, should have passed the platform's English proficiency test, and should have Russia as their country of residence. The respondents were compensated with 0.8$.

To analyze our data, we utilized the technique of structural equation modeling (SEM). On the first step, a researcher hypothesizes how a set of variables defines constructs (latent variables) together with the relationships between these constructs. On the next step, SEM tests to what degree data supports the theoretical model. In our work we use Covariance-Based SEM. In that case a sample variance-covariance matrix is compared to the variance-covariance matrix implied by the theoretical model. To estimate the parameters of the hypothesized theoretical model, we use a robust variant of a maximum likelihood estimator. Model fit is evaluated using indices listed in Table 6.

For the analysis we used the following software: python 3.10 (data cleaning), R 4.1.2 (analysis), lavaan 0.6-16 (structural equation modeling), psych 2.3 (factor analysis of the protection behavior).

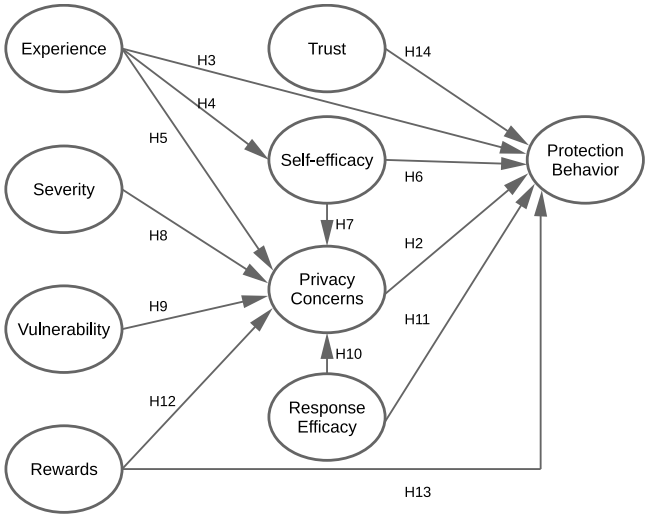


Figure 1: Structural model of factors affecting privacy protection behavior.

3.1 Ethics

Before conducting the study, we considered the ethical side of the research. We looked for opportunities to get ethical approval from our institution. At the time of the study design, our university did not have the institutional review board (IRB) for individual studies. Nevertheless, we followed best practices to ensure the high ethical standards of our research.

To design our study, we followed ethical principles outlined in the Menlo report [1]. First, we ensured that participants face minimal risk of harm. All questions measure attitudes towards general entities, e.g., websites, website owners, unspecified organizations. Second, we ensured compliance with Russian law and law enforcement practices. We did not include questions that ask about the use of VPN and traffic obfuscation technologies, since their use in Russia is condemned [2]. We also omitted questions that mention powerful entities, like the government or specific organizations. Third, we chose to not collect any information that might potentially reveal respondents' identity. Last, all participants were provided with an informed consent form; the participation was voluntarily.

3.2 Questionnaire Design

In our questionnaire we evaluate factors associated with privacy protection. To measure the privacy protection behavior, we adopted a set of questions from the previous research by Boerman et al [8]. It should be noted that we measured only a subset of protection behaviors. We excluded one question ("opt-out websites") from the original item set due to confusion among several respondents during the pre-test. For similar reasons, we refrained from including advanced PET software. Ethical concerns also led us to exclude items corresponding to VPN and traffic obfuscation software. (see Section 3.1). The resulting set of questions is listed in Table 1. The respondents were asked to indicate how often they perform these actions. The items were measured on the following five-point scale: "never", "rarely", "occasionally", "often", "very often".

To measure other factors, we adopted questions from several sources. We aimed to have at least three indicators per construct to avoid poor quality solutions [31]. To ensure content validity, we used items from existing scales. For the same reason, in most cases, each construct was loaded with items from a single source. The respondents were asked to rate each item on a 7-point scale ranging from "Strongly disagree" to "Strongly agree". To ensure the clarity of the survey questions, we conducted a pre-run study with 23 participants. We addressed the obtained feedback by removing or rephrasing poorly worded items. Additionally, we performed correlation analysis to remove conflicting items belonging to the same construct. To measure the construct of Privacy concern we decided not to use the IUIPC scale [34]. The latter implies an explicit second-order factorial structure (measuring control, awareness, collection as first-order factors) and is also known for not accounting for certain relationships, e.g., between privacy concerns and risk beliefs [9]. To eliminate the risk of the second-order factorial structure affecting the results of our structural equation modeling, we decided to measure the construct as a first-order factor and utilized items from three existing questionnaires [3, 38, 55]. The resulting set of the measurement items is presented in Table 2.

Our questionnaire was developed in English. Though our target audience is Russian Internet users, we found out that some privacy-related questions notably shift their meaning when translated. Thereby, to ease the comparison with similar works, we decided to conduct the survey in English. The implications of this decision will be discussed later.

3.3 Structural Model

To assess our hypotheses, we developed our research model (see Fig. 1). It incorporates nine latent constructs that were measured using corresponding items from Table 2. Additionally, the structural model exhibits hypothesized relationships between the constructs.

Table 1: Items that were used to measure privacy protection behavior (from Boerman et al. [8]).

Item name	Measurement item (type of the protection behavior)
PB1	using ad blocker
PB2	deleting cookies
PB3	deciding to refrain from visiting a website because it is only accessible when they accept cookies
PB4	declining to accept cookies when website offers the choice
PB5	using the private mode in their browser
PB6	deleting browser history
PB7	using the "Do Not Track" function in their browser
PB8	using special software in their browser (e.g., Ghostery or Privacy Badger) that makes it harder for companies to collect personal data
PB9	filling out wrong information about oneself (for instance, a fake name or wrong email address) when asked for such information

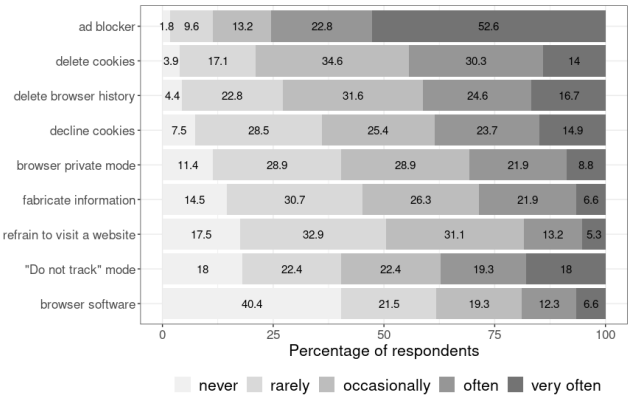


Figure 2: Frequency of privacy protection technologies use reported by the participants (the frequency groups might not sum up to 100 percents due to rounding errors).

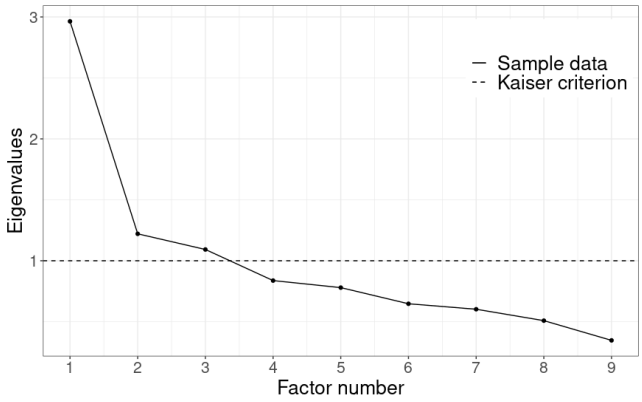


Figure 3: A scree plot of factors behind the protection behaviors.

4 RESULTS

After running the survey we obtained 292 responses in total. After filtering out 61 participants with wrong answers to the attention questions and three participants whose reported country of residence differed from Russia, we obtained 228 responses.

Descriptive statistics. The distribution of the respondents was the following: 83 (36.4%) participants were female, 144 (63.2%) were male and one participant preferred not to answer. The age for the female participants ranged from 18 to 74 ($M = 38.6, SD = 12.4$), and for the male respondents it ranged from 18 to 58 ($M = 34.3, SD = 8.4$). Lastly, the highest obtained education level of the participants was distributed in the following manner: secondary school – 9 (4%), high school or equivalent – 68 (30%), bachelor degree – 89 (39%), master degree or equivalent – 60 (26%), doctorate equivalent or above – 2 (1%).

In our study we measured privacy behavior via asking participants about the usage frequency of certain privacy-related technologies. Fig. 2 shows the obtained results. According to the analyzed responses, the most often used measure is the usage of an ad blocker, while the least used is the utilization of special browser software.

The obtained results exhibit one interesting pattern: the behavior associated with enabling "Do not track" mode in the browser has a distinctly more uniform pattern of the response distribution. That might suggest a higher uncertainty among respondents or a multidimensional nature of the protection behaviors.

Exploratory factor analysis of protection behaviors. To evaluate hypothesis H1 we performed exploratory factor analysis on the reported frequencies of the protection behaviors. We started from evaluating the number of underlying factors. According to the Kasier criterion of a number of eigenvalues-greater-than-one, we identified three factors (see Fig. 3 for details). In addition, we performed the parallel analysis to identify the number of factors. The same number of three factors was confirmed.

After identifying the number of factors, we performed factor analysis. Since the theoretical model assumes all items to measure a single construct (i.e. privacy behavior), we admitted that the factors are not orthogonal and the oblique rotation should be used. Thus, to identify the factor structure we used promax rotation.

Table 3 shows the obtained factor structure. Testing the model fit, we received a chi-squared value of 6.93 with p-value of 0.862. These values suggest a good model fit. The cumulative explained variance is 40.8%. Given the exploratory nature of our work and the

Table 2: Measurement items.

Construct	Item name	Measurement item	Source
Privacy concern	PC1	I am concerned that the information I submit on the Internet could be misused.	[55]
	PC2*	I do not see risks when providing data in the internet.	[55]
	PC3*	I do not feel comfortable with some types of information collected on the Internet.	[55]
	PC4	I am concerned about submitting my personal information in websites because of what others might do with it.	[38]
	PC5	I am concerned about submitting my personal information in websites because it could be used in a way I did not foresee.	[38]
	PC6	I usually think twice before providing my personal information in websites.	[3]
Self-efficacy	SEFF1	I believe I possess the ability to safeguard my personal information in websites.	[3]
	SEFF2	I believe I can enable the privacy protection features in websites without any assistance.	[3]
	SEFF3	I am confident in my ability to use privacy protection features in websites.	[3]
Rewards	REW1	Revealing my personal information on websites will help me obtain information/products/services I want.	[19]
	REW2	I need to provide my personal information on websites so I can get in touch with old friends and make new connections.	[3]
	REW3	I believe that as a result of my personal information disclosure, I will benefit from a better, customized service and/or better information and products.	[19]
	REW4	I need to provide my personal information so I can get exactly what I want from websites.	[19]
Experience	EXP1*	I believe that my online privacy has been invaded by other people or organizations.	[55]
	EXP2	I have had bad experiences with regard to my online privacy before.	[55]
	EXP3	I have experienced misuse of data by friends or family.	[55]
Trust	TR1	I feel that most website owners would act in a user's best interest.	[55]
	TR2	If a user required help, most website owners would do their best to help.	[55]
	TR3	Most website owners are interested in maintaining users' privacy, not just achieving their own goals.	[55]
Severity	SEV1	Losing personal information privacy through websites would be a serious problem for me.	[38]
	SEV2	Having my online identity stolen through websites (e.g., having accounts hacked) would be a serious problem for me.	[38]
	SEV3*	Possible losses (e.g., financial or reputational) resulting from a personal information privacy breach are not a serious problem for me.	[38]
	SEV4*	Losing photo privacy through websites (e.g. social networks) would be a serious problem for me.	[38]
Vulnerability	VUL1	It is likely that I will lose my information privacy when using websites.	[51]
	VUL2	I am at risk of experiencing a breach of my information privacy when using websites.	[51]
	VUL3	I could be subjected to an inappropriate use of my personal information by websites.	[51]
Response efficacy	REFF1	Enabling privacy protection options on my devices and applications prevents websites from violating my privacy.	[51]
	REFF2	Changing the settings of my devices and applications is effective in privacy protection.	[51]
	REFF3	Utilizing privacy protection measures in websites works to ensure my information privacy.	[38]
	REFF4	Enabling privacy protection features in websites could protect me from information privacy threats.	[3]

Note: Items marked with the asterisk were excluded during the confirmatory factor analysis due to the low loadings.

Table 3: Factor structure of the privacy protection behaviors.

Item	Factor 1	Factor 2	Factor 3
ad blocker (PB1)	-0.083	**0.417**	-0.117
delete cookies (PB2)	**0.566**	0.073	0.083
refrain to visit a website (PB3)	-0.032	-0.014	**0.731**
decline cookies (PB4)	0.012	0.018	**0.675**
browser private mode (PB5)	0.108	**0.630**	-0.149
delete browser history (PB6)	**0.996**	0.027	-0.029
"Do not track" mode (PB7)	-0.026	**0.497**	0.173
browser software (PB8)	-0.059	**0.455**	0.236
fabricate information (PB9)	-0.031	**0.425**	0.015

straightforward explanation of the factors (see the next paragraph), we consider that value to be satisfactory. For similar reasons we consider the value of 0.4 to be a threshold for an acceptable factor loading.

The revealed factor structure is quite easy to interpret. Factor 1 seems to represent the behavior of deleting personal information. Factor 2 exhibits the active protection behavior, mostly involving privacy enhancing technologies (PET). Factor 3 corresponds to the refraining behavior, when users either decline a website's cookies or decide not to visit a website. Due to the revealed multidimensional factor structure, in the following analysis we are going to distinguish three different protection behaviors: deleting behavior, privacy enhancing technology use behavior (PET behavior), and refraining behavior.

Measurement and structural models evaluation. To evaluate our model, we performed confirmatory factor analysis (CFA). During the evaluation each factor was associated only with its correspondent items. Our CFA model included eleven latent constructs, three of them corresponded to the privacy protection behaviors revealed during the exploratory factor analysis.

Before analyzing the structural model we assessed construct validity and reliability. The convergent validity is achieved when each standardized loading on corresponding constructs exceeds 0.5 [23]. As a result of the assessment we removed items with loadings less than the specified threshold (see Table 2 and Table 4). The internal consistency was assessed using Cronbach's α. While it is desirable for the coefficient to be greater than 0.7, it is suggested that for exploratory research the values greater than 0.6 are acceptable [23]. Similarly, for the exploratory research the compose reliability (CR) should exceed 0.6 and and the average value extracted (AVE) should be greater than 0.5 [23]. Most of the constructs exceeded these values. Unsurprisingly, due to the absence of a reliable underlying theory, two constructs (PET behavior and refraining behavior) exhibited lower internal consistency.

To ensure the discriminant validity we used the following criteria: the square root of each latent variable should exceed the absolute value of correlation of this latent variable with any other latent variable. Table 5 presents the correlation values among the constructs with the diagonal elements being square roots of AVE. There are two points to make with regard to the discriminant validity. First, though the aforementioned rule does not hold for some of the privacy behaviors, we suggest that their discriminant validity

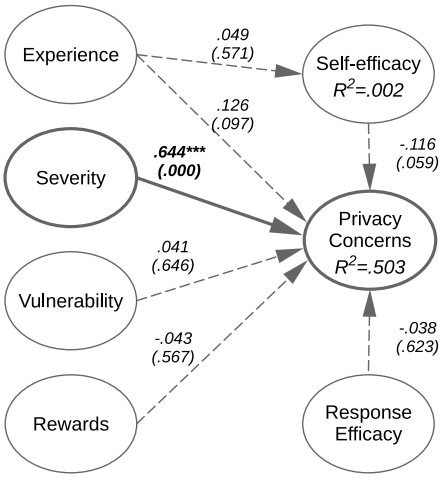


Figure 4: Results of model testing with regard to privacy concerns
Note: * — significance at 5%, ** — significance at 1%,
*** — significance at 0.1%. Solid lines represent significant links; dashed lines represent insignificant links.

was established during the exploratory factor analysis. Second, it is interesting to note a high correlation between the constructs of trust and reward. Though it does not break the validity criteria, it suggests that two constructs might measure very similar or related phenomena.

After assessing our measurement model, we conclude that it has a satisfactory validity. On the one hand, most of the previously measured constructs demonstrated very good validity and reliability metrics (Cronbach's $\alpha > 0.7, CR > 0.6, AVE > 0.5$). On the other hand, the lower values were obtained only for the newly introduced constructs. Given that their loadings, alpha and CR coefficients exceed the recommended values for exploratory analysis, we believe that the overall model demonstrates acceptable reliability and validity.

To evaluate the fit of our structural equation model we leveraged the technique of Covariance-Based SEM. Since all our measurement items were not distributed normally (according to the Shapiro-Wilk test), we performed the Satorra-Bentler correction that is widely used for dealing with nonnormality [31]. Table 6 presents model fit indices. We report the values after the Satorra-Bentler correction. It should be noted that χ^2 is sensitive to sample size and violations of multivariate normality, while GFI and AGFI are modifications of χ^2 and sensitive to sample size and degrees of freedom [50]. Given reasonable values for other fit indices (e.g., CFI, TLI, RMSEA), we believe our model demonstrated a good fit.

Hypotheses testing results. After fitting our structural model, we obtained the results shown in Fig. 4 and Fig. 5. It should be noted that these results were obtained during one fitting procedure and presented with two figures only to simplify the perception. In other words, three constructs of privacy behaviors and a latent construct corresponding to privacy concerns were evaluated simultaneously.

Hypotheses H4 and H5 possess the relationships of the previous privacy violation experience with self-efficacy and privacy concerns.

Table 4: Reliability of the measurement model.

Construct	Measurement item	Standardized loadings	AVE	Cronbach α	CR
PET behavior	PB5	0.509	0.35	0.605	0.611
	PB7	0.642			
	PB8	0.594			
Refraining behavior	PB3	0.695	0.492	0.657	0.659
	PB4	0.707			
Deleting behavior	PB2	0.744	0.633	0.767	0.774
	PB6	0.838			
Privacy concern	PC1	0.63	0.643	0.867	0.867
	PC4	0.933			
	PC5	0.946			
	PC6	0.65			
Self-efficacy	SEFF1	0.675	0.647	0.836	0.848
	SEFF2	0.807			
	SEFF3	0.916			
Rewards	REW1	0.659	0.584	0.845	0.844
	REW2	0.681			
	REW3	0.872			
	REW4	0.827			
Experience	EXP2	0.86	0.636	0.773	0.777
	EXP3	0.733			
Trust	TR1	0.805	0.647	0.846	0.846
	TR2	0.796			
	TR3	0.812			
Severity	SEV1	0.884	0.665	0.792	0.798
	SEV2	0.743			
Vulnerability	VUL1	0.75	0.682	0.858	0.868
	VUL2	0.907			
	VUL3	0.808			
Response efficacy	REFF1	0.698	0.695	0.899	0.898
	REFF2	0.823			
	REFF3	0.916			
	REFF4	0.890			

Table 5: Discriminant validity of the items.

Construct	PBpets	PBrefr	PBdel	PC	SEFF	REW	EXP	TR	SEV	VUL	REFF
PBpets	**0.592**										
PBrefr	0.710	**0.702**									
PBdel	0.528	0.382	**0.795**								
PC	0.328	0.355	0.378	**0.802**							
SEFF	0.313	0.023	0.240	-0.009	**0.804**						
REW	-0.272	-0.165	0.011	-0.084	0.046	**0.764**					
EXP	0.364	0.365	0.235	0.351	0.062	-0.027	**0.798**				
TR	-0.234	-0.041	-0.032	-0.125	0.200	0.750	-0.183	**0.804**			
SEV	0.290	0.336	0.366	0.673	0.178	-0.022	0.317	0.001	**0.815**		
VUL	0.153	0.265	0.148	0.337	0.026	0.078	0.409	-0.106	0.376	**0.826**	
REFF	0.242	0.002	0.177	0.123	0.480	0.281	-0.065	0.429	0.379	-0.102	**0.834**

Our results exhibit no support for these two statements. Thereby, we can conclude that even though previous experience of dealing with privacy protection is assumed to influence self-efficacy [5], privacy violation experience does not significantly contribute to the construct. Additionally, our results contradict with the results obtained by Zeissig et al.[55] but go in line with the accepted PMT-based models of privacy concerns.

Table 6: Model fit indices.

Fit measure	Recommended value	Observed value
χ^2		503.21
df		391
χ^2/df	$< 2^{b}$	1.29
p-value	$> .05$	.000
CFI	$\geq .95^{a}$	.959
TLI	$\geq .95^{a}$	.951
GFI	$\geq .90^{b}$	.857
AGFI	$\geq .90^{b}$	.818
IFI	$\geq .95^{a}$	.960
RMSEA	$\leq .05^{a}$	.035
SRMR	$\leq .08^{a}$	.078

Cut-off values are taken from:

[a] Hu and Bentler [24],

[b] Westland [50].

We have found no support for hypotheses H7, H9, H10, or H12, but the results revealed a significant relationship between severity and privacy concerns, thus supporting hypothesis H8. These results contribute to the ambiguity of the existing work with regard to the influence of vulnerability [8, 54], response efficacy [3, 38], and rewards on privacy concerns [3]. Interestingly, severity was found to be the only significant predicting factor. Given that our Russian sample is distinguished by the high level of experienced censorship and the influence of the ongoing war (e.g. threats of conscription/mobilization), we hypothesize that severity became the most affecting factor due to its importance for the respondents in the current situation. This reasoning suggests that the structure of factors affecting privacy concerns is dynamic and might not be easily generalizable to any population.

After performing the exploratory factor analysis, we were able to distinguish three different protection behaviors. Thereby, to test hypotheses H2, H3, H6, H11, H13, H14 we evaluated the relationships of the corresponding concepts with all three types of protection behaviors. Interestingly, different factors were found to be significant in different cases (see Fig. 5).

The utilization of the privacy enhancing technologies (PET) behavior has been found to be significantly affected by privacy violation experience, self-efficacy, and response efficacy (see Fig. 5a). The revealed structure has a simple explanation: one is more likely to use PET, if they are confident in their abilities and the tool efficiency and if they have experienced privacy violations before. It is worth noting that self-efficacy and response efficacy have not influenced privacy concerns (see Fig. 4) but directly affected the privacy behavior. Thereby, our results question the mediating role of privacy concerns that was assumed in previous research. For instance, Mohamed and Ahmad found no influence of response efficacy on privacy behavior using privacy concerns as mediating construct [38]. But the authors did not test the direct relationship between response efficacy and privacy behavior.

The refraining behavior is found to be significantly related to privacy violation experience, privacy concerns, and rewards (see Fig. 5b). Additionally, the influence from trust towards websites is found to approach significance. The observed structure for the refraining behavior also has a straightforward explanation. In this case a user tends not to use a website (or to decline the cookies) if they had a negative experience in the past, they are concerned about their privacy, or they do not think that visiting the website is beneficial enough for them. The last part can be viewed as an argument for the privacy calculus in this specific type of protection behavior.

The deleting behavior is found to be influenced by self-efficacy and privacy concerns (see Fig. 5b). While it is quite easy to justify the relationship between privacy concerns and the behavior, the influence of self-efficacy is not self-explanatory. We believe that deleting browser history and a website's cookies are two type of activities that require a lay user to perform some unusual actions. Thereby, this behavior is influenced by the person's self-efficacy [5].

5 DISCUSSION

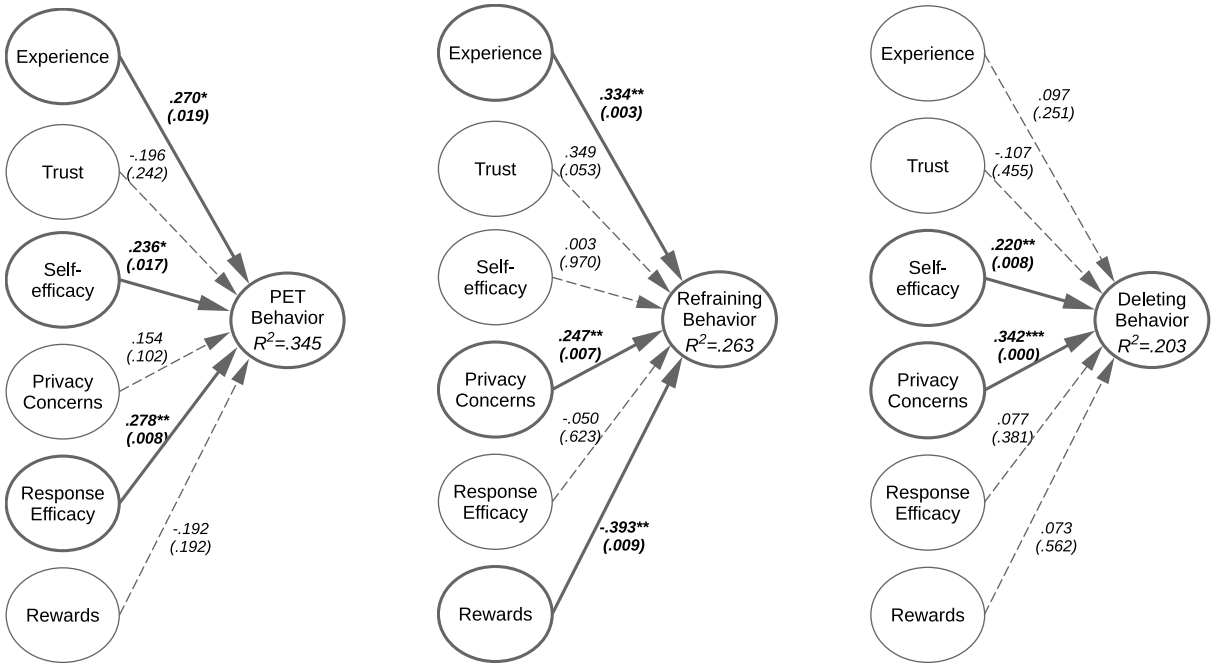
In this section we discuss our findings in the light of the existing research. We start from outlining the limitations of our work. Then, we proceed with the discussion of our contributions. Specifically, we demonstrate how the obtained evidence can empower future research.

5.1 Limitations

Before interpreting our findings, we need to point out the known limitations of the research. First, due to the exploratory nature of our work, it was not possible to ensure a good theoretical model underlying privacy protection behaviors. Thereby, the validity of the corresponding constructs is relatively low. At the same time, we should note that the validity was partially established by the means of the exploratory factors analysis that revealed the apprehensible factor structure. Second, our measurement model had several factors loaded with only two indicators. As discussed by Loehlin [31], a small number of indicators per latent construct (e.g., one or two) might lead to poor quality solutions, especially with low samples (less than 100). Though our analysis was done with an acceptable sample size of 228 respondents and most of the factors were loaded with three or four indicators, future researchers should consider this limitation by adopting and testing new measurement items. Third, the measurement of privacy protection behaviors might be biased due to the lack of the awareness by respondents. In our case, we observed an unusual distribution for the "Do not track" behavior, that might indicate a random choice. Last, the generalizability of our results is limited due to the characteristics of our sample. On the one hand, the gender distribution was skewed due to the survey platform's gender distribution. On the other hand, the survey was specifically conducted on a subset the Russian population with some English proficiency. Though the language choice allowed us to measure the constructs similar to previous studies (without any shift of meaning due to translation), it might have also resulted in a sample biased towards a more educated audience.

5.2 Multidimensionality of the Privacy Protection Behavior

The most prominent contribution of our work is the evidence on multidimensionality of the privacy protection behavior. We found



(a) Factors affecting PET behavior. **(b) Factors affecting refraining behavior.** **(c) Factors affecting deleting behavior.**

Figure 5: Results of model testing with regard to protection behaviors.

out that the protection behaviors, previously assumed to be unidimensional by Boerman et al. [8], can be in fact decomposed into three comprehensible categories: leveraging privacy enhancing technologies, refraining behavior, and behavior of information deletion.

Interestingly, our results are in line with earlier works, where authors also distinguished several types of protection behavior: help seeking, refraining from usage, fabricating personal information [39, 54]. In support of the hypothesis on the behavior multidimensionality, we received the evidence on different factors influencing three types of behavior. For instance, privacy concerns were found to influence significantly only two of three behaviors, while some other constructs, e.g. response efficacy, affected only a single behavior. These results might help to explain the privacy paradox: it is not a single behavior that is occasionally affected by privacy concerns but there are at least three different behaviors with different relationships with privacy concerns. These results are in agreement with the existing research of the privacy paradox: the latter disappears when a multidimensional nature of privacy is considered [15].

The multidimensionality of privacy protection behaviors allows one to reconsider existing knowledge. One straightforward possibility is to meticulously account for different types of protection behaviors. For instance, in the comprehensive review by Gerber et al., the authors investigate the phenomena of privacy paradox [22]. Similar to our work they consider several types of the behavior: "the examined privacy behavior comprises the disclosure of information <...>, as well as the actual usage of data sharing applications, the management of privacy settings and the performance of privacy protection behavior." However, the question of behavior granularity remains open. For instance, in their overview, the authors consider the construct of technical behaviors from the work by Park [41]. Interestingly, in the latter, the construct of technical behavior seems to be assessed with questions from different dimensions (e.g., "Cleared your web browser history" and "Used software that hides your computer's identity from websites you visit" corresponding to Deleting Behavior and PET Behavior). Since our work reveals that each protection behavior has a unique set of antecedents, we believe that the future research might benefit from thoroughly defining and distinguishing protection behaviors.

5.3 Structure of Privacy Concerns

Another contribution of this work is the evidence on the dynamic structure of privacy concerns. In contrast to the existing research on samples from benign environments, our sample was elicited from a country at war with existing threats of conscription/mobilization and high-level of surveillance. Our findings differ from the previous works. The only significant factor affecting privacy concerns was found to be the severity of consequences. Though this might not be directly related to the sample characteristics, it suggests that privacy concerns do not have a static structure and that the structure might vary in different populations.

We should note that our research questions the mediating role of privacy concerns for predicting privacy protection behavior. Similar to Adhikari [3] we found no influence from rewards on privacy concerns, at the same time, we revealed that the construct directly affected some privacy protection behaviors. These findings

are in accordance with Protection Motivation Theory [42]: the latter postulates that there are several factors that affect protection motivation, thereby influencing the behavior through behavioral intentions. The original theory does not justify the inclusion of privacy concerns as mediating construct. This is in line with the evidence on relationships between privacy concerns, privacy attitudes, and privacy behaviors [15].

5.4 National Samples in Privacy Research

Several works investigated the privacy phenomenon on populations from different nations or cultures. Chen et al. considered two populations in their research: the United States and China [10]. The authors reveal the divergence between the two countries in threat perception and coping behaviors. One of the interesting results is the higher influence of severity on perceived threat in the Chinese sample. The authors explain this finding stating that "Chinese users are more reactive to threat severity given their lower levels of economic resources and pessimistic perspectives". Though not directly comparable, our study supports this finding: in the Russian population, the severity of the threat becomes the only factor significantly affecting privacy concerns. The pessimistic perspectives in the Russian population might also be an explanation of the observed relationship.

Mitglen and Peyrat-Guillard performed a qualitative analysis of factors influencing privacy concerns in seven European countries [37]. The authors also consider several factors that underlie respondents' views: country location (South, East, North, or West Europe), age, individualism-collectivism of a national culture. In addition, the four prominent privacy-related "foci" are distinguished: control, protection and regulation, trust, and responsibility. The focus of control corresponds to our constructs of severity and self-efficacy. In our case severity has a noticeably higher impact on privacy concerns than self-efficacy. Thereby, we conclude that the increase of the foci granularity might lead to a better understanding of the phenomenon.

It is interesting to review our findings in the context of populations at risk. Shklovski and Wulf investigated the use of private mobile phones and some privacy concerns of participants of the Russian-Ukrainian conflict in 2017 [44]. The authors reveal that the main protection strategy was to refrain from usage of certain technologies. The most prominent factor influencing the decision was the severity of consequences (e.g., the usage of a mobile phone signal as targeting information or possible problems for the respondent's relatives after a successful government surveillance). Additionally, the authors disclose that soldiers were still using their mobile phones despite the danger. The reasons for such behavior are outlined as avoiding boredom and keeping sanity. Our work allows one to explain these findings. In our resulting model, the refraining behavior is indeed affected by the severity of consequences with privacy concerns being a mediating construct. Similarly, according to our findings, the major factor that prevents the refraining behavior adoption is the presence of rewards (e.g., avoiding boredom). Thereby, in the context of a war conflict, to promote the refraining behavior, we suggest to provide safe alternatives for the dangerous rewarding behaviors.

A case of the 2018-2019 Sudanese revolution was investigated by Daffalla et al. [14] The authors share several interesting findings, corresponding to protection behaviors of Sudanese activists. It is observed that some activists were not able to adopt protection technologies either due to the low efficacy of the solution (e.g., due to inability to build a mesh-network in the required settings) or because of the high complexity of the software. We believe that the influence of these two factors is reflected in our model: PET behavior is affected by the perceived response-efficacy and self-efficacy. Thereby, we conclude that PET developers can benefit from investigating their target audience and designing solutions that: a) would be effective in the settings common for that audience (high response-efficacy); b) would not require a significant adoption effort (lower self-efficacy needed for utilizing the technology).

5.5 Future Work

Our findings suggest that the measurement of privacy protection behaviors might not be a straightforward task. On the one hand, it is not always clear what actually constitutes the behavior: is it a single technology use? Or is it a set of technologies? On the other hand, measuring the adjacent constructs is not an easy task either. As it is noted in the review by Gerber et al. [22], in many cases researchers rely on slightly different constructs, thereby, complicating the generalizability of the results. To address this issue, we believe it would be beneficial for privacy researchers to establish and verify a set of privacy-behavior-related scales. In addition, we observed that the constructs shift in meaning when translated to another language. Therefore, it might be beneficial to account for this factor in the design of language-specific versions of the scales.

Another way to increase the generalizability and explainability in privacy research is to make use of neuroIS approach. This approach leverages methods and tools from neurocognitive science to better understand the perception of different aspects of information systems [16]. In addition to relying on the abstract concept of behavior, neuroIS researchers benefit from having a concrete research object: the human brain. For example, Warkentin et al. investigated neural responses to threat and coping appraisals using functional magnetic resonance imaging (fMRI) tools [47]. Along with the survey data, the authors observed differences in brain activations. One interesting result is that the coping appraisals did not elicit activation corresponding to a sense of reward. This finding was not in line with the fear appeal theory adopted for the research. Relying on the observed evidence, the authors pointed to the inconsistencies in the theory when applied to information security problems.

6 CONCLUSION

Previous work on privacy concerns and protection behaviors revealed a number of inconsistencies. The obtained evidence did not allow researchers to make conclusions on the exact structure of factors underlying two constructs of interest. Even more, to describe the ambiguous nature of the observed relations, a notion appeared, known as privacy paradox. To shed light on the phenomenon of privacy behaviors, we performed our exploratory study.

Our results suggest the following. First, we established that the privacy protection behavior is a multidimensional construct and

different types of the behavior are affected by different factors. This observation allows one to demystify the privacy paradox and warns researchers against mixing different types of protection behaviors. Second, our results indicate that privacy concern might have a dynamic structure. The latter might be significantly affected by the environment of the target population. Third, our findings contribute to a deeper understanding of protection behaviors in populations at risk. The resulting model enabled us to interpret evidence from existing qualitative studies and formulate suggestions for promoting the desired types of behavior. In summary, our work suggests that future researchers should be cautious when investigating protection behaviors: they should account for behavior type, behavioral context, and the environment of the observed sample.

ACKNOWLEDGMENTS

We would like to thank Julia Evans and Karsten Sohr for careful reading of earlier versions of the paper. We would also like to thank the anonymous referees for their valuable feedback. This work was co-funded by the European Research Council for the project ScienceGRAPH (Grant agreement ID: 819536) and the German Ministry of Education and Research (BmBF) for the project KISSKI AI Service Center (01IS22093C).

REFERENCES

[1] 2012. The menlo report. *IEEE Security & Privacy* 10, 2 (2012), 71–75.
[2] 2017. Federal Law of 29.07.2017 276-FZ "On Amendments to the Federal Law" On Information, Information Technology and Information Protection. Apr. 2019. h. (2017). http://publication.pravo.gov.ru/Document/View/0001201707300002?rangeSize=1&index=1
[3] Kishalay Adhikari and Rajeev Kumar Panda. 2018. Users' information privacy concerns and privacy protection behaviors in social networks. *Journal of Global Marketing* 31, 2 (2018), 96–110.
[4] Irwin Altman. 1976. A conceptual analysis. *Environment and behavior* 8, 1 (1976), 7–29.
[5] Albert Bandura. 1977. Self-efficacy: toward a unifying theory of behavioral change. *Psychological review* 84, 2 (1977), 191.
[6] Gaurav Bansal, David Gefen, et al. 2010. The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision support systems* 49, 2 (2010), 138–150.
[7] Lemi Baruh, Ekin Secinti, and Zeynep Cemalcilar. 2017. Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication* 67, 1 (2017), 26–53.
[8] Sophie C Boerman, Sanne Kruikemeier, and Frederik J Zuiderveen Borgesius. 2021. Exploring motivations for online privacy protection behavior: Insights from panel data. *Communication Research* 48, 7 (2021), 953–977.
[9] Janice C. Sipior, Burke T. Ward, and Regina Connolly. 2013. Empirically assessing the continued applicability of the IUIPC construct. *Journal of Enterprise Information Management* 26, 6 (2013), 661–678.
[10] Yan Chen and Fatemeh Mariam Zahedi. 2016. Individuals' internet security perceptions and behaviors. *Mis Quarterly* 40, 1 (2016), 205–222.
[11] Danielle Keats Citron and Frank Pasquale. 2014. The scored society: Due process for automated predictions. *Wash. L. Rev.* 89 (2014), 1.
[12] Robert E Crossler. 2010. Protection motivation theory: Understanding determinants to backing up personal data. In *2010 43rd Hawaii International Conference on System Sciences*. IEEE, 1–10.
[13] Mary J Culnan and Pamela K Armstrong. 1999. Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization science* 10, 1 (1999), 104–115.
[14] Alaa Daffalla, Lucy Simko, Tadayoshi Kohno, and Alexandru G Bardas. 2021. Defensive Technology Use During the 2018-2019 Sudanese Revolution. *IEEE Security & Privacy* 20, 2 (2021), 40–48.
[15] Tobias Dienlin and Sabine Trepte. 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 (2015), 285–297.
[16] Angelika Dimoka, Fred D Davis, Alok Gupta, Paul A Pavlou, Rajiv D Banker, Alan R Dennis, Anja Ischebeck, Gernot Müller-Putz, Izak Benbasat, David Gefen, et al. 2012. On the use of neurophysiological tools in IS research: Developing a research agenda for NeuroIS. *MIS quarterly* (2012), 679–702.
[17] Tamara Dinev and Paul Hart. 2004. Internet privacy concerns and their antecedents-measurement validity and a regression model. *Behaviour & Information Technology* 23, 6 (2004), 413–422.
[18] Tamara Dinev and Paul Hart. 2006. An extended privacy calculus model for e-commerce transactions. *Information systems research* 17, 1 (2006), 61–80.
[19] Tamara Dinev, Heng Xu, Jeff H Smith, and Paul Hart. 2013. Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems* 22, 3 (2013), 295–316.
[20] Ksenia Ermoshina, Benjamin Loveluck, and Francesca Musiani. 2022. A market of black boxes: The political economy of Internet surveillance and censorship in Russia. *Journal of Information Technology & Politics* 19, 1 (2022), 18–33.
[21] Steve M Furnell, Peter Bryant, and Andrew D Phippen. 2007. Assessing the security perceptions of personal Internet users. *Computers & Security* 26, 5 (2007), 410–417.
[22] Nina Gerber, Paul Gerber, and Melanie Volkamer. 2018. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & security* 77 (2018), 226–261.
[23] Joseph F Hair. 2009. Multivariate data analysis. (2009).
[24] Li-tze Hu and Peter M Bentler. 1999. Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural equation modeling: a multidisciplinary journal* 6, 1 (1999), 1–55.
[25] Jim Isaak and Mina J Hanna. 2018. User data privacy: Facebook, Cambridge Analytica, and privacy protection. *Computer* 51, 8 (2018), 56–59.
[26] Hanna Krasnova, Sarah Spiekermann, Ksenia Koroleva, and Thomas Hildebrand. 2010. Online social networks: Why we disclose. *Journal of information technology* 25, 2 (2010), 109–125.
[27] Robert LaRose and Nora J Rifon. 2007. Promoting i-safety: effects of privacy warnings and privacy seals on risk assessment and online privacy behavior. *Journal of Consumer Affairs* 41, 1 (2007), 127–149.
[28] Doohwang Lee, Robert Larose, and Nora Rifon. 2008. Keeping our network safe: a model of online protection behaviour. *Behaviour & Information Technology* 27, 5 (2008), 445–454.
[29] Yuan Li. 2014. The impact of disposition to privacy, website reputation and website familiarity on information privacy concerns. *Decision support systems* 57 (2014), 343–354.
[30] Huigang Liang and Yajiong Xue. 2009. Avoidance of information technology threats: A theoretical perspective. *MIS quarterly* (2009), 71–90.
[31] John C Loehlin. 2004. Latent variable models: An introduction to factor, path, and structural equation analysis. (2004).
[32] James E Maddux and Ronald W Rogers. 1983. Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of experimental social psychology* 19, 5 (1983), 469–479.
[33] Jens-Erik Mai. 2016. Big data privacy: The datafication of personal information. *The Information Society* 32, 3 (2016), 192–199.
[34] Naresh K Malhotra, Sung S Kim, and James Agarwal. 2004. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information systems research* 15, 4 (2004), 336–355.
[35] D Harrison McKnight, Vivek Choudhury, and Charles Kacmar. 2002. Developing and validating trust measures for e-commerce: An integrative typology. *Information systems research* 13, 3 (2002), 334–359.
[36] Sarah Milne, Paschal Sheeran, and Sheina Orbell. 2000. Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory. *Journal of applied social psychology* 30, 1 (2000), 106–143.
[37] Caroline Lancelot Miltgen and Dominique Peyrat-Guillard. 2014. Cultural and generational influences on privacy concerns: a qualitative study in seven European countries. *European journal of information systems* 23, 2 (2014), 103–125.
[38] Norshidah Mohamed and Ili Hawa Ahmad. 2012. Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in human behavior* 28, 6 (2012), 2366–2375.
[39] Deborah M Moscardelli and Richard Divine. 2007. Adolescents' concern for privacy when using the Internet: An empirical analysis of predictors and relationships with privacy-protecting behaviors. *Family and Consumer Sciences Research Journal* 35, 3 (2007), 232–252.
[40] Patricia A Norberg, Daniel R Horne, and David A Horne. 2007. The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of consumer affairs* 41, 1 (2007), 100–126.
[41] Yong Jin Park. 2015. Do men and women differ in privacy? Gendered privacy and (in) equality in the Internet. *Computers in Human Behavior* 50 (2015), 252–258.
[42] Ronald W Rogers. 1975. A protection motivation theory of fear appeals and attitude change. *The journal of psychology* 91, 1 (1975), 93–114.
[43] Ronald W Rogers. 1983. Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. *Social psychology: A source book* (1983), 153–176.
[44] Irina Shklovski and Volker Wulf. 2018. The use of private mobile phones at war: Accounts from the Donbas conflict. In *Proceedings of the 2018 CHI conference on human factors in computing systems*. 1–13.
[45] H Jeff Smith, Sandra J Milberg, and Sandra J Burke. 1996. Information privacy: Measuring individuals' concerns about organizational practices. *MIS quarterly*

(1996), 167–196.
[46] Sabine Trepte, Michael Scharkow, and Tobias Dienlin. 2020. The privacy calculus contextualized: The influence of affordances. *Computers in Human Behavior* 104 (2020), 106115.
[47] Merrill Warkentin, Eric Walden, Allen C Johnston, and Detmar W Straub. 2016. Neural correlates of protection motivation for secure IT behaviors: An fMRI examination. *Journal of the Association for Information Systems* 17, 3 (2016), 1.
[48] Maor Weinberger, Dan Bouhnik, and Maayan Zhitomirsky-Geffet. 2017. Factors affecting students' privacy paradox and privacy protection behavior. *Open Information Science* 1, 1 (2017), 3–20.
[49] Alan F Westin. 1968. Privacy and freedom. *Washington and Lee Law Review* 25, 1 (1968), 166.
[50] James Christopher Westland. 2015. Structural Equation Models - From Paths to Networks, Second Edition. In *Studies in Systems, Decision and Control.*
[51] Irene Woon, Gek-Woo Tan, and R Low. 2005. A protection motivation theory approach to home wireless security. (2005).
[52] Heng Xu, Tamara Dinev, H Jeff Smith, and Paul Hart. 2008. Examining the formation of individual's privacy concerns: Toward an integrative view. (2008).
[53] Diwen Xue, Benjamin Mixon-Baca, ValdikSS, Anna Ablove, Beau Kujath, Jedidiah R Crandall, and Roya Ensafi. 2022. TSPU: Russia's decentralized censorship system. In *Proceedings of the 22nd ACM Internet Measurement Conference*. 179–194.
[54] Seounmi Youn. 2009. Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *Journal of Consumer affairs* 43, 3 (2009), 389–418.
[55] Eva-Maria Zeissig, Chantal Lidynia, Luisa Vervier, Andera Gadeib, and Martina Ziefle. 2017. Online privacy perceptions of older adults. In *Human Aspects of IT for the Aged Population. Applications, Services and Contexts: Third International Conference, ITAP 2017, Held as Part of HCI International 2017, Vancouver, BC, Canada, July 9-14, 2017, Proceedings, Part II 3*. Springer, 181–200.
[56] Lixuan Zhang and William C McDowell. 2009. Am I really at risk? Determinants of online users' intentions to use strong passwords. *Journal of Internet Commerce* 8, 3-4 (2009), 180–197.