JonDonym Users' Information Privacy Concerns

David Harborth, Sebastian Pape

JonDonym Users' Information Privacy Concerns

David Harborth[1][0000−0001−9554−7567] and
Sebastian Pape[1](✉)[0000−0002−0893−7856]

Chair of Mobile Business and Multilateral Security
Goethe University, Frankfurt, Germany

Abstract. Privacy concerns as well as trust and risk beliefs are important factors that can influence users' decision to use a service. One popular model that integrates these factors is relating the Internet Users Information Privacy Concerns (IUIPC) construct to trust and risk beliefs. However, studies haven't yet applied it to a privacy enhancing technology (PET) such as an anonymization service. Therefore, we conducted a survey among 416 users of the anonymization service JonDonym [1] and collected 141 complete questionnaires. We rely on the IUIPC construct and the related trust-risk model and show that it needs to be adapted for the case of PETs. In addition, we extend the original causal model by including trust beliefs in the anonymization service provider and show that they have a significant effect on the actual use behavior of the PET.

Keywords: Internet Users' Information Privacy Concerns, IUIPC, Anonymity Services, Privacy Concerns, Trust Beliefs, Risk Beliefs

1 Introduction

Privacy concerns have been discussed since the very beginning of computer sharing [2]. With a raising economic interest in the internet [3], they gain importance. Bruce Schneier [4] states: "Surveillance is the business model of the internet. Everyone is under constant surveillance by many companies, ranging from social networks like Facebook to cellphone providers." Thus, it can not be a surprise that users have privacy concerns and feel a strong need to protect their privacy[1].

One popular model for measuring and explaining privacy concerns of online users is the Internet Users Information Privacy Concerns (IUIPC) construct by Malhotra et al. [6]. Their research involves a theoretical framework and an instrument for operationalizing privacy concerns, as well as a causal model for this construct including trust and risk beliefs about the online companies' data handling of personal information. The IUIPC construct has been used in various contexts, e.g. Internet of Things [7], internet transactions [8] and Mobile Apps [9], but to the best of our knowledge the IUIPC construct has never been applied to a privacy enhancing technology (PET) such as anonymization services. The IUIPC

[1] "The mean value for the statement 'I feel very strongly about protecting my privacy' was 3.64 on a five-point scale with no statistically significant differences across gender, income groups, educational levels, or political affiliation." [5]

instrument shows its strengths best when a service with a certain use for the customer (primary use) is investigated with respect to privacy concerns. However, for anonymization services the primary purpose is to help users to protect their privacy. As a consequence, it is necessary to distinguish between trust and risk beliefs with respect to technologies which aim to protect personal (PETs) and regular internet services. Therefore, the trust model within IUIPC's causal model needs to be adapted for the investigation of anonymization services. For that purpose, we conducted a survey among 416 users of the anonymization service JonDonym [1] and collected 141 complete questionnaires. Our results contribute to the understanding of users' perceptions about PETs and indicate how privacy concerns and trust and risk beliefs influence the use behavior of PETs.

The remainder of the paper is structured as follows: Sect. 2 briefly introduces the JonDonym anonymization service and lists related work on PETs. In section 3, we present the research hypotheses and describe the questionnaire and the data collection process. We assess the quality of our empirical results with regard to reliability and validity in section 4. In section 5, we discuss the implications of the results, elaborate on limitations of the framework and conclude the paper with suggestions for future work.

2 Background and Related Work

Privacy-Enhancing Technologies (PETs) is an umbrella term for different privacy protecting technologies. Borking and Raab define PETs as a "coherent system of ICT measures that protects privacy [...] by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data; all without losing the functionality of the data system" [10, S. 1].

In this paper, we investigate the privacy, trust and risk beliefs associated with PETs for the case of the anonymity service JonDonym [1]. Comparable to Tor, JonDonym is an anonymity service. However, unlike Tor, it is a proxy system based on mix cascades. It is available for free with several limitations, like the maximum download speed. In addition, there are different premium rates without these limitations that differ with regard to duration and included data volume. Thus, JonDonym offers several different tariffs and is not based on donations like Tor. The actual number of users is not predictable since the service does not keep track of this. JonDonym is also the focus of an earlier user study on user characteristics of privacy services [11]. However, the focus of the study is rather descriptive and does not focus on users' beliefs and concerns.

Previous non-technical work on PETs considers mainly usability studies and does not primarily focus on privacy concerns and related trust and risk beliefs of PET users. For example, Lee et al. [12] assess the usability of the Tor Launcher and propose recommendations to overcome the found usability issues. Benenson et al. [13] investigate acceptance factors for anonymous credentials. Among other things, they find that trust in the PET has no statistically significant impact on the intention to use the service. This result is relevant for our study since we also hypothesize that trust in JonDonym has a positive effect on the actual use of

the service (see Section 3.1). Janic et al. [14] claim to consider the relationship between privacy concerns, transparency enhancing technologies (TETs) and PETs, but have a strong focus on TETs and only provide a literature review.

3 Methodology

We base our research on the Internet Users Information Privacy Concerns (IUIPC) model by Malhotra et al. [6]. The original research on this model investigates the role of users' information privacy concerns in the context of releasing personal information to a marketing service provider. Since we want to investigate the role of privacy concerns, trust and risk beliefs for using a PET (i.e. JonDonym), we can adapt the model by substituting the behavioral intention to perform an action with the actual use of JonDonym. This is possible since we asked current users of JonDonym who actively use the PET. In addition, we extend the original model by trusting beliefs in the PET itself. We argue that the level of trust in a PET is a crucial factor determining the use decision.

For analyzing the cause-effect relationships between the latent (unobserved) variables, we use structural equation modelling (SEM). There are two main approaches for SEM, namely covariance-based SEM (CB-SEM) and partial least squares SEM (PLS-SEM) [15]. Since our research goal is to predict the target construct actual use behavior of JonDonym, we use PLS-SEM for our analysis [15, 16]. In the following subsections, we discuss the hypotheses based on the IUIPC model [6], the questionnaire and the data collection process.

3.1 Research Hypotheses

As Figure 1 shows, the structural model contains several relationships between exogenous and endogenous variables. We develop our research hypotheses for these relationships based on the original hypotheses of the IUIPC model [6]. In the original article, IUIPC is operationalized as a second-order construct of the sub-constructs collection (COLL), awareness (AWA) and control (CONTROL) [2]. Thus, the privacy concerns of users are determined by their concerns about "[...]individual-specific data possessed by others relative to the value of benefits receive" [6, p. 338], the control they have over their own data (i.e. possibilities to change or opt-out) and the "[...] degree to which a consumer is concerned about his/her awareness of organizational information privacy practices" [6, p. 339].

The effect of IUIPC on the behavioral intention (in our model the actual use behavior) is moderated by trusting beliefs and risk beliefs. Trusting beliefs represent users' perceptions about the behavior of online firms to protect the users' personal information. In contrast, risk beliefs represent users' perception about losses associated with providing personal data to online firms [6]. Thus, the higher the privacy concerns of a user, the lower are his or her trusting beliefs and

[2] Due to space limitations, we will not elaborate on the statistics of second-order constructs here. For an extensive discussion see Steward and Malhotra [17, 6].

the higher are his or her risk beliefs. In addition, a higher level of trust is assumed to decrease the risk beliefs. Thus, we derive the following three hypotheses:

H 1: *Internet Users Information Privacy Concerns (IUIPC) have a negative effect on Trusting Beliefs (TB).*

H 2: *Internet Users Information Privacy Concerns (IUIPC) have a positive effect on Risk Beliefs (RB).*

H 3: *Trusting Beliefs (TB) have a negative effect on Risk Beliefs (RB).*

Since we investigate the use of a specific PET, JonDonym, we extend the model by including the trust of users in JonDonym itself. For that purpose, we adapt the trust construct by Pavlou [18]. However, in order to protect their privacy, users with higher privacy concerns are assumed to rather trust the privacy-enhancing technology compared to online firms that process personal data. In particular, because we surveyed users of the PET. Therefore, we hypothesize:

H 4: *Internet Users Information Privacy Concerns (IUIPC) have a positive effect on the trusting beliefs in JonDonym (TB_{JD}).*

Trust is an important factor in the acceptance decision of users [18]. Especially for the case of privacy protection, we assume that trust in JonDonym is a major factor in the decision to use the technology. Thus, we hypothesize that:

H 5: *Trusting beliefs in JonDonym (TB_{JD}) have a positive effect on the actual use behavior of JonDonym (USE).*

When considering the effects of trusting and risk beliefs on behavior in the context of releasing data to online companies, it is logical that trusting beliefs have a positive effect and risk beliefs have a negative effect on releasing data. However, in our case with actual use behavior of a PET, we assume these effects reverse. The higher the trusting beliefs in online firms, the lower is the use frequency of JonDonym, since the protection of data becomes less important. Following this rationale, a higher degree of risk beliefs with respect to the data processing of online firms leads to a higher degree of use. Therefore, we hypothesize that:

H 6: *Trusting beliefs (TB) have a negative effect on actual use behavior of JonDonym (USE).*

H 7: *Risk beliefs (RB) have a positive effect on actual use behavior of JonDonym (USE).*

3.2 Questionnaire Composition and Data Collection Procedure

The questionnaire constructs are adapted from the original IUIPC paper [6]. We conducted the study with German and English speaking JonDonym users. Thus, we administered two questionnaires. All items for the German questionnaire had to be translated into German since all of the constructs are adapted from English

literature. To ensure content validity of the translation, we followed a rigorous translation process [19, 20]. First, we translated the English questionnaire into German with the help of a certified translator (translators are standardized following the DIN EN 15038 norm). The German version was then given to a second independent certified translator who retranslated the questionnaire to English. This step was done to ensure the equivalence of the translation. Third, a group of five academic colleagues checked the two English versions with regard to this equivalence. All items were found to be equivalent. The items of the English version can be found in Appendix A.

Since we investigate the effect of privacy concerns, trust and risk beliefs on the use of JonDonym, we collected data of actual users of the PET. We installed the surveys on a university server and managed it with the survey software LimeSurvey (version 2.63.1) [21]. The links to the English and German version were distributed with the beta version of the JonDonym browser and published on the official JonDonym homepage. In sum, 416 participants started the questionnaire (173 for the English version and 243 for the German version). Of those 416 approached participants, 141 (53 for the English version and 88 for the German version) remained after deleting unfinished sets and all participants who answered a test question in the middle of the survey incorrectly.

The demographic questions were not mandatory to fill out. This was done on purpose since we assumed that most of the participants are highly sensitive with respect to their personal data. Therefore, we resign from a discussion of the demographics in our research context. This decision is backed up by Singh and Hill, who found no statistically significant differences across gender, income groups, educational levels, or political affiliation in the desire to protect one's privacy [5].

4 Results

We tested the model using SmartPLS version 3.2.6 [22]. Before looking at the result of the structural model and discussing its implications, we discuss the measurement model, and check for the reliability and validity of our results. This is a precondition of being able to interpret the results of the structural model. Furthermore, it is recommended to report the computational settings. For the PLS algorithm, we choose the path weighting scheme with a maximum of 300 iterations and a stop criterion of 10^{-7}. For the bootstrapping procedure, we use 5000 bootstrap subsamples and no sign changes as the method for handling sign changes during the iterations of the bootstrapping procedure.

4.1 Assessment of the Measurement Model

As the model is measured solely reflectively, we need to evaluate the internal consistency reliability, convergent validity and discriminant validity to assess the measurement model properly [15].

Table 1. Loadings and Cross-Loadings of the Reflective Items and Internal Consistency Reliability

Constructs	AWA	CONTROL	COLL	RB	TB	TB_{JD}	IUIPC	USE
AWA1	**0.892**	0.254	0.297	0.050	-0.107	0.073	0.614	0.143
AWA2	**0.927**	0.254	0.287	0.072	-0.152	0.057	0.622	0.098
AWA3	**0.883**	0.297	0.356	0.235	-0.207	0.071	0.648	0.169
CONTROL1	0.284	**0.837**	0.379	0.271	-0.306	0.163	0.618	0.208
CONTROL2	0.244	**0.808**	0.238	0.205	-0.075	0.103	0.505	0.175
CONTROL3	0.201	**0.819**	0.348	0.287	-0.195	0.089	0.514	0.138
COLL1	0.202	0.309	**0.781**	0.237	-0.084	0.152	0.588	0.133
COLL2	0.199	0.185	**0.760**	0.141	0.001	0.262	0.548	0.300
COLL3	0.380	0.364	**0.873**	0.192	-0.063	0.297	0.733	0.302
COLL4	0.336	0.416	**0.872**	0.349	-0.213	0.193	0.720	0.261
RB1	0.117	0.213	0.230	**0.814**	-0.324	0.022	0.194	0.157
RB2	0.061	0.172	0.100	**0.710**	-0.201	-0.114	0.116	0.050
RB3	0.132	0.225	0.193	**0.815**	-0.179	-0.098	0.196	0.123
RB4	0.075	0.214	0.266	**0.811**	-0.241	-0.076	0.211	0.050
RB5	-0.112	-0.311	-0.244	**-0.682**	0.392	0.050	-0.277	-0.092
TB1	-0.174	-0.217	-0.078	-0.296	**0.832**	0.028	-0.196	-0.117
TB2	-0.114	-0.171	-0.033	-0.281	**0.835**	-0.101	-0.130	-0.134
TB3	-0.167	-0.210	-0.116	-0.343	**0.815**	0.004	-0.209	-0.024
TB4	-0.123	-0.160	-0.089	-0.212	**0.666**	-0.051	-0.129	-0.060
TB5	-0.121	-0.210	-0.137	-0.354	**0.855**	-0.158	-0.200	-0.210
$TB_{JD}1$	0.017	0.104	0.244	-0.058	-0.100	**0.898**	0.130	0.281
$TB_{JD}2$	0.088	0.117	0.222	-0.109	-0.043	**0.922**	0.165	0.303
$TB_{JD}3$	0.090	0.176	0.284	-0.032	-0.060	**0.922**	0.199	0.330
IUIPC	0.698	0.669	0.794	0.276	-0.220	0.183	**1.000**	0.333
USE	0.152	0.214	0.304	0.130	-0.142	0.335	0.333	**1.000**
Cronbach's α	0.883	0.761	0.841	0.612	0.862	0.902	1.000	1.000
Composite Reliability	0.928	0.862	0.893	0.749	0.901	0.938	1.000	1.000

Internal Consistency Reliability Internal consistency reliability (ICR) measurements indicate how well certain indicators of a construct measure the same latent phenomenon. Two standard approaches for assessing ICR are Cronbach's α and the composite reliability. The values of both measures should be between 0.7 and 0.95 for research that builds upon accepted models. Values of Cronbach's α are seen as a lower bound and values of the composite reliability as an upper bound of the assessment [16]. Table 1 includes the ICR of the variables in the last two rows. It can be seen that all values for Cronbach's α are above the lower threshold of 0.7 except for RB. However, for the composite reliability the value for RB is higher than 0.7. Therefore, we argue that ICR is not an issue for this variable. For all variables, no value is above 0.95. Values above that upper threshold indicate that the indicators measure the same dimension of the latent variable, which is not optimal with regard to the validity [16]. In sum, ICR is established for our variables. The variables IUIPC and USE are single-item constructs, and thus have ICR values of 1.

Table 2. Discriminant Validity with AVEs and Construct Correlations

Constructs (AVE)	AWA	COLL	CONTROL	IUIPC	RB	TB	TB_{JD}	USE
AWA (0.811)	0.901							
COLL (0.678)	0.349	0.823						
CONTROL (0.675)	0.298	0.396	0.822					
IUIPC (1.000)	0.698	0.794	0.669	1,000				
RB (0.591)	0.134	0.284	0.311	0.276	0.769			
TB (0.646)	-0.173	-0.116	-0.243	-0.220	-0.377	0.804		
TB_{JD} (0.835)	0.074	0.275	0.148	0.183	-0.071	-0.072	0.914	
USE (1.000)	0.152	0.304	0.214	0.333	0.130	-0.142	0.335	1.000

Note: AVEs in parentheses in the first column. Values for $\sqrt{AVE}$ are shown on the diagonal and construct correlations are off-diagonal elements.

Convergent Validity Convergent validity determines the degree to which indicators of a certain reflective construct are explained by that construct. This is assessed by calculating the outer loadings of the indicators of the constructs (indicator reliability) and by looking at the average variance extracted (AVE) [15]. Loadings above 0.7 imply that the indicators have much in common, which is desirable for reflective measurement models [16]. Table 1 shows the outer loadings in bold on the diagonal. All loadings are higher than 0.7, except for RISK5 and TB5. Since the AVE of these constructs is still above 0.5, we do not drop these items. Convergent validity for the construct is assessed by the AVE. AVE is equal to the sum of the squared loadings divided by the number of indicators. A threshold of 0.5 is acceptable, indicating that the construct explains at least half of the variance of the indicators [16]. The diagonal values of Table 2 present the AVE of our constructs. All values are well above 0.5, demonstrating convergent validity.

Discriminant Validity Discriminant validity measures the degree of uniqueness of a construct compared to other constructs. Comparable to the convergent validity assessment, two approaches are used for investigated discriminant validity. The first approach, assessing cross-loadings, is dealing with single indicators. All outer loadings of a certain construct should be larger than its cross-loadings with other constructs [15]. Table 1 illustrates the cross-loadings as off-diagonal elements. All cross-loadings are smaller than the outer loadings, fulfilling the first assessment approach of discriminant validity. The second approach is on the construct level and compares the square root of the constructs' AVE with the correlations with other constructs. The square root of the AVE of a single construct should be larger than the correlation with other constructs (Fornell-Larcker criterion) [16]. Table 2 contains the square root of the AVE on the diagonal in parentheses. All values are larger than the correlations with other constructs, indicating discriminant validity. Since there are problems in determining the discriminant validity with both approaches, researchers propose the heterotrait-monotrait ratio (HTMT) for assessing discriminant validity as a superior approach to the former ones [23]. HTMT divides between-trait correlations by within-trait correlations, therefore providing a measure of what the true correlation of two constructs would be if

Table 3. Heterotrait-Monotrait Ratio (HTMT)

Constructs	AWA	COLL	CONTROL	IUIPC	RB	TB	TB_{JD}	USE
AWA								
COLL	0.393							
CONTROL	0.360	0.478						
IUIPC	0.742	0.858	0.761					
RB	0.155	0.313	0.368	0.282				
TB	0.198	0.142	0.287	0.232	0.402			
TB_{JD}	0.091	0.314	0.171	0.190	0.109	0.118		
USE	0.161	0.330	0.242	0.333	0.133	0.146	0.351	

the measurement is flawless [16]. Values close to 1 for HTMT indicate a lack of discriminant validity. A conservative threshold is 0.85 [23]. Table 3 contains the values for HTMT and no value is above the suggested threshold of 0.85.

To evaluate whether the HTMT statistics are significantly different from 1, a bootstrapping procedure with 5,000 subsamples is conducted to get the confidence interval in which the true HTMT value lies with a 95% chance. The HTMT measure requires that no confidence interval contains the value 1. The conducted analysis shows that this is the case. Thus, discriminant validity is established for our model.

Common Method Bias The common method bias (CMB) can occur if data is gathered with a self-reported survey at one point in time in one questionnaire [24]. Since this is the case in our research design, the need to test for CMB arises.

An unrotated principal component factor analysis is performed with the software package STATA 14.0 to conduct the Harman's single-factor test to address the issue of CMB [25]. The assumptions of the test are that CMB is not an issue if there is no single factor that results from the factor analysis or that the first factor does not account for the majority of the total variance [25]. The test shows that six factors have eigenvalues larger than 1 which account for 69.45% of the total variance. The first factor explains 23.74% of the total variance. Based on the results of previous literature [26], we argue that CMB is not likely to be an issue in the data set.

4.2 Assessment and Results of the Structural Model

To assess the structural model, we follow the steps proposed by Hair et al. [16] which include an assessment of possible collinearity problems, of path coefficients, of the level of R^2, of the effect size f^2, of the predictive relevance Q^2 and the effect size q^2. We address these evaluation steps to ensure the predictive power of the model with regard to the target constructs.

Collinearity Collinearity is present if two predictor variables are highly correlated with each other. To address this issue, we assess the inner variance inflation factor (inner VIF). All VIF values above 5 indicate that collinearity between constructs is present. For our model, the highest VIF is 1.179. Thus collinearity is apparently not an issue.

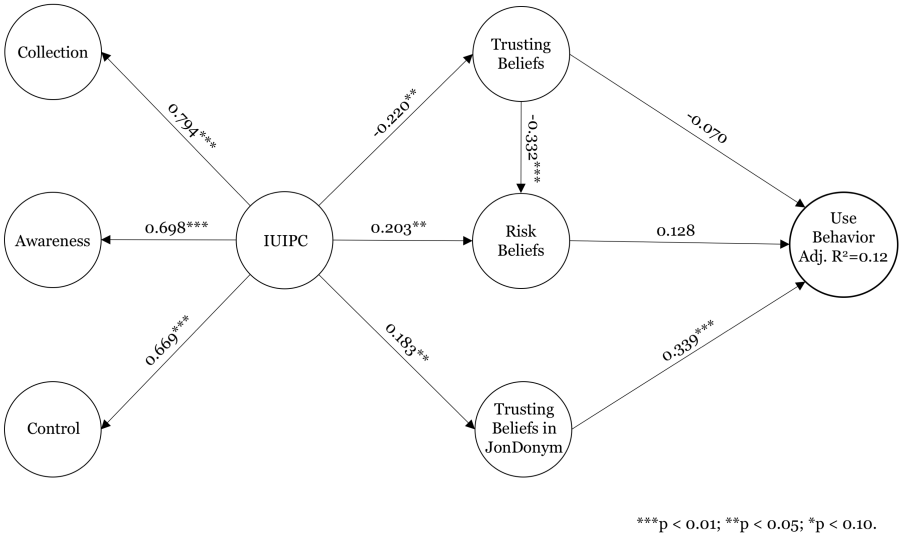

Fig. 1. Path Estimates and Adjusted R^2 values of the Structural Model

Significance and Relevance of Model Relationships Figure 1 presents the results of the path estimations and the adjusted R^2 of the endogenous variable USE. We used the adjusted R^2 as it is a conservative measure for the explained variance of a dependent variable by avoiding a bias towards more complex models [16]. The R^2 is 0.12 for USE. Thus, our models explains 12% of the variance in USE. There are different proposals for interpreting the size of this value. We choose to use the very conservative threshold proposed by Hair et al. [15], where R^2 values are weak with values around 0.25, moderate with 0.50 and substantial with 0.75. Based on this classification, the R^2 value for USE is rather weak. The path coefficients are presented on the arrows connecting the exogenous and endogenous constructs in Figure 1. Statistical significance is indicated by asterisks, ranging from three asterisks for p-values smaller than 0.01 to one asterisk for p-values smaller than 0.10. The p-value indicates the probability that a path estimate is incorrectly assumed to be significant. Thus, the lower the p-value, the higher the probability that the given relationship exists. The relevance of the path coefficients is expressed by the relative size of the coefficient compared to the other explanatory variables [16].

It can be seen that IUIPC has a statistically significant negative medium-sized effect on trusting beliefs and a positive effect on risk beliefs. The effect of IUIPC on trusting beliefs in JonDonym is significant, positive and medium-sized. The construct trusting beliefs has a statistically significant medium-sized negative effect on risk beliefs. The effect of trusting beliefs on use behavior is negative, but not statistically significant. The same holds for the relationship between risk beliefs and use behavior (for both $p \geq 0.10$). In contrast, the effect of trusting beliefs in JonDonym on use behavior is highly statistically significant, positive and large with 0.339.

Table 4. Values for the f^2 and q^2 Effect Size Assessment

Variables	f^2	q^2
Endogenous / Exogenous	USE	USE
RB	0.016	0.012
TB	0.005	-0.016
TB_{JD}	*0.131*	*0.109*

Effect Sizes f^2 The f^2 effect size measures the impact of a construct on the endogenous variable by omitting it from the analysis and assessing the resulting change in the R^2 value [16]. The values are assessed based on thresholds by Cohen [27], who defines effects as small, medium and large for values of 0.02, 0.15 and 0.35, respectively. Table 4 shows the results of the f^2 evaluation. Values in italics indicate small effects and values in bold indicate medium effects. All other values have no substantial effect. The results correspond to those of the previous analysis of the path coefficients.

Predictive Relevance Q^2 The Q^2 measure indicates the out-of-sample predictive relevance of the structural model with regard to the endogenous latent variables based on a blindfolding procedure [16]. We used an omission distance d=7. Recommended values for d are between five and ten [15]. Furthermore, we report the Q^2 values of the cross-validated redundancy approach, since this approach is based on both the results of the measurement model as well as of the structural model [16]. Detailed information about the calculation cannot be provided due to space limitations. For further information see Chin [28]. For our model, Q^2 is calculated for USE. Values above 0 indicate that the model has the property of predictive relevance. In our case, the Q^2 value is equal to 0.097 for USE. Since they are larger than 0, predictive relevance of the model is established.

Effect Sizes q^2 The assessment of q^2 follows the same logic as the one of f^2. It is based on the Q^2 values of the endogenous variables and calculates the individual predictive power of the exogenous variables by omitting them and comparing the change in Q^2. The effect sizes q^2 have to be calculated with the formula [16]:

$$q^2_{X \to Y} = \frac{Q^2_{included} - Q^2_{excluded}}{1 - Q^2_{included}}$$

All individual values for q^2 are calculated with an omission distance d of seven. The results are shown in Table 4. The thresholds for the f^2 interpretation can be applied here, too [27]. Values in italics indicate small effects and values in bold indicate medium effects. All other values have no substantial effect. As before, only the trust in JonDonym has a medium-sized effect, implying the highest predictive power of all included exogenous variables.

5 Discussion and Conclusion

Based on our results, hypotheses H1 to H5 can be confirmed, whereas H6 and H7 cannot be confirmed (cf. Table 5). The results for H6 and H7 are very surprising,

Table 5. Summary of the Results

	Hypothesis	Result
H1:	Internet Users Information Privacy Concerns (IUIPC) have a negative effect on Trusting Beliefs (TB)	✓
H2:	Internet Users Information Privacy Concerns (IUIPC) have a positive effect on Risk Beliefs (RB)	✓
H3:	Trusting Beliefs (TB) have a negative effect on Risk Beliefs (RB)	✓
H4:	Internet Users Information Privacy Concerns (IUIPC) have a positive effect on the trusting beliefs in JonDonym (TB_{JD})	✓
H5:	Trusting beliefs in JonDonym (TB_{JD}) have a positive effect on the actualuse behavior of JonDonym (USE)	✓
H6:	Trusting beliefs (TB) have a negative effect on actual use behavior of JonDonym (USE)	✗
H7:	Risk beliefs (RB) have a positive effect on actual use behavior of JonDonym (USE)	✗

considering that they are in contrast to the rationale explained in Section 3.1 and the results from previous literature [6]. However, it must be said that it is possible that the relatively small sample size of 141 leads to a statistical non-significance when effect sizes are rather small. Therefore, we cannot rule out that the effects of risk beliefs and trusting beliefs on use would be significant with a larger sample size. Thus, only the degree of trust in the PET (JonDonym) has a significant and large effect on the use behavior. This result shows that it is crucial for a PET provider to establish a trustful reputation to get used. The trusting beliefs in the PET itself are positively influenced by the users' information privacy concerns. Thus, the results imply that users with a higher level of privacy concerns rather tend to trust a PET. The limitations of the study primarily concern the sample composition and size. First, a larger sample would have been beneficial. However, in general, a sample of 141 participants is acceptable for our kind of statistical analysis [16] and active users of a PET are hard to find for a relatively long online questionnaire. This is especially the case, if they do not have any financial rewards as in our study. Second, the combination of the results of the German and the English questionnaire can be a potential source for errors. Participants might have understood the questionnaire in German differently than the participants who filled out the English version. We argue that we achieved equivalence with regard to the meaning through conducting a thorough translation process, and therefore limiting this potential source of error to the largest extent possible. In addition, combining the data was necessary from a pragmatic point of view to get a sample size as large as possible for the statistical analysis.

Further work is required to investigate the specific determinants of use decisions for or against PETs and break down the interrelationships between the associated antecedents. In particular, it would be interesting to investigate the relationship between trusting beliefs in online companies and trust in the PET itself. A theoretical underlying is required to include this relationship in our structural equation model.

In this paper, we contributed to the literature on privacy-enhancing technologies and users' privacy by assessing the specific relationships between information privacy concerns, trusting beliefs in online firms and a privacy-enhancing technology (in our case JonDonym), risk beliefs associated with online firms data processing and the actual use behavior of JonDonym. By adapting and extending the IUIPC model by Malhotra et al.[6], we could show that several of the assumptions for regular online services do not hold for PETs.

Acknowledgments

This research was partly funded by the German Federal Ministry of Education and Research (BMBF) with grant number: 16KIS0371. In addition, we thank Rolf Wendolski (JonDos GmbH) for his help during the data collection process.

References

1. JonDos Gmbh: Official Homepage of JonDonym (2018)
2. David, E.E., Fano, R.M.: Some thoughts about the social implications of accessible computing. In: Proceedings 1965 Fall Joint Computer Conference. (1965) Available via http://www.multicians.org/fjcc6.html.
3. Bédard, M.: The underestimated economic benefits of the internet. Regulation series, The Montreal Economic Institute (2016) Economic Notes.
4. Mineo, L.: On internet privacy, be very afraid (Interview with Bruce Schneier). https://news.harvard.edu/gazette/story/2017/08/when-it-comes-to-internet-privacy-be-very-afraid-analyst-suggests/ (08 2017)
5. Singh, T., Hill, M.E.: Consumer privacy and the Internet in Europe: a view from Germany. Journal of consumer marketing **20**(7) (2003) 634–651
6. Malhotra, N.K., Kim, S.S., Agarwal, J.: Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. Information Systems Research **15**(4) (dec 2004) 336–355
7. Naeini, P.E., Bhagavatula, S., Habib, H., Degeling, M., Bauer, L., Cranor, L., Sadeh, N.: Privacy expectations and preferences in an iot world. In: Symposium on Usable Privacy and Security (SOUPS). (2017)
8. Heales, J., Cockcroft, S., Trieu, V.H.: The influence of privacy, trust, and national culture on internet transactions. In Meiselwitz, G., ed.: Social Computing and Social Media. Human Behavior, Cham, Springer International Publishing (2017) 159–176
9. Raber, F., Krueger, A.: Towards understanding the influence of personality on mobile app permission settings. In: IFIP Conference on Human-Computer Interaction, Springer (2017) 62–82
10. Borking, J.J., Raab, C.: Laws, PETs and Other Technologies for Privacy Protection. Journal of Information, Law and Technology **1** (2001) 1–14
11. Spiekermann, S.: The Desire for Privacy: Insights into the Views and Nature of the Early Adopters of Privacy Services. International Journal of Technology and Human Interaction **1**(1) (2005) 74–83

12. Lee, L., Fifield, D., Malkin, N., Iyer, G., Egelman, S., Wagner, D.: A Usability Evaluation of Tor Launcher. Proceedings on Privacy Enhancing Technologies (3) (2017) 90–109
13. Benenson, Z., Girard, A., Krontiris, I.: User Acceptance Factors for Anonymous Credentials: An Empirical Investigation. 14th Annual Workshop on the Economics of Information Security (WEIS) (2015) 1–33
14. Janic, M., Wijbenga, J.P., Veugen, T.: Transparency enhancing tools (tets): an overview. In: Socio-Technical Aspects in Security and Trust (STAST), 2013 Third Workshop on, IEEE (2013) 18–25
15. Hair, J.F., Ringle, C.M., Sarstedt, M.: PLS-SEM: Indeed a Silver Bullet. The Journal of Marketing Theory and Practice **19**(2) (2011) 139–152
16. Hair, J.F., Hult, G.T.M., Ringle, C.M., Sarstedt, M.: A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM). SAGE Publications (2017)
17. Stewart, K.A., Segars, A.H.: An Empirical Examination of the Concern for Information Privacy Instrument. Information Systems Research **13**(1) (2002) 36–49
18. Pavlou, P.A.: Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model. International Journal of Electronic Commerce **7**(3) (2003) 101–134
19. Harborth, D., Pape, S.: Exploring the Hype: Investigating Technology Acceptance Factors of Pokémon Go. In: 2017 IEEE International Symposium on Mixed and Augmented Reality (ISMAR). (2017) 155–168
20. Harborth, D., Pape, S.: Privacy Concerns and Behavior of Pokémon Go Players in Germany. In: Proceedings of IFIP Summer School on Privacy and Identity Management (IFIPSC2017). (2017) 1–18
21. Schmitz, C.: LimeSurvey Project Team (2015)
22. Ringle, C.M., Wende, S., Becker, J.M.: SmartPLS 3 (2015)
23. Henseler, J., Ringle, C.M., Sarstedt, M.: A new criterion for assessing discriminant validity in variance-based structural equation modeling. Journal of the Academy of Marketing Science **43**(1) (2015) 115–135
24. Malhotra, N.K., Kim, S.S., Patil, A.: Common Method Variance in IS Research: A Comparison of Alternative Approaches and a Reanalysis of Past Research. Management Science **52**(12) (2006) 1865–1883
25. Podsakoff, P.M., MacKenzie, S.B., Lee, J.Y., Podsakoff, N.P.: Common method biases in behavioral research: a critical review of the literature and recommended remedies. Journal of Applied Psychology **88**(5) (2003) 879–903
26. Blome, C., Paulraj, A.: Ethical Climate and Purchasing Social Responsibility: A Benevolence Focus. Journal of Business Ethics **116**(3) (2013) 567–585
27. Cohen, J.: Statistical Power Analysis for the Behavioral Sciences, HillsDale, NJ (1988)
28. Chin, W.W.: The Partial Least Squares Approach to Structural Equation Modeling. In Marcoulides, G.A., ed.: Modern Methods for Business Research. Lawrence Erlbaum, Mahwah, NJ (1998) 295–336
29. Rosen, L., Whaling, K., Carrier, L., Cheever, N., Rokkum, J.: The Media and Technology Usage and Attitudes Scale: An empirical investigation. Comput Human Behav. **29**(6) (2013) 2501–2511

A Questionnaire

The following items are measured with a seven-point Likert scale, ranging from "strongly disagree" to "strongly agree".

Collection (COLL)

1. It usually bothers me when online companies ask me for personal information.
2. When online companies ask me for personal information, I sometimes think twice before providing it.
3. It bothers me to give personal information to so many online companies.
4. Im concerned that online companies are collecting too much personal information about me.

Awareness (AWA)

1. Companies seeking information online should disclose the way the data are collected, processed, and used.
2. A good consumer online privacy policy should have a clear and conspicuous disclosure.
3. It is very important to me that I am aware and knowledgeable about how my personal information will be used.

Control (CONTROL)

1. Consumer online privacy is really a matter of consumers right to exercise control and autonomy over decisions about how their information is collected, used, and shared.
2. Consumer control of personal information lies at the heart of consumer privacy.
3. I believe that online privacy is invaded when control is lost or unwillingly reduced as a result of a marketing transaction.

Trusting Beliefs (TB)

1. Online companies are trustworthy in handling information.
2. Online companies tell the truth and fulfill promises related to information provided by me.
3. I trust that online companies would keep my best interests in mind when dealing with information.
4. Online companies are in general predictable and consistent regarding the usage of information.
5. Online companies are always honest with customers when it comes to using the provided information.

Risk Beliefs (RB)

1. In general, it would be risky to give information to online companies.
2. There would be high potential for loss associated with giving information to online firms.
3. There would be too much uncertainty associated with giving information to online firms.
4. Providing online firms with information would involve many unexpected problems.
5. I would feel safe giving information to online companies.

Trusting Beliefs in JonDonym ($\mathbf{TB_{JD}}$)

1. JonDonym ist trustworthy.
2. JonDonym keeps promises and commitments.
3. I trust JonDonym because they keep my best interests in mind.

Use Behavior (USE)

1. Please choose your usage frequency for JonDonym[3]

- Never
- Once a month
- Several times a month
- Once a week
- Several times a week
- Once a day
- Several times a day
- Once an hour
- Several times an hour
- All the time

[3] The frequency scale is adapted from Rosen et al. [29].