To (Psychologically) Own Data is to Protect Data: How Psychological Ownership Determines Protective Behavior in a Work and Private Context

Margareta Heidt[1], Christian Michael Olt[1], Peter Buxmann[1]

[1] Technische Universität Darmstadt, Information Systems, Darmstadt, Germany
{heidt,olt,buxmann}@is.tu-darmstadt.de

Abstract. The ever rising rates of data generation entail new opportunities for business and society but also an increasing risk of data breaches. Apart from technical measures, approaches like password authentication to ensure data protection revolve around the end-user as the human element in information security. Drawing on organizational research which argues that the sole feeling of ownership towards an intangible target like data can lead to heightened levels of the individual's responsibility, we investigate whether and to what extent this ownership feeling differs between personal files and data accessed in the work context. To this end, we draw on data derived through a two-phase questionnaire among a representative group of 209 employees. Consequently, we find evidence that psychological ownership shows stronger effects on protection motivation among participants in a private context. Furthermore, results indicate that employees partly relinquish their responsibility regarding security responses to protect data in their work context.

Keywords: password security, psychological ownership, employee, home user, protection motivation theory

1 Introduction

According to the latest estimations in 2012, 2.7 million terabytes existed in the digital universe with roughly 35 zettabytes of data generated annually by 2020 [1]. Data generation is further fueled through the acceleration of the Internet of Things and the growth of worldwide internet users to 4 billion in 2018 [2].

Unsurprisingly, the age of big data promises new opportunities for business and everyday life but entails new flip sides as evidenced by the ever increasing frequency and amount of damage of data breaches committed by cyber criminals. Verizon's annual report estimates that 81 percent of data breaches that occurred since 2014 were caused by stolen or weak passwords [3]. An estimation particularly striking given that the most prevalent approach to both access and protect private and business data remains through password authentication. Passwords can thus be considered a particular vulnerability as they are especially intertwined with the human element in information systems – the end-user. Since end-users have been continuously identified

14th International Conference on Wirtschaftsinformatik,
February 24-27, 2019, Siegen, Germany

as the “weakest link” within the security chain, behavioral information security research emerged as an important subfield of information systems (IS) [4, 5].

Research on human behavior in IS security has been drawing on psychology, criminology, or health science and various adapted frameworks and models have been applied within the end-user context, examining either employee or individual private user behavior [5-7]. These models show that factors such as the certainty of sanctions, the risk appraisal of a cyber threat or perceived behavioral control are strong indicators leading to the behavioral intention to perform certain protective actions [8, 9]. However, extant studies have only identified and analyzed the effectiveness of these factors on security in *either* a work environment *or* in the context of private use [10]. Thus, it remains unclear if certain factors affect the intention to behave in a more secure way in order to protect – one’s own or the company’s – data even though the context-sensitivity of findings has recently received increased attention among IS scholars [11].

In this regard, existing studies [e.g., 12, 13] have suggested that the sole feeling of possession or “being psychologically tied to an object” [14, p. 299] might lead to heightened levels of individual responsibility and engagement in IS security behavior. This feeling is referred to as “*psychological ownership*”, a concept that describes the self-derived perception of ownership opposed to the actual legal ownership which is backed by the perception of others and the legal system. Psychological ownership (PO) is rooted within the innate human need to experience possession of either tangible or intangible targets [15] and the sense of regarding this target as extension of one’s self [16]. In turn, human desire to experience control and accountability over the target differs according to the level of PO an individual experiences [14, 17].

However, IS studies thus far have either focused on feelings of ownership towards the targets ‘internet’ and ‘one’s computer’ among home-users [12] *or* towards the target ‘information’ in a generic work-based scenario [13]. Whereas the first study argues for a direct influence of PO on intention to protect the target of ownership, the latter theorizes how PO affects the protection motivation, i.e., antecedents of intention to protect information. Due to the dearth of research on the influence of PO on security behavior, both aforementioned studies call for future research with Anderson and Agarwal specifically recommending additional studies that “explore the differences in behavior between employees and home users” [12, p. A15]. Nevertheless, other IS studies that integrated PO into the privacy calculus [18] or explored PO of IT [19] have only examined the role of PO in one single context and have not questioned yet how levels of PO might differ according to situational differences in contexts. But do individuals really experience the same degree of PO regarding, for example, their own electronic device or one provided through their company? Or do individuals experience higher levels of PO regarding their personal data as opposed to PO regarding the data they work with – and are supposed to protect through appropriate security measures – in their professional environment?

Against this backdrop, we seek to (1) extend prior IS research on individuals’ protection motivation of data by highlighting the distinct role of PO both in a work and a private context. Furthermore, our study is the first to our knowledge that actually (2) compares protection motivation based on a repeated measures study design and one distinct sample in both contexts.

The remainder of this article is structured as follows: the theoretical background of both Protection Motivation Theory and psychological ownership is presented and serves as the foundation of our hypotheses which are integrated into a research model and tested in both a work and private setting. Subsequently, the results of our study are demonstrated and discussed before implications for theory and practice are derived.

2 Theoretical Background and Hypotheses Development

The following section provides an overview of the current state of behavioral IS security research in both work and private contexts along with the basics of the aforementioned concept of psychological ownership and how it has been accounted for thus far in IS security literature. Based on the theoretical background, hypotheses are developed and integrated into our research model which draws on Protection Motivation Theory (PMT).

2.1 Information Security Research

IS research has a long-standing tradition of analyzing security-related issues on an organizational and individual level [20, 21]. In an organizational context, researchers continue to advance technical approaches to prevent intrusion or to detect attacks [22, 23], however behavioral information security research has gained considerable momentum during the last two decades by focusing on human, and in particular, end-user behavior in work and private use contexts.

Within behavioral information security research, users in a work context can generally be divided into two subgroups: users that exhibit deviant behavior, i.e., compromising information security through espionage, theft, or sabotage, and those users who misbehave without the intent to cause damage [24]. By means of example, the latter group's misbehavior can manifest itself through defiance of security policy aspects such as using corporate devices to access non-work related websites or utilizing weak, repetitive and thus easy-to-compromise passwords for important work accounts [25]. In order to understand the driving factors of such "unintended" misbehavior or to identify aspects that encourage the use of safeguarding practices, IS researchers have heavily relied on behavioral theories that originate in behavioral psychology, organizational science, criminology, or health research [6-9, 12].

Protection Motivation Theory has been widely used to analyze "any threat for which there is an effective recommended response that can be carried out by the individual" [26, p. 409] and thus serves as a widespread theory in IS security research due to its applicability to security threats such as violating security compliances [27] or losing data due to irregular backups or weak passwords [28]. At the core of PMT, attitudes of individuals are assessed through two cognitive processes which lead to an increased intention to protect oneself against a potential threat: namely, *threat* and *coping appraisal*.

Threat appraisal comprises the perception and assessment of threat severity as well as the personal vulnerability to a threat. In our security context, perceived severity of a data breach and one's own vulnerability to fall prey to such an event will affect the protection motivation regarding data. As both perceived severity and vulnerability are positively correlated with the response behavior to protect one's data, which in our case will be through strong passwords, we hypothesize:

> **H1a** *Perceived vulnerability will have a positive effect on an end-user's intention to protect (work and private) data.*
> **H1b** *Perceived severity will have a positive effect on an end-user's intention to protect (work and private) data.*

Once the threat is assessed, e.g., the potential severity of data loss or theft and one's susceptibility or likeliness to experience such an incident, individuals will evaluate a potential behavioral response to the threat during the so-called coping appraisal.

Coping appraisal includes the concepts response efficacy and the associated response costs of the planned coping response necessary to protect oneself from the specific threat, as well as one's perceived self-efficacy in performing the response. If self-efficacy and response efficacy outweigh response costs, an individual yields a positive coping appraisal, i.e., individuals will install anti-virus software despite the associated costs in terms of purchase price or time to install because they feel capable of performing the installation and also deem the software to be effective in averting viruses and malware [12, 28]. More precisely, response efficacy in PMT refers to the belief that a certain response performed by the individual actually leads to a reduction or elimination of the considered threat.

Regarding IS security, end-users might wonder if strong passwords actually increase the security of their own or their company's data. If this specific response is considered effective in actually decreasing the threat (such as potential misuse of data caused by unauthorized access) an individual will be more inclined towards actually using strong passwords. However, this response also entails the cognitive effort of remembering several complex passwords. The concept of response costs thus assesses all efforts and expenditures associated with the coping behavior which will have a negative impact on the intention of actually performing the response in question. We thus hypothesize:

> **H1c** *Response efficacy will have a positive effect on an end-user's intention to protect (work and private) data.*
> **H1d** *Response costs will have a negative effect on an end-user's intention to protect (work and private) data.*

The core nomology of PMT additionally includes the concept of self-efficacy which has also been applied in various other theories to assess IS security behavior, often as part of the construct perceived behavioral control (PBC) [8, 29, 30]. On the one hand, self-efficacy relates to the confidence of individuals in their own skill, knowledge and ability to perform the response. On the other hand, controllability, as the second aspect of PBC, describes how much of the performance is actually up to the individual [30, 31]. One example would be that employees might be hindered to implement a security measure due to missing administrator rights on their work computers. Similar to other PMT-based studies which extended their research model with elements of the models originating from Theory of Planned Behavior, we also integrate the complete concept of PBC into our model as it could serve as a differentiator between the work and private context [12, 32].

In an IS security context, end-users who are confident in their ability to perform an appropriate security measure like backing up data at home or at their workplace, will be more inclined to progress with that chosen coping mechanism. However, controllability might differ across contexts, because employees might not express the same extent of assumed controllability regarding their actions if they cannot implement a security measure due to missing administrator rights – even if they had the skill and knowledge in doing so. As a result, they might shift the responsibility to their IT department or employer. Nevertheless, if employees just like private end-user ascribe responsibility to themselves, i.e., perceive higher degrees of controllability regarding the coping mechanism, they will be more proactive in taking appropriate security measures [32]. Hence, we expect that:

H1e *Self-efficacy will have a positive effect on an end-user's intention to protect (work and private) data.*
H1f *Controllability will have a positive effect on an end-user's intention to protect (work and private) data.*

2.2 Psychological Ownership

The following examples serve as an introduction to the general concept of PO: 1) Alice and Bob, both three-year-old toddlers, erupt in a fight over a doll in a physician's practice: both children claim the doll belongs to them and attempt to protect it from the other claimant by shouting "It is MINE!" – Although, technically, the doll is legally owned by the physician. 2) Alice's mother is a project manager. She lovingly calls one of her recent projects her 'baby' and takes many project-related tasks home to continue working after hours instead of delegating tasks because she feels a high sense of commitment and ownership towards this particular project. These scenarios depict how individuals behave when they feel that they possess an ownership stake in a physical or intangible object – a phenomenon called psychological ownership.

The term PO stems from psychology and describes the sense of ownership of a target like the aforementioned doll or project, but can also be felt towards a concept, another person, or an entire organization or community. The target is seen as an extension of the self [33], i.e., the owners regard the target as an expression of themselves or feel a strong sense of belongingness towards the target – as evidenced for example by football supporters who feel strong ownership towards their football club [14, 16]. Although related, PO is distinct from legal ownership which is recognized by society and protected by legislation – whereas PO is a "condition of which one is aware through intellectual perception […] coupled with an emotional or affective sensation" [34, p. 86]. The resulting effects of PO have been analyzed and categorized into positive outcomes – such as citizenship, personal sacrifice and assumption of risk, or experienced responsibility and stewardship – and negative effects like territoriality and other defiant behavior, or personal maladies like stress or frustration if the target is subject to any form of alteration [34, 36].

The roots of PO or the reason why this cognitive-affective state exists is best explained by an innate need of having a place or belongingness to the target [15], a sense of symbolic expression though the target or self-identity [16], and the desire to experience causal efficacy through control and accountability over the target [14, 17]. Due to the versatility of the PO concept, it has found extensive application especially in management and organizational research. More recently, studies in an IS context have started to introduce PO and demonstrated its impact on system usage and appreciation of IT [19, 35], willingness to disclose data [18], or intentions to perform security-related behavior [12, 13]. However, only the latter two studies examine the role of PO as antecedent of the threat and coping appraisal or its direct effect on intention in a behavioral security context [12,13]. In line with their reasoning and to further explicate how PO possibly affects the coping and threat appraisal, we present a third example: 3) Bob's father uses a CRM application on a daily basis at work which is accessed through password authentication. He is fully aware of the criticality of customer and business data stored in the application and has an intimate knowledge of many entries since he found and recorded a lot of the information himself. The data is not simply his company's data but also his own in his perception and a loss thereof would hurt him personally. Thus, threats to the target can be regarded as threats to oneself because the target represents an extension of one's self-concept or identity. In our context, higher levels of PO will lead to heightened perceptions of severity and vulnerability when faced with the prospect of losing one's data. This will more likely occur in the context of private data as opposed to data in a work context. Hence, we assume that risk appraisal will be influenced through psychological ownership as follows:

> **H2a** *PO of (work and private) data will increase perceptions of threat vulnerability. This effect will be more pronounced in a private context.*
> **H2b** *PO of (work and private) data will increase_perceptions of threat severity. This effect will be more pronounced in a private context.*

Intimate knowledge or a deep understanding and familiarity of an object will lead to higher degrees of association with the object [37]. This is evidenced by individuals' statements of preferring own targets to comparable others, simply because one knows them better, e.g., the favorite spot in the canteen. Acquiring knowledge about a target is also linked to investment of the self into the target which represents the third route to PO. Investing time, effort, or energy into the creation or development of a target, e.g., in a mentor-mentee relationship or into do-it-yourself-projects, facilitates feelings of PO by seeing one's own reflection in the target [34]. In organizational studies, employees who feel PO toward their company are shown to express higher levels of organizational commitment, organizational-based self-esteem, and job performance [36, 38, 39]. Subsequently, Pierce and colleagues argue that pronounced feelings of PO will influence the degree of its effects – both positive and negative [38]. In line with Menard and colleagues, we also expect that PO will exert influence on the coping appraisal considering the use of diverse and strong passwords in both the private and work context [13], and thus hypothesize:

> **H2c** *PO of (work and private) data will increase perceptions of response efficacy. This effect will be more pronounced in a private context.*
> **H2d** *PO of (work and private) data will decrease perceptions of response costs. This effect will be more pronounced in a private context.*

Apart from intimate knowledge of the target, and investment of the self, Pierce and colleagues also argue that perceived control is closely tied to feelings of PO [14]. Numerous studies prove that control is a core feature of ownership as objects that are habitually used or can even be manipulated by an individual become more assimilated into the user's self-concept [17]. According to Avey and colleagues, individuals will be "feeling more efficacious about working with the target, feeling more accountable for what happens with respect to the target" [39, p. 24] when they feel psychologically tied to the target. In our context, PO regarding their data will thus facilitate feelings of responsibility and as a result lead to heightened levels of willingness and confidence in their ability to carry out a protective response against the IS security threat [40].

> **H2e** *PO of (work and private) data will increase perceptions of self-efficacy. This effect will be more pronounced in a private context.*
> **H2f** *PO of (work and private) data will increase perceptions of controllability. This effect will be more pronounced in a private context.*

3 Research Model and Methodology

Our research model draws primarily on the approach of Menard and colleagues [12] which examines how psychological ownership affects the protection motivation based on PMT. We further extend the model with the additional construct of controllability in order to include and examine another important but yet often overlooked aspect of perceived behavioral control. In both contexts, we examine how the behavioral intention to use strong passwords in order to protect data is influenced by both the classic determinants of PMT and how these are in turn influenced by PO in our two contexts.

3.1 Data Collection Procedure

In order to investigate our research questions, we conducted an online survey among employees in Germany who use electronic devices to access software applications or websites and are interacting with company data in their professional environment on an everyday basis. Since comparing work and private contexts involves repeated measures for our research model, certain biases have to be considered and countered. In order to avoid that participants remember their answers from the first context (i.e., work) and aspire to repeat the same answer in the second context (i.e., private) to ensure self-consistency [42], we decided not to survey both contexts (work vs. private) in one single questionnaire. Furthermore, we chose to survey the same panel of respondents (cohorts) for both contexts. This enables us to investigate differences in an individual's perception handling work-related data as well as private data.

As threat scenario we chose the misuse of data caused by insecure passwords. Consequently, the coping strategy depicted the usage of strong passwords which are distinct between different user accounts. Both questionnaires were distributed online in August 2018 in two waves with the help of a market research institute. Seven days upon completion, the same cohort was invited to participate in a second survey assessing their password behavior within their private context. This timespan was chosen in order to avoid manipulating risk appraisal and coping appraisal between both conditions through unforeseen incidents or factors (work vs. private context) and is comparable to other IS studies using a repeated measures design [41, 42]. Using an even longer time-span entails the risk of external influences (security incidents and other message cues) to bias the respondents' perceptions compared to the first wave. Both surveys commenced with a welcome page which ensured the participants' anonymity and that there are no "wrong" answers in order to counteract common method and social desirability biases [13,43].

Only those participants who completed both survey questionnaires were included in the data analyses (N = 217). Since eight participants failed our attention check during the second wave, their answers were deemed unreliable resulting in a final sample size of 209. The effective response rate after the second wave – and the elimination of unreliable responses and attention checks – amounted to 70.37 percent, an acceptable rate for questionnaires considering security-related behavior [e.g., 28, 44].

The sample was evenly distributed in terms of gender (51.2 % female; 48.8 % male) and age (mean = 44.9; min = 19; max = 65) through quotas mirroring the percentage of the overall population in Germany and thus providing an adequate snapshot of reality of German employees. We report a more detailed sample statistic in the online appendix (Table A1).

3.2 Operationalization of Research Variables and Instruments

All measurements to operationalize our research variables are based on previously validated operationalization and have been adapted to the context of our study as we report in the online appendix (Table A2). The items for all threat related PMT constructs (vulnerability [VULN], severity [SEV]) were adopted from Johnston and Warkentin [45]. Items for response efficacy [RE] have been extracted from Witte [46] whereas response costs [RC] as well as self-efficacy [SE] were adapted from Milne at al. [41]. Controllability [CON] was measured using the scale from Kraft and colleagues [47]. Our dependent variable behavioral intention [INT] has been operationalized using items from Herath and Rao [25] whereas psychological ownership [PO] has been adopted from van Dyne and Pierce [38].

4 Data Analysis and Results

Our data set contains 209 responses for each context based on the same respondent cohort. Therefore, we distinguish between two contexts: the work versus the private context. In the following, the hypothesized relationships between variables are analyzed relying on the PLS algorithm as implemented in SmartPLS in order to simultaneously validate the measurement model and the conceptual path model [48].

Measurement Model Testing. We begin by assessing convergent validity of all our variables for each condition (work and private). Internal consistency can be assumed for constructs if Cronbach's alpha (Cr α) as well as composite reliability (CR) are at least 0.7 [49]. To establish convergent validity, the average variance extracted (AVE) should exceed 0.5 [50]. In addition, item loadings are assessed against a threshold of 0.65 or higher [51]. We find minimum loadings of 0.707 / 0.840 in the work and private context respectively. Therefore, we conclude that convergent validity is ensured.

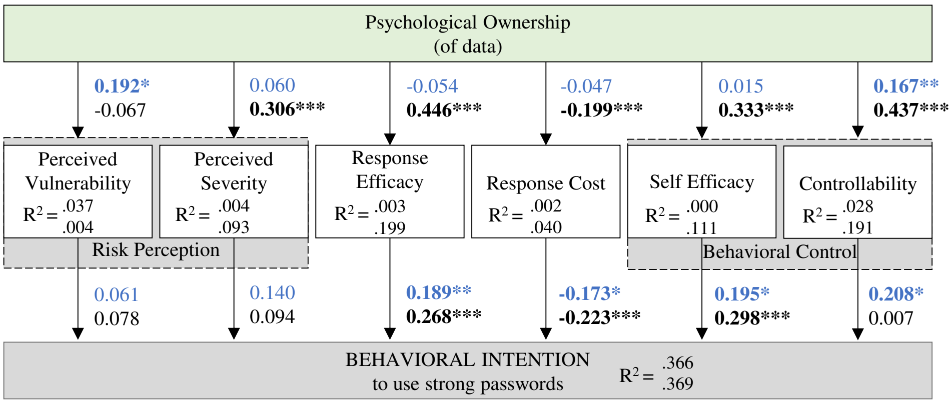
Table 1. Measurement Model Validation

	Work Context										
	Cr α	CR	AVE	CON	INT	PO	RE	RC	SE	SEV	VULN
CON	.915	.937	.790	**.889**							
INT	.948	.967	.906	.383	**.952**						
PO	.906	.941	.843	.167	.095	**.918**					
RC	.940	.957	.848	.252	.403	-.054	**.896**				
RE	.879	.924	.803	-.248	-.399	-.047	-.223	**.921**			
SE	.854	.912	.775	.236	.469	.015	.387	-.662	**.880**		
SEV	.927	.948	.821	.273	.355	.060	.361	-.126	.315	**.906**	
VULN	.794	.859	.606	.004	.001	.192	-.061	.237	-.116	.102	**.778**
	Private Context										
	Cr α	CR	AVE	CON	INT	PO	RE	RC	SE	SEV	VULN
CON	.937	.954	.840	**.916**							
INT	.930	.955	.876	.366	**.936**						
PO	.888	.931	.818	.437	.297	**.904**					
RC	.949	.963	.867	.582	.364	.446	**.898**				
RE	.881	.926	.807	-.354	-.446	-.199	-.070	**.931**			
SE	.881	.927	.810	.399	.514	.333	.189	-.746	**.900**		
SEV	.929	.950	.825	.252	.260	.306	.364	-.080	.137	**.909**	
VULN	.898	.928	.762	-.235	-.102	-.067	-.171	.356	-.209	.095	**.873**

For acceptable discriminant validity, we rely on the criteria suggested by Fornell and Larcker [52]. Accordingly, the square-root of AVE (**bold** numbers in Table 1) needs to be greater than the correlations to all other constructs. Since this holds true for all constructs within both conditions, we assume our measurement model to be accurate as further evidenced by cross loadings reported in the online appendix (Table A3).

Structural Model Testing. Continuing with the validated measurement model, we assess the overall model fit of our conceptual models. The standardized root mean square residual (SRMR) is 0.066 resp. 0.046 (work resp. private) which is well below the cutoff-point of 0.08 recommended by Hu and Bentler, indicating a good model fit [53]. The amount of variance explained within our dependent variables (R^2) are presented in Figure 1. We use a bootstrapping procedure with 5,000 subsamples to test for statistical significance of path coefficient estimates which results are also reported.

Figure 1. Results of the PLS Model Estimation



Condition. top: work | bottom: private ** p<0.05 ** p<0.01 *** p<0.001*

Work context. In the work context, all hypotheses based on PMT (H1c, d, e, f) except for risk perception, i.e., perceived vulnerability and severity, are supported. Furthermore, psychological ownership of data shows only significant influences on the variables perceived vulnerability (H2a) and controllability (H2f).

Private context. The results show that risk perception has no significant influence on behavioral intention to use strong passwords in the private context. Nevertheless, response efficacy, response costs and self-efficacy significantly influence behavioral intention to use strong passwords and thus support H1c, d, e. The expected effect of controllability on behavioral intention is not supported. However, PO has a strong influence on the majority of PMT related constructs (H2b, c, d, e, f supported) whereas the effect on perceived vulnerability could not be supported in the private context (H2a rejected).

Multi Group Analysis. As an extended analysis of the differences between the two contexts, we conducted a multi group analysis. Due to space limitations we report hypotheses which ultimately show significant differences in their path-coefficients only in our online appendix (Table A4). Hereby, the context shows a mediating effect on H1f and H2a as the effects are stronger in the work context compared to the private context. The context furthermore mediates all other relations from psychological ownership. Hence, the effect of psychological ownership is stronger in the private context compared to the work context for H2b, c, d, e, f.

5 Discussion and Contributions

With this study, we contribute to a better understanding of PMT according to the situational context and via an extension through PO. By using a repeated measures design, we are able to demonstrate varying mechanisms leading to the intention to protect either private or work data through strong passwords. Specifically, our results demonstrate that risk appraisal through perceived severity and vulnerability does not significantly affect the intention to use a security measures such as strong passwords which is in line with some recent findings of other researchers [8, 13].

Furthermore, we find significant differences regarding the effect of controllability across contexts: whereas a significant effect of controllability on the intention to use strong passwords indicates that employees feel accountable for their choice, this effect could not be shown among private end-users. This might indicate that they do not even perceive an opportunity to shift control, and thus accountability, to some third party such as the employer. Therefore, we find evidence that individuals in the private context are aware of their sole accountability when responding to security threats. Otherwise, we found the influence of coping appraisal to be generally stronger in a private context.

Similarly, but opposed to the study of Menard and colleagues, we could demonstrate lesser and mostly insignificant effects of PO on PMT antecedents in a work context [13]. PO effects are mostly only significant in a private context apart from the hypothesized influence on perceived vulnerability – which, in turn, is only evident in a work context – and with controllability which is significant in both contexts. Additionally, a post-hoc performed paired t-test ($t(208) = -20.36$; $p < 0.001$) of PO according to the condition work ($M = 3.07$; $SD = 2.77$) or private context ($M = 5.89$; $SD = 1.34$) showed significant differences. Accordingly, we can subsume that PO is more pronounced considering the protection of private data and, as individuals tend to evaluate a target more favorably when they own it, feelings of accountability, responsibility, and investment of the self in the target are stronger [34, 38, 39]. This leads to several potential implications for both theory and practice.

Theoretical Contributions. From a research point of view, our approach is the first to our knowledge that is based on a repeated measures design which enables the comparison of PMT's explanatory power in a work and private context based on the same safeguarding behavior, i.e., the use of strong passwords. Our study contributes to an improved understanding of the relationships within the theory and shows varying support of the general concepts of risk and coping appraisal. Risk perception in isolation does not promote safeguarding measures in any context, whereas the inclusion of controllability could contribute to more thorough understanding of employee intention regarding the use of strong passwords. Additionally, our findings contribute to the still scarce literature on psychological ownership in IS security. IS research and studies on information security in particular, have incorporated PO very rarely and diversely in terms of context and the mode of influence which calls for replication studies as called for by Menard et al. or Anderson and Agarwal [12, 13]. In this regard, we could demonstrate that PO significantly influences several PMT antecedents only in a private context and barely affects the protection motivation among employees.

Practical Implications. As such, our study informs IS scholars but also practitioners about how a sense of ownership can regulate protection motivation and thus lead to the actual use of safeguarding mechanisms like strong passwords. Practitioners in particular should stimulate feelings of PO regarding company data in order to increase protection motivation. PO can, for example, be increased and stimulated by tapping into its antecedents, e.g., through more intimate knowledge of the target, in our case data. Also if employees invest more time and effort into understanding how data can be protected, employees will develop a feeling of freedom of choice and more accountability which in turn increases PO and thus exert a positive effect on safeguarding mechanisms [19].

6 Conclusion, Limitations, and Future Research

Despite taking all necessary measures to ensure qualitative results, our study is not without limitations. In this regard, a typical limitation of behavioral IS theories is the measurement of intention rather than actual behavior. Although intention is widely regarded to be a very robust predictor of actual behavior [29, 54], future research could build onto our findings with an experimental design that observes the influence of PO on actual behavior. Similarly, previous research has identified several other influencing factors like culture or personal characteristics which had to be omitted due to duration constrains but could enhance our understanding about the modes of action of PO in an organizational and individual security context. Especially, since culture has been shown to have an effect of the level of PO expressed, our results could be culturally constrained to Western, more individualistic, cultures [13]. From a methodological point of view, the rather short timeframe of our two surveys might add to the general finding that humans strive for a consistent manner of self-representation which might result in memory effects or so-called experimenter demand effects [42, 43]. However, an extension of the time frame might be affected by unidentifiable external influences due to unforeseen incidents or other biases that arise during the survey period.

An avenue for future research could be the analysis of PO antecedents through an action research design measuring whether increased feelings of PO also lead to improved actual security behavior in both a work and a private context. Our study thus serves as an important stepping stone which first compared the behavior of individuals in these contexts in a repeated measures design revealing varying degrees of effect sizes in well-established PMT and newly hypothesized PO relationships. Furthermore, future research could develop a new operationalization of PO for the IS context, as current measures are often based on physical, tangible targets. A different approach could be the use of an Implicit Association Test which can detect underlying attitudes of users or consumers particularly when subjects are unaware or unwilling to identify sources of influence – like PO in our context [55]. This could prove to be particularly interesting since an additional estimated PLS model including a path from PO to intention showed that no direct influence on intention was found in both contexts as opposed to the previous studies. This could be related to the differences in targets as one’s own device might elicit more pronounced feelings of PO compared to intangible data or the operationalization of PO through scenario manipulation and represents another possible avenue for future research [11].

7 Acknowledgments

This research project was funded by “Hessisches Ministerium des Innern und für Sport”. We express our gratitude to everybody involved in enabling us with the conduct of this study – in particular to Henrik Schlünkes and Zhengchao Wu.

References

1. IBM: The Flood of Big Data - Driving Marketing Effectiveness by Managing, http://www.ibmbigdatahub.com/infographic/flood-big-data (Accessed: 08.08.2018)
2. Statista: Global Digital Population as of July 2018, https://www.statista.com/statistics/617136/ (Accessed: 08.08.2018)
3. Verizon: Verizon Data Breach Investigations Report, https://www.ictsecuritymagazine.com/wp-content/uploads/2017-Data-Breach-Investigations-Report.pdf (Accessed: 08.08.2018)
4. Schneier, B.: Secrets and Lies: Digital Security in a Networked World. John Wiley and Sons., New York, NY (2000)
5. Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M., Baskerville, R.: Future Directions for Behavioral Information Security Research. Comp. & Sec. 32, 90-101 (2013)
6. Lebek, B., Uffen, J., Neumann, M., Hohler, B., Breitner, M.: Information Security Awareness and Behavior: A Theory-based Literature Review. Management Research Review 37, 1049-1092 (2014)
7. Mayer, P., Kunz, A., Volkamer, M.: Reliable Behavioural Factors in the Information Security Context. 12th International Conference on Availability, Reliability and Security, Reggio Calabria, Italy (2017)
8. Boss, S.R., Galletta, D.F., Lowry, P.B., Moody, G.M., Polak, P.: What do Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Behaviors in Users. MIS Quarterly 39, 837-864 (2015)
9. Bulgurcu, B., Cavusoglu, H., Benbasat, I.: Information Security Policy Compliance: an Empirical Study of Rationality-based Beliefs and Information Security Awareness. MIS Quarterly 34, 523-548 (2010)
10. Mou, J., Cohen, J., Kim, J.: A Meta-Analytic Structural Equation Modeling Test of Protection Motivation Theory in Information Security Literature. 38th International Conference on Inf. Systems (ICIS), Seoul, South Korea (2017)
11. Davison, R.M., Martinsons, M.G.: Context is King! Considering Particularism in Research Design and Reporting. Journ. of Inf. Technology 31, 241-249 (2016)
12. Anderson, C.L., Agarwal, R.: Practicing Safe Computing: A Multimedia Empirical Examination of Home Computer User Security Behavioral Intentions. MIS Quarterly 34, 613-643 (2010)
13. Menard, P., Warkentin, M., Lowry, P.B.: The Impact of Collectivism and Psychological Ownership on Protection Motivation: A Cross-Cultural Examination. Comp. & Sec. 75, 147-166 (2018)
14. Pierce, J.L., Kostova, T., Dirks, K.T.: Toward a Theory of Psychological Ownership in Organizations. Academy of Management Review 26, 298-310 (2001)

15. Duncan, N.G.: Home Ownership and Social Theory. In: Duncan, J.S. (ed.) Housing and Identity: Cross-Cultural Perspectives, pp. 98-134. Croom Helm, London (1981)
16. Dittmar, H.: The Social Psychology of Material Possessions: To Have Is to Be. Hemel Hampstead, Harvester Wheatsheaf and St Martin's Press, New York (1992)
17. Furby, L.: Understanding the Psychology of Possession and Ownership. Social Behavior and Personality 6, 49-65 (1978)
18. Cichy, P., Salge, T.O., Kohli, R.: Extending the Privacy Calculus: The Role of Psychological Ownership. 35th International Conference on Information Systems (ICIS), Auckland (2014)
19. Klesel, M., Ndicu, M., Niehaves, B.: Exploring Psychological Ownership of IT: An Empirical Study. 24th European Conference on Inf. Systems (ECIS , Istanbul, Turkey (2016)
20. Straub, D., Welke, R.: Coping with Systems Risk: Security Planning Models for Management Decision Making. MIS Quarterly 22, 441-469 (1998)
21. Liang, H., Xue, Y.: Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective. Journ. of the Association for Inf. Systems 11, 394-413 (2010)
22. Hansen, J.V., P.B., L., R., M., McDonald, D.M.: Genetic Programming for Prevention of Cyberterrorism through Dynamic and Evolving Intrusion Detection. Decision Support Systems 43, 1362-1374 (2007)
23. Cavusoglu, H., Raghunathan, S., Cavusoglu, H.: Configuration of and Interaction between Information Security Technologies: The Case of Firewalls and Intrusion Detection Systems. Inf. Systems Research 20, 198–217 (2009)
24. Willison, R., Warkentin, M.: Beyond Deterrence: An Expanded View of Employee Computer Abuse. MIS Quarterly 37, 1-20 (2013)
25. Herath, T., Rao, H.R.: Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations. Europ. Journ. of Inf. Systems 18, 106-125 (2009)
26. Floyd, D.L., Prentice-Dunn, S., Rogers, R.W.: A Meta-Analysis of Research on Protection Motivation Theory. Journ. of Applied Social Psychology 30, 407-429 (2000)
27. Pahnila, S., Siponen, M., Mahmood, A.: Employees' Behavior towards IS Security Policy Compliance. 40th Annual Hawaii International Conference on System Sciences (HICSS), Hawaii, US (2007)
28. Crossler, R.E.: Protection Motivation Theory: Understanding Determinants to Backing Up Personal Data. 43rd Annual Hawaii International Conference on System Sciences (HICSS), Hawaii, US (2010)
29. Ajzen, I.: The Theory of Planned Behavior. Organizational Behavior and Human Decision Processes 50, 179–211 (1991)
30. Ajzen, I.: Perceived Behavioral Control, Self-Efficacy, Locus of Control, and the Theory of Planned Behavior. Journ. of Applied Social Psychology 32, 665-683 (2002)
31. Bandura, A.: Self-Efficacy: Toward a Unifying Theory of Behavioral Change. Psychological Review 84, 191-215 (1997)
32. Workman, M., Bommer, W.H., Straub, D.: Security Lapses and the Omission of Information Security Measures: A Threat Control Model and Empirical Test. Computers in Human Behavior 24, 2799-2816 (2008)
33. Webb, T.L., Sheeran, P.: Does Changing Behavioral Intentions Engender Behavior Change? A Meta-Analysis of the Experimental Evidence. Psychological Bulletin 132, 249-268 (2006)
34. Pierce, J.L., Kostova, T., Dirks, K.T.: The State of Psychological Ownership: Integrating and Extending a Century of Research. Review of General Psychology 7, 84-107 (2003)
35. Lee, Y., Chen, A.N.K.: Usability Design and Psychological Ownership of a Virtual World. Journ. of Management Inf. Systems 28, 269-307 (2011)
36. Vandewalle, D., Van Dyne, L., Kostova, T.: Psychological Ownership: An Empirical Examination of its Consequences. Group & Organization Management 20, 210-226 (1995)

37. Rudmin, F.W., Berry, J.W.: Semantics of Ownership: A Free-recall Study of Property. Psychological Record 37, 257–268 (1987)
38. Van Dyne, L., Pierce, J.L.: Psychological Ownership and Feelings of Possession: Three Field Studies Predicting Employee Attitudes and Organizational Citizenship Behavior. Journ. of Organizational Behavior, 439-459 (2004)
39. Avey, J.B., Avolio, B.J., Crossley, C.D., Luthans, F.: Psychological Ownership: Theoretical Extensions, Measurement and Relation to Work Outcomes. Journ. of Organizational Behavior 30, 173-191 (2009)
40. Dipboye, R.L.: A Critical Review of Korman's Self-Consistency Theory of Work Motivation and Occupational Choice. Org. Beh. and Human Perf. 18, 108-126 (1977)
41. Milne, S., Orbell, S., Sheeran, P.: Combining Motivational and Volitional Interventions to Promote Exercise Participation: Protection Motivation Theory and Implementation Intentions. British Journ. of Health Psychology 7, 163-184 (2002)
42. Kehr, F., Kowatsch, T.: Quantitative Longitudinal Research: A Review of IS Literature, and a Set of Methodological Guidelines. 23rd European Conference on Inf. Systems (ECIS), Münster, Germany (2015)
43. Podsakoff, P.M., MacKenzie, S.B., Leong-Yeon, L., Podsakoff, N.P.: Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies. Journ. of Applied Psychology 88, 879-903 (2003)
44. Sonnenschein, R., Loske, A., Buxmann, P.: Gender Differences in Mobile Users' IT Security Appraisals and Protective Actions: Findings from a Mixed-Method Study. 37th International Conference on Inf. Systems (ICIS), Dublin, Ireland (2016)
45. Johnston, A.C., Warkentin, M.: Fear Appeals and Information Security Behaviors: An Empirical Study. MIS Quarterly 34, 549-566 (2010)
46. Witte, K.: Predicting Risk Behaviors: Development and Validation of a Diagnostic Scale. Journ. of Health Communication 1, 317-342 (1996)
47. Kraft, P., Rise, J., Sutton, S., Røysamb, E.: Perceived Difficulty in the Theory of Planned Behaviour: Perceived Behavioural Control or Affective Attitude? British Journ. of Social Psychology 44, 479-496 (2005)
48. Bagozzi, R.P., Yi, Y.: On the Use of Structural Equation Models in Experimental Designs. Journ. of Marketing Research 26, 271-284 (1989)
49. Bagozzi, R.P., Yi, Y.: Specification, Evaluation, and Interpretation of Structural Equation Models. Journ. of the Academy of Marketing Science 40, 8-34 (2012)
50. Hair, J.F., Ringle, C.M., Sarstedt, M.: Partial Least Squares Structural Equation Modeling: Rigorous Applications, Better Results and Higher Acceptance. Long Range Planning 46, 1-12 (2013)
51. Falk, R.F., Miller, N.B.: A Primer for Soft Modeling. University of Akron Press, Akron, Ohio (1992)
52. Fornell, C., Larcker, D.F.: Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. Journ. of Marketing Research 18, 39-50 (1981)
53. Hu, L.-T., Bentler, P.M.: Fit Indices in Covariance Structure Modeling: Sensitivity to Underparameterized Model Misspecification. Psychological Methods 3, 424-453 (1998)
54. Fishbein, M., Ajzen, I.: Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research. Addison-Wesley, Reading, MA (1975)
55. Brunel, F.F., Tietje, B.C., Greenwald, A.G.: Is the Implicit Association Test a Valid and Valuable Measure of Implicit Consumer Social Cognition? Journ. of Consumer Psychology 14, 385-404 (2004)