Having Two Conflicting Goals in Mind: The Tension Between IS Security and Privacy when Avoiding Threats

Christian M. Olt
Technische Universität Darmstadt
olt@is.tu-darmstadt.de

Amina Wagner
Technische Universität Darmstadt
wagner@is.tu-darmstadt.de

Abstract

Despite users of personal IT devices perceive high risks of losing their personal data if their devices get lost or damaged, many are reluctant to use user-friendly online services (i.e., online backups) to recover from such incidents. We suggest that the reason for this denial are information privacy concerns because users need to disclose their personal files to the safeguard provider. As safeguarding services promise to reduce the IS security threat of losing data, individuals are subsequently tensed between two goals: protecting their data against loss (IS security) and their information privacy. To shed light on this goal conflict, our work builds on the theory of goal-directed behavior. Based on a quantitative online survey among 446 participants, we show that privacy concerns impede threat avoidance to prevent data loss. Comparing current users and non-users of online backup services, our results confirm that provider-related privacy concerns are significantly higher for non-users.

1. Introduction

Imagine Claire, being on holiday in a foreign country. Meanwhile, she uses her smartphone to take pictures and to write down her experiences and memories. Storing personal information on her smartphone without adequate security applications in place, it is conceivable that those get lost [1]. Resulting from this situation, Claire feels vulnerable facing this semi-catastrophic security threat. Luckily, she heard about the possibility to secure her data against loss in an online backup (e.g., Android Backup, iCloud backup or third party apps). As soon as her smartphone is connected to a WiFi network, all pictures, her writing and all other data stored on her smartphone are uploaded to a safe online storage. Although this online backup seems to be effective in protecting her personal data against loss, Claire has second thoughts — she is concerned that the provider of the online backup gains access to her private data and could subsequently use her information in an unforeseen way [2]. Thus, Claire feels tensed between the chance to protect her data against loss caused by her smartphone being stolen or damaged (IS security goal) and the risk that she loses control over her data by uploading it to a safeguard provider (information privacy goal). In this vein, the question whether privacy or security is the predominant goal arises. Should she nevertheless upload her valuable but personal data to this online storage?

This exemplary decision process of an individual striving to carefully handle her personal data demonstrates that security (i.e., availability) and privacy of personal data is not always the same side of a coin. Instead, they may stand in conflict. Against this background, prior literature addressing IS security behavior is at least limited in two ways. First, using security safeguards as well as disclosing personal information to service providers have mostly been understood and studied as two independent behavioral aspects of IS usage [e.g., 2, 3, 4-7]. IS security research states that *threat avoidance behavior* in terms of using IS security safeguards is mainly determined by the perception of security threats, such as the consequences of a stolen personal IT device or hackers infecting an IS with e.g., ransomware and causing harm [4]. In contrast to this, information privacy research is guided by the privacy calculus model [7] which links privacy concerns to information disclosure intentions. As both research streams try to explain antecedents of IS usage behavior, a junction of IS security and privacy research is necessary. Only very few scholars bridged those research streams, e.g., Zhang, et al. [8], but further examination seems promising.

Second, the reluctance of individuals to use available security safeguards is not yet fully understood. Past literature has pointed to this lack of understanding why individuals do not intend to use a security safeguard even though they perceive a high security threat [3, 9]. Beyond that, scholars agree that research on IS security behavior needs to integrate new technical and behavioral approaches [10].

Drawing on the theory of goal directed behavior [11], we postulate that privacy concerns resemble a conflicting goal of IS security that provide an explanation why individuals still hesitate to use effective security safeguards. Therefore, we investigate the tension between privacy and security based on threat avoidance theory [4] in the light of using online safeguarding services. Against this

URI: https://hdl.handle.net/10125/64258
978-0-9981331-3-3

background, our study investigates the following research questions:

RQ1: Does protecting IS security stand in conflict to the goal of maintaining information privacy when using online safeguarding services?

RQ2: How does this goal conflict differentiate between users and non-users of those services?

To accomplish these research goals, we begin with the theoretical background, explaining goal driven behavior and its relevance to understand the antecedents of threat avoidance behavior. This is followed by the introduction of information privacy concerns as conflict to IS security and the development of a research model. To support our theoretical reasoning, we provide empirical evidence based on an online survey among 446 smartphone users. As such, our research aims to add to IS research by bridging the IS security and information privacy literature. Beyond implications for research, we create awareness among security safeguard providers to address individual's privacy concerns. Thus, providers caring for information privacy can also be a competitive factor for those who offer solutions to protect security.

2. Theoretical Background

In this section we provide a theoretical basis for the tension between perceived IS security threats and information privacy concerns in the context of threat avoidance behavior. Subsequently, we integrate the theory of goal directed behavior (Carver and Scheier 2000) along with its underlying goal conflicts (Segerstrom and Nes 2006) into the theory of threat avoidance behavior [4].

2.1 Security as Avoidance Goal

Setting goals and striving for goals is an important aspect to explain individuals' IS usage behavior [12]. In IS research, the underlying goals that humans strive to achieve determine usage intention of technologies [13]. Goals can be pictured as reference values that individuals have in mind and compare against their current state. Hence, using an IS changes someone's current state towards certain goals [11].

With regard to IS security behavior and safeguarding personal data, Liang and Xue [4] explain that avoiding IS security threats is a goal as well that determines a cognitive appraisal process whether to use a safeguard. For example, being infected by malware is a negative reference value which individuals strive to avoid. Thereby, threat avoidance behavior is derived from the underlying goal to circumvent a malicious IS security incident [11].

2.2 Privacy as Conflicting Goal

As argued by Conger and Landry [14] and Smith, et al. [2], information privacy is a concept which needs to be distinguished from IS security. Information privacy concerns rather deal with the expected use of personal information by a service provider, subsequent to disclosing information to that specific provider [2] whereby security threats jeopardize confidentiality, integrity and availability of data against a possibly unknown source (e.g., malware, hackers, fire, unintended manipulation/deletion). For this reason, privacy scholars emphasize that IS security measures are indeed necessary to establish information privacy but not sufficient [2]. Therefore, even if a safeguard against security threats is effective in reducing a perceived security threat, this does not necessarily imply that the user's information privacy is ensured.

Using a safeguarding service for the means of reliable protection against security threats on the user's side, as Claire is about to do, this threat avoidance behavior results in a second consequence. Usage of safeguarding services comprises personal data being collected, stored and processed by the service provider [e.g., 15]. The very same provider can subsequently use this information in an unpredictable manner or even share it with third parties (e.g., data-brokers or cooperating firms). This is associated with a worry about organizational information practices [16]. Thus, privacy concerns refer to individuals' perceived extent of loss of control over their personal data [2]. This perceived loss is conceptualized as "perceived risks of information disclosure" and has been largely investigated as an impediment of transacting with a provider in general [e.g., 17, 18] and disclosure intentions in particular [e.g., 19, 20].

Against the background of IS privacy research, we conceive user's information privacy as second goal which individuals pursue in the context of using IS. When following the IS security goal by using a safeguarding service, personal data would be protected against threats concerning the user's device (e.g., availability of data, in case Claire loses her personal data stored on her smartphone) [21]. However, using a safeguarding service also contradicts the information privacy goal. Hence, a goal conflict arises which results in a cognitive tension when individuals try to succeed in both goals [22]. As a consequence, users disengage their goal pursuit and ultimately in termination of the threat avoidance behavior itself [23]. Figure 1 depicts the main idea of conflicting goals resulting from an IS security behavior relying on a safeguarding service.

Notably, the process of goal directed avoidance behavior does not only result in active threat

avoidance behavior postulated by IS security research [e.g., 4], it can also lead to disengagement of pursuing the IS security goal. In this case, it is not possible to simultaneously achieve the security as well as the privacy goal. To exemplify this tension: using a VPN in a public WiFi (protecting confidentiality) implies that the VPN provider reads all unencrypted information – thus information disclosure to the service provider is necessary in order to secure data. Hence, individuals have two conflicting goals in mind and find themselves in an avoidance dilemma.

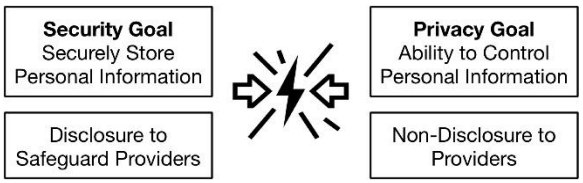

Figure 1. Conflict of Goals

3. The Security-Privacy Goal Conflict

In the following, we investigate whether IS security and information privacy are indeed two conflicting goals when individuals form intentions to avoid threats by using safeguarding service. Our research model (Figure 2) illustrates all hypotheses which we develop in this section and in particular the expected goal conflict between IS security and information privacy.

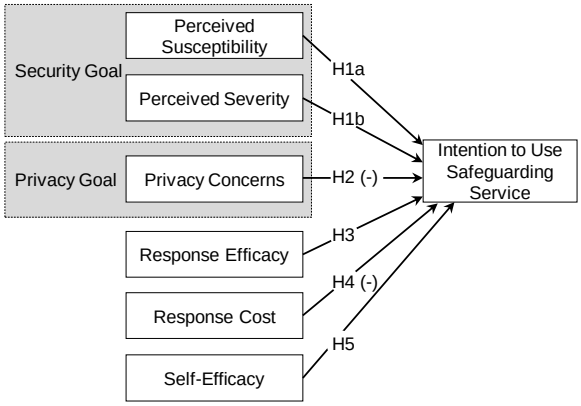

Figure 2. Research Model

The cognitive process determining threat avoidance is two-folded: preliminary threat appraisal and subsequent coping appraisal [4, 6]. Threat appraisal lets individuals form an expectation about the risk of an IS being attacked or personal data being manipulated or deleted. When a specific threat is perceived as sufficiently harmful, the search for an effective and easy-to-use safeguard begins [3]. In the context of IS security, this commonly implies using of anti-malware [21], strong passwords [24] or running backups [6]. Following the rationale of threat avoidance theory [4], we hypothesize the perceived susceptibility as well as severity of an IS security threat to be two variables promoting the intention to use a safeguarding service:

***H1a**: Perceived threat susceptibility increases the individual's intention to use a safeguarding service.*
***H1b**: Perceived threat severity increases the individual's intention to use a safeguarding service.*

When individuals appraise the threat to IS security as harmful, they begin to evaluate available safeguards in order to protect against the risk and consequently achieve their IS security goal. During this coping appraisal, individuals evaluate what is necessary to actually use a safeguard in question [4].

As explicated in the previous section, using safeguarding services entails the disclosure of users' personal information to the service provider. In order to account for individuals' privacy concerns, several studies in the field of e-commerce and social networks have relied on the privacy calculus model to show how they affect the intention to use a privacy-invasive system in general or the intention to disclose in particular [e.g., 7, 19, 25]. They all share one common approach: The higher the perceived privacy concerns, the lower the intention to disclose personal information and thus the likelihood of transacting with the provider [7]. Adding to this, a recent study also showed that users of mobile cloud services (i.e. backup services) may very well perceive privacy concerns [20]. Hence, even though valuable data could be effectively secured by the safeguard provider and external threats averted, the provider could still treat the data in a privacy invasive way. In line with privacy research, we argue that using a safeguarding service to achieve effective protection, for which disclosure of personal data is necessary, the same negative effect of privacy concerns arises:

***H2**: Information privacy concerns decrease individual's intention to use a safeguarding service.*

Beside the promoting and inhibiting effects derived by both conflicting goals, technological aspects may determine coping appraisal in terms of threat avoidance, hence the intention to use a safeguard. As briefly mentioned previously, the safeguard's effectiveness perceived by the user is imperative when evaluating the avoidability of an IS security threat [21]. Literature within the field of IS security often relies on the term 'response efficacy' to describe the effectiveness of a safeguard in alleviating an IS security threat [e.g., 5]. It has also been shown in previous studies that the individual's perception of response efficacy is one of the main drivers to use one specific safeguard such as anti-malware [26], strong

passwords and data encryption [1] as well as fake website detectors [9]. We therefore hypothesize:
***H3**: Perceived response efficacy increases individual's intention to use a safeguarding service.*

Next to response efficacy, coping appraisal further comprises all resources necessary to use a safeguard are included in response costs. Hereby, especially inconvenience that results from threat avoidance behavior is the most relevant predictor of response cost [27]. When individuals perceive the adoption and usage of a safeguarding service as effortful, this decreases the usage intention [28]. As a result, we postulate the following:
***H4**: Perceived response cost decreases individual's intention to use a safeguarding service.*

Finally, perceived self-efficacy is referred to as the user's ability to actually perform all required actions to initiate and sustain a certain coping behavior [21]. Therefore, the intention to use a safeguarding service is also determined by the extent of perceived self-efficacy fulfilling all actions necessary to be protected [3]. In line with this reasoning, we hypothesize that:
***H5**: Perceived self-efficacy increases individual's intention to use a safeguarding service.*

4. Empirical Study

To emphasize on the tension between security and privacy as conflicting goals, we chose the loss of personal data stored on individual's smartphones as the security threat scenario. Loosing personal data is a relevant aspect of IS security since one aspect of protection is avoiding an accidental or unintended data loss [28, 29]. Hence, we particularly focus on the availability of personal data as main interest (next to integrity and confidentiality of data). We agreed on personal data which is stored on the smartphone, because it is that device where individuals store most of their personal information [30] and which consequently should be stored safely. As safeguarding service, we relied on a fictive mobile application which regularly creates backups of personal data and uploads those to an online storage. Thus, it enables the user to restore files in the case of data loss. An online backup is a suitable case, since the same data that users strive to protect against an external risk of data loss has to be transmitted and disclosed to the provider of the safeguarding service (i.e., the mobile application and online storage). Subsequently, it is assumed to create privacy concerns [31] – remember Claire, for example, having second thoughts. Moreover, the use of backups to prevent data loss is not only a common approach in IS security research [6, 32], it should also be known smartphone users as IS security recommendation.

We deliberately chose a hypothetical scenario, because contextual factors have been found to substantially impact threat avoidance behavior [10] and moreover it has been shown to be successful in controlling independent variables and in obtaining construct validity [33]. In order to investigate our research questions and test our hypotheses, we followed a quantitative approach which helped us to investigate whether smartphone users perceive information privacy concerns regarding the disclosure of personal data in the context of using an online backup as safeguarding service.

4.1 Measurements

Based on the above scenario, we created an online survey relying on established scales in IS research. All constructs were measured on a 7-point Likert scale ranging from "strongly disagree" to "strongly agree". The survey commenced with a welcome page informing about the purpose of the study and that there are no right or wrong answers as well as ensuring participant's anonymity to counteract common method biases [34]. All measurements have been taken from established literature and have been adapted to the context of our scenario. We report all items and original references in the Appendix.

Despite of these constructs in our conceptual model, we additionally measured demographics (age, gender, education, profession) and a marker variable to test for common method bias [35]. At the survey's very end, the participants were asked, if they currently use any online backup application that protects their personal data from being lost in case of an accident or device theft. As such, we were able to analyze the magnitude of security threat and privacy concern perceptions between current and non-users of an online backup and thus respond to RQ2.

4.2 Pretest and Sample Characteristics

In order to ensure that the hypothetical description of the online backup service as well as the item's phrasing are comprehensive, we conducted a pretest among a student sample of 43 participants within Germany. Afterwards, minor changes have been applied to the scenario description. We thereon invited participants with the assistance of a market research agency all located in Germany; justification for this approach can be found in Lowry, et al. [36]. In total, we obtained 481 completed questionnaires. We added one question instructing the participants to respond a specific value to identify careless answers [37]. As a

result, we excluded 35 respondents from the analysis since those did not respond correctly and in turn we deem the answers as not reliable. Finally, the remaining sample size was 446.

212 respondents (48.6%) are females, while 234 are males (52.4%). Our respondents were aged between 18 and 71 years with a sample's mean age of 38.15 years. Regarding employment status, the major group was employed (60.31%), followed by students (13.45%). The educational background was distributed among secondary school (5.16%), junior school (28.03%), high school (33.86%) and bachelor or master degree (32.96%).

5. Results

To begin reporting the study results, we evaluate the validity of our measurement model. Thereon, we continue by analyzing our hypothesized relationships between constructs of the structural model. We used a PLS algorithm as implemented in SmartPLS [38] to validate the measurement model. Relying on PLS allowed us to validate the measurement model and to test our conceptual path model simultaneously [39].

5.1 Measurement Model Validation

In order to assess item reliability of our measurement model, we checked the items' loadings with their respective construct. As the lowest loading is 0.76, we deem our measurement model as reliable [40]. We report convergent validity constructs by Cronbach's alpha (Cr. α) and composite reliability (CR) (Table 1). Convergent validity can be assumed for constructs with a Cr. α of at least 0.7 [41] and CR greater than 0.7 [41]. Furthermore, average variance extracted (AVE) should be at least 0.5 [42].

Table 1. Reliability and Validity

					Corralation Matrix and Sqrt of AVE						
	Constructs	Cr. α	CR	AVE	1	2	3	4	5	6	7
1	Perc. Susc.	0.75	0.85	0.66	**0.81**						
2	Perc. Vuln.	0.96	0.98	0.93	0.18	**0.97**					
3	Priv. Conc.	0.97	0.97	0.91	0.20	-0.01	**0.95**				
4	Resp. Eff.	0.95	0.97	0.90	0.16	0.24	-0.22	**0.95**			
5	Resp. Cost	0.92	0.95	0.86	0.08	0.06	0.13	-0.26	**0.93**		
6	Self-Eff.	0.97	0.98	0.94	0.04	0.00	0.08	0.27	-0.48	**0.97**	
7	Int. to Use	0.98	0.99	0.96	0.12	0.36	-0.41	0.50	-0.07	0.04	**0.98**

We additionally report a correlation matrix for all constructs as depicted in Table 1. The square root of the AVE for all constructs is reported along the main diagonal. To test for acceptable discriminant validity of constructs, the square root of AVE needs to be greater than the correlation to all other constructs [43]. We conclude that all necessary requirements for item reliability as well as convergent validity and discriminant validity for all latent variables of the measurement model are met.

5.2 Analysis of Structural Model

Based on the validated measurement model, we continue to assess the overall model fit of our structural model (Figure 3). The standardized root mean square residual (SRMR) is 0.049 what is below the cut-off criteria of 0.08 and thus indicates a good model fit [44]. Furthermore, the predictive validity of our model can be measured by the amount of variance explained for the dependent variable (intention to use a safeguarding service) of $R^2 = 43.8\%$.

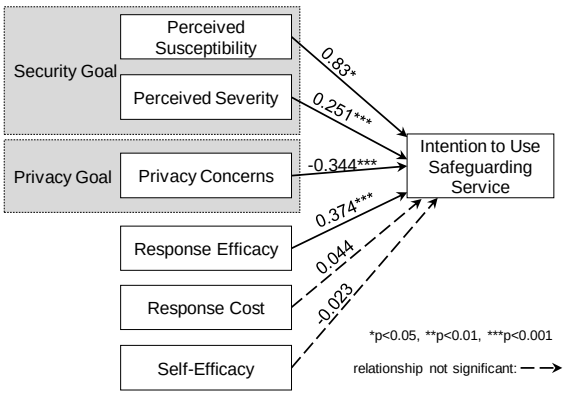

Figure 3. Results

Using a bootstrapping procedure with 5,000 subsamples, we tested for statistical significance of path coefficient estimates in our structural model. Hereby, paths from perceived severity, privacy concerns and response-efficacy to usage intention are significant at $p < 0.001$ as well as perceived susceptibility to usage intention ($p = 0.035$). The path-coefficient is positive for perceived susceptibility, severity, and response efficacy, negative for privacy concerns. This corresponds to our hypotheses H1a/b, H2 and H3 which are thus supported. However, two paths turned out to show only insignificant effects. Results for perceived response cost ($p = 0.372$) and perceived self-efficacy ($p = 0.620$) lead us to reject H4 and H5.

We additionally test for common method bias which could be an issue in our data [34] based on our marker variable, following the guidelines by Rönkkö and Ylitalo [45]. Including the tendency to fantasize when predicting our single endogenous variable (protection motivation), no path-coefficients in our research model became statistically insignificant. In this light, we conclude that our data is not compromised by common method bias [45].

5.3 Post-Hoc Analysis of the Goal Conflict

Moving beyond the analysis of our model relationships, we conducted a further post-hoc analysis of our data. This gives us deeper insights, to what extent the level of threat perception and privacy concerns differ between current (n=89) and non-users (n=348) of safeguarding services (i.e., online backup).

To investigate if a difference in perception of security threat or privacy concern exists between those groups, we rely on the independent samples Mann-Whitney U test [46]. We hereby test for a median difference between both groups for all goal conflict related variables (perceived susceptibility, perceived vulnerability, information privacy concern).

We find no statistically significant difference between the groups neither for perceived susceptibility ($z=1.524$, $p=0.127$) nor for perceived severity ($z=1.579$, $p=0.114$). Hence, individuals who are currently using online backups do not show a significantly higher threat perception of losing personal data. However, individuals who currently use an online backup application have lower privacy concerns (median=4.5) related to providers of safeguarding services such as the one we described within our hypothetical scenario compared to non-users (median=5.5). This difference is statistically significant ($z=-5.031$, $p<0.001$). Hence, current users of online backups did perceive significantly lower privacy concerns compared to non-users based on the presented scenario of the safeguarding service.

6. Discussion and Implications

The goal of this empirical study was to evaluate the tension of IS security and information privacy as two conflicting goals [22] related to providers of safeguarding services. We extend theory on threat avoidance behavior based on an empirical study among 446 smartphone users and show that perceived privacy concerns impede individuals' intention to use safeguarding services. Furthermore, we provide evidence that current users and non-users of online backups do not differ in their security threat perception but in their perceived privacy concern. This indicates that privacy concerns are indeed a major inhibitor of usage even if the security goal is still present.

6.1 Implications for Research

Based on our results, we contribute to theory in several ways. First, our study sets itself off as it bridges established IS security research building on threat avoidance behavior [4] and IS privacy research guided by the privacy calculus model [7, 47]. IS security research so far understands threat avoidance behavior as driven by the single goal of security [4]. We include a second goal stemming from privacy research into the cognitive processes of threat and coping appraisal [e.g., 2, 7, 16, 48]. We therefore connect IS security and information privacy perspectives building on theory of goal directed behavior. In this vein, we provide evidence that privacy concerns also need to be taken into account as an antecedent of threat avoidance behavior.

Second, we demonstrate the tension between privacy and security as two conflicting goals. Perceived security threats and privacy concerns are not always directed to the same goal of keeping information safe and private, as assumed in previous research [e.g., 1, 49]. We emphasize the importance of the concern to lose control over personal information against the background of threat avoidance behavior and find the goal of IS security being impaired by the goal of information privacy. As a consequence, individuals in our sample perceive privacy concerns, which are negatively linked to the intention to use safeguarding services (H2 supported). As we also find support for established promotors of threat avoidance behavior, such as perceived threat (H1a/b supported) and perceived response efficacy (H3 supported), this conveys our postulated tension between both avoidance goals.

Other technological factors, such as response cost (measured as effort) and self-efficacy in using an online backup, have diminished in explaining threat avoidance behavior. Since we are not the first, who find response cost to have no significant effect on intention to use a safeguard [10, 50], we believe that the majority of smartphone users do not perceive effort as hurdle for using safeguarding services (H4 not supported). Similar to this argument, self-efficacy in using a fictive but realistic safeguard service does not impede usage intention (H5 not supported). Taken together, privacy concerns have been found as the sole impediment of threat avoidance behavior in our data.

Third, we also tested for group differences in the goal related construct's median levels. Users and non-users of online-backups perceive the threat of losing personal data as similarly significant. One explanation for this finding would be, that threat appraisal is a cognitive process which happens *earlier* than coping appraisal. Even if threat appraisal creates a similar need of coping for both groups, different strategies to reduce the threat perception are possible [4]. Our interpretation of this finding is that current users as well as non-users run through a similar threat appraisal process but form different expectations regarding the usage of our proposed safeguard. This conclusion seems to be valid since we found empirical support for

H2 and find significant differences within the levels of perceived privacy concerns during the post-hoc analysis: Non-users of security safeguards are subject to greater privacy concerns and are reluctant to use further safeguards although the IS security goal remains unchanged.

Thus, we conclude that actual users of safeguarding services and non-users perceive a different level of tension between threat levels which motivates coping appraisal and privacy concerns and inhibits safeguarding behavior. This finding further supports our novel perspective of conflicting goals within protection motivation theory.

6.2 Managerial Implications

Our findings also offer timely implications for providers of safeguarding services. So far, most data driven companies (such as Google or Facebook) are getting bad publicity due to their propensity to collect personal data of their clients [51, 52]. Security safeguard providers on the other hand can easily be considered as "the good guys", since their mission is to safeguard their client's information systems and personal data. Protection against external threats is however not sufficient any more to mitigate all risks and concerns, their customers are burdened with. Since user data is also transmitted to the service provider, and this is especially the case for valuable files to be protected, a trade-off is indispensable.

Providers of security safeguards should instead foster new means to maintain user's information privacy in order to avoid being regarded as a "bad guy" and even gain a competitive advantage in the market of safeguarding services. There are past examples of information privacy being invaded either by the service provider itself [e.g., Windows 10's malware detection mechanism: 53] or by adversaries breaching into the provider's information systems [e.g., iCloud hack: 54]. These examples show even more that service providers who focus on secure products can easily receive a bad reputation when their customer's privacy is invaded. We thereby suggest that safeguard providers should not only invest resources in enhancing their protective capabilities on their client's side. It is necessary to strengthen information privacy as well, especially when sensible data is being collected, stored and processed in order to detect intruders and avert other threats. The tension between the user's security threat perception and privacy concern should thus be considered by providers in a similar vein, when choosing their protection strategy.

Governmental regulations which are privacy friendly, can furthermore be used by safeguard providers to gain a competitive advantage. When customers choose among different safeguarding services, companies which operate in countries with privacy friendly regulations in place, should be preferred [55].

7. Limitations and Future Research

Our study certainly has its limitations which give good reason to further validate and challenge our findings. First of all, the context and scenario we presented to our participants was the use of a mobile application to backup personal data online in an automated fashion. This case has its justification, since individuals disclose exactly that information to the provider which should be protected against data loss. But since this pertains particularly to availability of data, it would be interesting to see whether researchers can replicate our results in different security-related contexts such as VPN services, password managers, anti-malware or spam filters for e-mail. Hence, we suggest to further validate this goal conflict between privacy and security for confidentiality and integrity of data.

The second limitation is that we surveyed for self-stated intention to use the proposed online backup which may differ from actual behavior. However, given that previous studies have demonstrated a clear relationship between intentions and actual behavior [56], and the approach of online questionnaires and scenarios is a common in IS research [e.g., 1, 21, 27], we deem this methodology to be suitable to test this new relation of security and privacy.

A third limitation lies within the sample we chose. Compared to different cultures, such as from Asia or the U.S., population in Europe commonly has higher privacy concerns [15]. However, especially after the misuse of personal information by Cambridge Analytica, there are indicators that information privacy gains in importance also for U.S. citizens [57]. It would be still interesting to investigate whether the multidimensionality of IS security behavior is moderated by cultural aspects as well [10, 24].

We suggest to further elaborate on the cognitive tension between security and privacy related aspects of IS security behavior. In this respect, future research can not only extend the scope of particular security interests but we also call for the investigation of potential alternative coping mechanisms that individuals pursue. Liang and Xue [21] suggest that protection motivation only exists if individuals perceive a sufficient threat level. However, when security threats appear to be inevitable, users may seek alternative coping strategies instead [58]. We propose to validate this assumption in future research, exploring how individuals act when the goal conflict does not seem resolvable.

8. Conclusion

Individuals are having two conflicting goals in mind when deciding whether to use an effective safeguarding technology against security threats. First, they aim to protect themselves against security threats which drives protection motivation and subsequently implies a disclosure of personal information to a safeguard provider. Second, they seek to have control over their personal information that impedes self-disclosure to any provider. This brings along a tension between security and privacy which have predominantly studied as two independent research streams directed to the same behavior goal. Thus, this study sheds light on impediments of safeguarding usage and guides safeguard providers as they need to establish an image of "security defender" instead of "privacy abuser".

Acknowledgements. This research project was funded by the Hessian state ministry "Hessisches Ministerium des Innern und für Sport" in Germany.

Appendix

Intention to use a safeguarding service [59]:
1. I intend to use an online backup service for my smartphone.
2. I aim to use an online backup service for my smartphone.
3. I plan to use an online backup service for my smartphone.

Perceived susceptibility [5]:
1. I am at risk to lose my smartphone.
2. It is likely that my smartphone will be damaged or destroyed.
3. It is possible that my smartphone gets stolen.

Perceived severity [5]:
1. If I would lose the data solely stored on my smartphone, it would be severe.
2. If I would lose the data solely stored on my smartphone, it would be serious.
3. If I would lose the data solely stored on my smartphone, it would be significant.

Information privacy concern [7]:
1. I am concerned that the data I disclose to the backup service provider could be misused.
2. I am concerned that a third person can access the data I disclose to the backup service provider.
3. I am concerned about uploading data to the backup service provider, because of what others might do with it.
4. I am concerned about uploading data on an online backup, because it could be used in a way I did not foresee.

Response efficacy [5]:
1. An online backup solution works for protection against data loss.
2. An online backup solution is effective for protection against data loss.
3. When using an online backup solution, my smartphone is more likely to be protected against data loss.

Response cost [21]:
1. I don't have an online backup solution on my smartphone because I don't know how to get a service for doing online backups.
2. I don't have an online backup solution on my smartphone because the online backup solution my cause problems to other applications on my smartphone.
3. I don't have an online backup solution on my smartphone because installing and maintaining an online backup solution is too much trouble.

Self-efficacy [60]:
1. I could use the described application if there was no one around to tell me what to do as I go.
2. I could use the described application if I had never used a package like it before.
3. I could use the described application if I had just the built-in help facility for assistance.

Escapism (marker variable) [61]:
1. I daydream a lot.
2. When I go to the movies I find it easy to lose myself in the film.
3. I often think of what might have been.

Current usage of an online backup:
Do you already use a mobile application to backup data online? [yes; no]

References

[1] Z. Tu and Y. Yuan, "Understanding user's behaviors in coping with security threat of mobile devices Loss and theft," in *Proceedings of the 45rd Hawaii International Conference on System Sciences*, 2012, pp. 1393-1402: IEEE.

[2] H. J. Smith, T. Dinev, and H. Xu, "Information privacy research: an interdisciplinary review," *MIS Quarterly*, vol. 35, no. 4, pp. 989-1016, 2011.

[3] D. Lee, R. Larose, and N. Rifon, "Keeping our network safe: a model of online protection behaviour," *Behaviour & Information Technology*, vol. 27, no. 5, pp. 445-454, 2008.

[4] H. Liang and Y. Xue, "Avoidance of information technology threats: a theoretical perspective," *MIS Quarterly*, vol. 33, no. 1, pp. 71-90, 2009.

[5] A. C. Johnston and M. Warkentin, "Fear appeals and information security behaviors: an empirical study," *MIS Quarterly*, vol. 34, no. 3, pp. 549-566, 2010.

[6] S. R. Boss, D. F. Galletta, P. Benjamin Lowry, G. D. Moody, and P. Polak, "What Do Systems Users Have

to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors," *MIS Quarterly*, Article vol. 39, no. 4, pp. 837-864, 2015.
[7] T. Dinev and P. Hart, "An extended privacy calculus model for e-commerce transactions," *Information Systems Research*, vol. 17, no. 1, pp. 61-80, 2006.
[8] X. Zhang, S. Liu, X. Chen, L. Wang, B. Gao, and Q. Zhu, "Health information privacy concerns, antecedents, and information disclosure intention in online health communities," *Information & Management*, vol. 55, no. 4, pp. 482-493, 2018.
[9] F. M. Zahedi, A. Abbasi, and Y. Chen, "Fake-website detection tools: Identifying elements that promote individuals' use and enhance their performance," *Journal of the Association for Information Systems*, vol. 16, no. 6, pp. 448-484, 2015.
[10] J. Mou, J. Cohen, and J. Kim, "A Meta-Analytic Structural Equation Modeling Test of Protection Motivation Theory in Information Security Literature," in *ICIS 2017 Proceedings*, South Korea, 2017.
[11] C. S. Carver and M. F. Scheier, "On the structure of behavioral self-regulation," *Handbook of Self-Regulation*, pp. 41-84, 2000.
[12] E. A. Locke and G. P. Latham, "Building a practically useful theory of goal setting and task motivation: A 35-year odyssey," *American Psychologist*, vol. 57, no. 9, p. 705, 2002.
[13] R. P. Bagozzi, "The legacy of the technology acceptance model and a proposal for a paradigm shift," *Journal of the Association for Information Systems*, vol. 8, no. 4, pp. 244-254, 2007.
[14] S. Conger and B. J. Landry, "The intersection of privacy and security," in *Association of Information Systems SIGSEC Workshop on Information Security & Privacy (WISP 2008), Paris*, 2008.
[15] T. Dinev, M. Bellotto, P. Hart, V. Russo, I. Serra, and C. Colautti, "Privacy calculus model in e-commerce–a study of Italy and the United States," *European Journal of Information Systems*, vol. 15, no. 4, pp. 389-402, 2006.
[16] N. K. Malhotra, S. S. Kim, and J. Agarwal, "Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model," *Information systems research*, vol. 15, no. 4, pp. 336-355, 2004.
[17] F. Bélanger and L. Carter, "Trust and risk in e-government adoption," *The Journal of Strategic Information Systems*, vol. 17, no. 2, pp. 165-176, 2008.
[18] H. Xu, X. R. Luo, J. M. Carroll, and M. B. Rosson, "The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing," *Decision support systems*, vol. 51, no. 1, pp. 42-52, 2011.
[19] H. Krasnova and N. F. Veltri, "Privacy calculus on social networking sites: Explorative evidence from Germany and USA," in *Proceedings of the 43rd Hawaii International Conference on System Sciences*, 2010, pp. 1-10: IEEE.
[20] H. R. Nikkhah and R. Sabherwal, "A Privacy-Security Model of Mobile Cloud Computing Applications," in *ICIS 2017 proceedings*, South Korea, 2017.
[21] H. Liang and Y. Xue, "Understanding security behaviors in personal computer usage: A threat avoidance perspective," *Journal of the Association for Information Systems*, vol. 11, no. 7, pp. 394-413, 2010.
[22] S. C. Segerstrom and L. S. Nes, "When goals conflict but people prosper: The case of dispositional optimism," *Journal of Research in Personality*, vol. 40, no. 5, pp. 675-693, 2006.
[23] C. Wrosch, M. F. Scheier, G. E. Miller, R. Schulz, and C. S. Carver, "Adaptive self-regulation of unattainable goals: Goal disengagement, goal reengagement, and subjective well-being," *Personality and Social Psychology Bulletin*, vol. 29, no. 12, pp. 1494-1508, 2003.
[24] Y. Chen and F. M. Zahedi, "Individuals' Internet Security Perceptions and Behaviors: Polycontextual Contrasts Between the United States and China," *MIS Quarterly*, vol. 40, no. 1, pp. 205-222, 2016.
[25] C. Nam, C. Song, E. L. Park, and C. Ik, "Consumers' privacy concerns and willingness to provide marketing-related personal information online," *ACR North American Advances*, pp. 212-217, 2006.
[26] Y. Lee and K. R. Larsen, "Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software," *European Journal of Information Systems*, vol. 18, no. 2, pp. 177-187, 2009.
[27] A. Vance, M. Siponen, and S. Pahnila, "Motivating IS security compliance: Insights from Habit and Protection Motivation Theory," *Information & Management*, vol. 49, no. 3, pp. 190-198, 2012.
[28] I. Woon, G.-W. Tan, and R. Low, "A protection motivation theory approach to home wireless security," in *ICIS 2005 Proceedings*, 2005.
[29] P. Ifinedo, "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory," *Computers & Security*, vol. 31, no. 1, pp. 83-95, 2012.
[30] Bitdefender. (2017, 2019-05-09). *Personal data stored on smartphones by 50 percent of users*. Available: https://www.bitdefender.com/news/us:-personal-data-stored-on-smartphones-by-50-percent-of-users-3368.html
[31] H. R. Nikkhah and R. Sabherwal, "Mobile Cloud-Computing Applications: A Privacy Cost-Benefit Model," in *AMCIS 2017 Proceedings*, Boston, MA, 2017.
[32] P. Menard, R. Gatlin, and M. Warkentin, "Threat protection and convenience: Antecedents of cloud-based data backup," *Journal of Computer Information Systems*, vol. 55, no. 1, pp. 83-91, 2014.
[33] J. Weber, "Scenarios in business ethics research: Review, critical assessment, and recommendations," *Business Ethics Quarterly*, vol. 2, no. 2, pp. 137-160, 1992.
[34] P. M. Podsakoff, S. B. MacKenzie, J.-Y. Lee, and N. P. Podsakoff, "Common method biases in behavioral research: a critical review of the literature and

recommended remedies," *Journal of Applied Psychology*, vol. 88, no. 5, pp. 879-903, 2003.
[35] L. J. Williams, N. Hartman, and F. Cavazotte, "Method variance and marker variables: A review and comprehensive CFA marker technique," *Organizational Research Methods*, vol. 13, no. 3, pp. 477-514, 2010.
[36] P. B. Lowry, J. D'Arcy, B. Hammer, and G. D. Moody, ""Cargo Cult" science in traditional organization and information systems survey research: A case for using nontraditional methods of data collection, including Mechanical Turk and online panels," *The Journal of Strategic Information Systems*, vol. 25, no. 3, pp. 232-240, 2016.
[37] A. W. Meade and S. B. Craig, "Identifying careless responses in survey data," *Psychological methods*, vol. 17, no. 3, pp. 437-456, 2012.
[38] C. M. Ringle, S. Wende, and J.-M. Becker. (2015). *SmartPLS 3*.
[39] R. P. Bagozzi and Y. Yi, "On the use of structural equation models in experimental designs," *Journal of Marketing Research*, vol. 26, no. 3, pp. 271-284, 1989.
[40] R. F. Falk and N. B. Miller, *A primer for soft modeling*. Akron, Ohio: University of Akron Press, 1992.
[41] R. P. Bagozzi and Y. Yi, "Specification, evaluation, and interpretation of structural equation models," *Journal of the Academy of Marketing Science*, vol. 40, no. 1, pp. 8-34, 2012.
[42] J. F. Hair, C. M. Ringle, and M. Sarstedt, "Partial least squares structural equation modeling: Rigorous applications, better results and higher acceptance," *Long Range Planning*, vol. 46, no. 1-2, pp. 1-12, 2013.
[43] C. Fornell and D. F. Larcker, "Evaluating structural equation models with unobservable variables and measurement error," *Journal of Marketing Research*, vol. 18, no. 1, pp. 39-50, 1981.
[44] L.-t. Hu and P. M. Bentler, "Fit indices in covariance structure modeling: Sensitivity to underparameterized model misspecification," *Psychological Methods*, vol. 3, no. 4, pp. 424-453, 1998.
[45] M. Rönkkö and J. Ylitalo, "PLS marker variable approach to diagnosing and controlling for method variance," in *ICIS 2011 Proceedings*, 2011.
[46] H. B. Mann and D. R. Whitney, "On a test of whether one of two random variables is stochastically larger than the other," *The Annals of Mathematical Statistics*, vol. 18, no. 1, pp. 50-60, 1947.
[47] M. J. Culnan and P. K. Armstrong, "Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation," *Organization science*, vol. 10, no. 1, pp. 104-115, 1999.
[48] H. Xu and H.-H. Teo, "Alleviating consumers' privacy concerns in location-based services: a psychological control perspective," in *ICIS 2004 Proceedings*, 2004, pp. 793-806.
[49] F. Bélanger, J. S. Hiller, and W. J. Smith, "Trustworthiness in electronic commerce: the role of privacy, security, and site attributes," *The Journal of Strategic Information Systems*, vol. 11, no. 3, pp. 245-270, 2002.
[50] R. Crossler and F. Bélanger, "An extended perspective on individual security behaviors: Protection motivation theory and a unified security practices (USP) instrument," *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, vol. 45, no. 4, pp. 51-71, 2014.
[51] The Telegraph. (2010, 2019-05-09). *Google apologises for collecting personal web data*. Available: http://www.telegraph.co.uk/technology/google/7727907/Google-apologises-for-collecting-personal-web-data.html
[52] BBC News. (2015, 2019-05-09). *What is Facebook doing with my data?* Available: http://www.bbc.com/news/magazine-34776191
[53] Business Insider. (2015, 2019-05-09). *Windows 10 automatically scans your computer for pirated software, but that's a good thing*. Available: http://www.businessinsider.com/why-windows-10-scans-for-pirated-games-2015-8
[54] BBC News. (2014, 2019-05-09). *A cloud of uncertainty*. Available: http://www.bbc.com/news/technology-29030229
[55] M. Leppaniemi and H. Karjaluoto, "Factors influencing consumers' willingness to accept mobile advertising: a conceptual model," *International Journal of Mobile Communications*, vol. 3, no. 3, pp. 197-213, 2005.
[56] I. Ajzen, "The Theory of Planned Behavior," *Organizational Behavior and Human Decision Processes*, vol. 50, no. 2, pp. 179-211, 1991.
[57] The New York Times. (2018, 2019-05-09). *After Cambridge Analytica, Privacy Experts Get to Say 'I Told You So'*. Available: https://www.nytimes.com/2018/04/12/technology/privacy-researchers-facebook.html
[58] H. Liang, Y. Xue, and L. Wu, "Ensuring employees' it compliance: Carrot or stick?," *Information Systems Research*, vol. 24, no. 2, pp. 279-294, 2013.
[59] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, "User acceptance of information technology: Toward a unified view," *MIS Quarterly*, vol. 27, no. 3, pp. 425-478, 2003.
[60] D. R. Compeau and C. A. Higgins, "Computer self-efficacy: Development of a measure and initial test," *MIS Quarterly*, vol. 19, no. 2, pp. 189-211, 1995.
[61] T. C. O'Guinn and R. J. Faber, "Compulsive buying: A phenomenological exploration," *Journal of Consumer Research*, vol. 16, no. 2, pp. 147-157, 1989.