How Privacy Concerns and Trust and Risk Beliefs Influence Users' Intentions to Use Privacy-Enhancing Technologies - The Case of Tor

David Harborth
Chair of Mobile Business and Multilateral Security
Goethe University Frankfurt am Main
david.harborth@m-chair.de

Sebastian Pape
Chair of Mobile Business and Multilateral Security
Goethe University Frankfurt am Main
sebastian.pape@m-chair.de

Abstract

Due to an increasing collection of personal data by internet companies and several data breaches, research related to privacy gained importance in the last years in the information systems domain. Privacy concerns can strongly influence users' decision to use a service. The Internet Users Information Privacy Concerns (IUIPC) construct is one operationalization to measure the impact of privacy concerns on the use of technologies. However, when applied to a privacy enhancing technology (PET) such as an anonymization service the original rationales do not hold anymore. In particular, an inverted impact of trusting and risk beliefs on behavioral intentions can be expected. We show that the IUIPC model 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 itself. A survey among 124 users of the anonymization service Tor shows that they have a significant effect on the actual use behavior of the PET.

1. Introduction

"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." [1]. Privacy and the related concerns have been discussed since the very beginning of computer sharing [2]. Due to a raising economic interest in personal data during the last years [3], privacy gains an increasing importance in individuals' everyday life. The majority of internet users has privacy concerns and feels a strong need to protect their privacy [4].

A popular model for measuring and explaining privacy concerns of online users is the model focusing on the Internet Users Information Privacy Concerns (IUIPC) construct by Malhotra et al. [5]. 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 [6], internet transactions [7] and Mobile Apps [8]. Originally, the IUIPC instrument was applied to use cases for individuals' decisions to disclose personal information to service providers. However, for privacy enhancing technologies (PETs) the primary purpose is to help users to protect personal information when using regular internet services. As a consequence, it is necessary to reconsider the impact of trust and risk beliefs within IUIPC's causal model with respect to PETs. We expected this impact to be inverted and thus the trust model needs to be adapted for the investigation of PETs. In addition, trust in the PET itself is an important factor to consider. This is the case since Tor is used by a diverse group of people whose life might be endangered in case their identity is revealed (e.g. whistleblowers, opposition supporters, etc. [9]). To the best of our knowledge the IUIPC construct has never been applied to a PET. Thus, we address the following research questions:

1. *What influence have privacy concerns and associated trust and risk beliefs on the behavioral intention and actual use of Tor?*
2. *What influence does trust in Tor itself have on the behavioral intention and the actual use?*

For that purpose, we conducted an online survey with users of one of the most widely used anonymization services Tor (Tor has approximately 2,000,000 regular users) [9]. We collected 124 complete questionnaires out of 314 participants for the empirical analysis. 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 as follows: Sect. 2 introduces Tor and lists related work on PETs. In Sect. 3, we present research hypotheses and the data collection process. We assess the reliability and validity of our results in Sect. 4. In Sect. 5, we discuss the implications and limitations of our work and suggest future work.

This research was partly funded by the German Federal Ministry of Education and Research (BMBF) with grant number: 16KIS0371.

URI: https://hdl.handle.net/10125/59923
ISBN: 978-0-9981331-2-6

2. Background and Related Work

Privacy-Enhancing Technologies (PETs) is an umbrella term for different privacy protecting technologies. PETs can be defined 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, p. 1].

In this paper, we investigate the privacy, trust and risk beliefs associated with PETs for the case of the anonymity service Tor [9]. Tor is a free-to-use anonymity service that is based on the onion routing principle. Everybody can operate a server (relay) over which the encrypted traffic is routed. The routing occurs randomly over several different servers distributed world-wide. Tor aims to protect against an adversary who can observe or control some fraction of network traffic, but it does not protect against a global passive adversary, which means an adversary who can observe all network connections. Among the available PETs, Tor has one of the biggest user bases with approximately 2,000,000 active users [9].

Related 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. [11] assess the usability of the Tor Launcher and propose recommendations to overcome the found usability issues. Benenson et al. [12] 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 hypothesize that trust in Tor has a positive effect on the actual use of the service (see Section 3.1). Another highly relevant study for our research is the one by Brecht et al. [13], who investigate acceptance factors of anonymization services. Among other variables, they hypothesize a positive influence of privacy concerns on the intention to use such a service. Although they find a statistically significant effect, the effect is relatively small (effect size of 0.061) compared to other variables like perceived usefulness or internet privacy awareness. In contrast to our study, Brecht et al. [13] use another operationalization of privacy concerns (the one by Dinev and Hart [14]) and they do not investigate it in the nomological network with trust and risk beliefs.

3. Methodology

We base our research on the Internet Users Information Privacy Concerns (IUIPC) model by Malhotra et al. [5]. 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 are focusing on the role of privacy concerns, trust and risk beliefs for the case of a PET (i.e. Tor), we adapt the original model according to the following logic. Originally, the service in question can be seen as the attacker (from a privacy point of view). If we apply the model to a service with the opposite goal, namely protecting the privacy of its users, certain relationships need to change. We will elaborate on the detailed changes in the next section. In addition, to this 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). Since our research goal is to predict the target constructs behavioral intention and actual use behavior of Tor, we use partial least squares SEM (PLS-SEM) for our analysis [15, 16] and not covariance-based SEM. In the following subsections, we discuss the hypotheses based on the IUIPC model [5], the questionnaire and the data collection process.

3.1. Research Hypotheses

The structural model contains several relationships between exogenous and endogenous variables (cf. Fig. 1). We develop our research hypotheses for these relationships along the hypotheses of the IUIPC model [5]. IUIPC is operationalized as a second-order construct[1] of the sub-constructs collection (COLL), awareness (AWA) and control (CONTROL). Thus, the users' privacy concerns are determined by their concerns about "[...] individual-specific data possessed by others relative to the value of benefits receive" [5, 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" [5, p. 339].

The effect of IUIPC on the behavioral intention is mediated by trusting beliefs and risk beliefs. Trusting beliefs are 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 [5]. Thus, the higher the privacy concerns of a user, the lower are his or her trusting beliefs and the higher are his or her risk beliefs. In addition, a higher level of trust is assumed to decrease the risk beliefs. Thus, we hypothesize:

[1] Due to space limitations, we will not elaborate on second-order constructs in more detail. For an extensive discussion see Steward [17].

1. *Internet Users Information Privacy Concerns (IUIPC) have a negative effect on Trusting Beliefs (TB).*
2. *Internet Users Information Privacy Concerns (IUIPC) have a positive effect on Risk Beliefs (RB).*
3. *Trusting Beliefs (TB) have a negative effect on Risk Beliefs (RB).*

Since we investigate the use of a specific PET, we extend the model by the trust in Tor itself with the adapted 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 which process personal data. This is especially true, because we surveyed users of a PET which are assumed to take great care of their privacy. Therefore, we hypothesize:

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

Trust is an important factor in the acceptance decision of users [18]. Mcknight et al. [19] show that trust in a specific technology will positively affect individuals intention to explore the technology and to use more features of the technology in a postadoption context. Especially for the case of privacy protection, we assume that trust in the technology is a major factor for the intention to use the technology. For a further discussion on the concept of trust in a technology, we refer to Lankton et al. [20]. We hypothesize that:

5. *Trusting beliefs in Tor (TB_{Tor}) have a positive effect on the behavioral intention to use Tor (BI).*

It is logical that trusting beliefs have a positive effect and risk beliefs have a negative effect on releasing data and thus the intended behavior of using a regular service. However, for 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 Tor, since the protection of data becomes less important. Following this rationale, a higher degree of risk beliefs in data processing of online firms leads to a higher degree of use. Thus, we hypothesize that:

6. *Trusting beliefs (TB) have a negative effect on the behavioral intention to use Tor (BI).*
7. *Risk beliefs (RB) have a positive effect on the behavioral intention to use Tor (BI).*

Research on the relationship between behavioral intention and use behavior goes back to Fishbein et al. [21]. Later research indicates a positive link between the two constructs [22]. Thus, we hypothesize that:

8. *The behavioral intention to use Tor (BI) has a positive effect on the actual use behavior (USE).*

3.2. Data Collection

The questionnaire constructs are adapted from the original IUIPC paper [5]. We conducted the study with German and English speaking Tor 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. 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 B.

Since we investigate the effect of privacy concerns, trust and risk beliefs on the use of Tor, we collected data of actual users. We installed the surveys on a university server and managed it with the survey software LimeSurvey (version 2.72.6) [23]. The links to the English and German version were distributed over multiple channels on the internet. Although there are approximately 2,000,000 active users of the service, it was relatively difficult to gather the necessary number of complete answers for a valid and reliable quantitative analysis. Thus, to foster future research about Tor users, we provide an overview of every distribution channel in the Appendix A. In sum, 314 participants started the questionnaire (245 for the English version, 40 for the English version posted in hidden service forums and 29 for the German version). Of those 314 approached participants, 135 (105 for the English version, 13 for the English version posted in hidden service forums and 17 for the German version) filled out the questionnaires completely. After deleting all sets from participants who answered a test question in the middle of the survey incorrectly, 124 usable data sets remained for the following analysis.

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 had to 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 [4].

4. Results

We tested the model using SmartPLS version 3.2.7 [24]. 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].

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 RISK. However, for the composite reliability the value for RISK is higher than 0.7. Therefore, we argue that ICR is not a major 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. Since IUIPC and USE are single-item constructs they have ICR values of 1.

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 were higher than 0.7, except for TRUST4 with a value of 0.275. Therefore, we dropped this item after an initial analysis. 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 investigating 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 [25]. HTMT divides between-trait correlations by within-trait correlations, therefore providing a measure of what the true correlation of two constructs would be if the measurement is flawless [16]. Values close to 1 for HTMT indicate a lack of discriminant validity. A conservative threshold is 0.85 [25]. Table 3 contains the values for HTMT and no value, except for the correlation between IUIPC and COLL (with 0.888), is above the suggested threshold of 0.85. To assess if the HTMT statistics are significantly different from 1, we conducted a bootstrapping procedure with 5,000 subsamples 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, and 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 [26]. Since this is the case in our research design, the need to

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

Construct	AWA	CONTROL	COLL	RB	TB	TB_{Tor}	BI	IUIPC	USE
AWA1	**0.911**	0.234	0.302	0.223	-0.136	0.066	0.202	0,630	-0.124
AWA2	**0.923**	0.230	0.219	0.136	-0.155	0.072	0.198	0.586	-0.171
AWA3	**0.891**	0.323	0.315	0.221	-0.103	0.066	0.250	0.660	-0.059
CONTROL1	0.095	**0.825**	0.271	0.106	-0.167	0.137	0.215	0.475	-0.021
CONTROL2	0.405	**0.821**	0.226	0.245	-0.156	0.132	0.237	0.577	-0.033
CONTROL3	0.174	**0.756**	0.438	0.214	-0.345	0.098	0.099	0.578	0.068
COLL1	0.264	0.358	**0.888**	0.547	-0.468	0.176	0.301	0.742	0.045
COLL2	0.206	0.332	**0.812**	0.205	-0.335	0.232	0.376	0.665	0.042
COLL3	0.292	0.359	**0.906**	0.444	-0.446	0.272	0.376	0.764	0.071
COLL4	0.304	0.309	**0.850**	0.467	-0.403	0.182	0.316	0.720	0.091
RB1	0.196	0.200	0.487	**0.880**	-0.453	0.217	0.258	0.429	-0.015
RB2	0.170	0.160	0.326	**0.831**	-0.298	0.156	0.233	0.312	0.015
RB3	0.155	0.252	0.364	**0.857**	-0.354	0.233	0.221	0.359	0.007
RB4	0.245	0.231	0.374	**0.827**	-0.260	0.257	0.326	0.396	0.042
RB5	-0.105	-0.145	-0.427	**-0.702**	0.401	-0.004	-0.144	-0.339	0.003
TB1	-0.149	-0.261	-0.455	-0.417	**0.898**	-0.097	-0.265	-0.412	-0.050
TB2	-0.118	-0.186	-0.410	-0.377	**0.887**	-0.033	-0.194	-0.347	-0.109
TB3	-0.107	-0.339	-0.397	-0.395	**0.775**	-0.131	-0.155	-0.387	-0.007
TB5	-0.069	-0.009	-0.219	-0.070	**0.663**	-0.109	-0.169	-0.158	-0.007
$TB_{Tor}1$	0.064	0.149	0.257	0.159	-0.087	**0.879**	0.561	0.225	-0.050
$TB_{Tor}2$	0.077	0.121	0.236	0.244	-0.124	**0.925**	0.554	0.209	-0.020
$TB_{Tor}3$	0.059	0.138	0.169	0.178	-0.079	**0.883**	0.488	0.169	0.002
BI1	0.236	0.240	0.355	0.228	-0.249	0.586	**0.865**	0.384	0.166
BI2	0.262	0.202	0.322	0.319	-0.152	0.465	**0.859**	0.363	0.075
BI3	0.143	0.158	0.363	0.234	-0.233	0.522	**0.923**	0.323	0.216
IUIPC	0.691	0.685	0.837	0.451	-0.431	0.226	0.404	**1,000**	-0.009
USE	-0.128	0.008	0.073	0.010	-0.059	-0.026	0.177	-0.009	**1,000**
Cronbach's α	0.894	0.722	0.887	0.567	0.831	0.877	0.859	1.000	1.000
Comp. Reliability	0.934	0.843	0.922	0.817	0.884	0.924	0.914	1.000	1.000

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 [27]. 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 [27]. The test shows that seven factors have eigenvalues larger than 1 which account for 75.35% of the total variance. The first factor explains 30.29% of the total variance. Based on the results of previous literature [28], 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 (VIF). All VIFs above 5 indicate that collinearity between constructs is present. For our model, the highest VIF is 1.278. Thus collinearity is apparently not an issue.

Significance and Relevance of Model Relationships Figure 1 shows the results of the path estimations and the R^2-values of the endogenous variables BI and USE. The R^2 is 0.400 for BI and 0.031 for USE. Thus, our models explains 40% of the variance of BI and 3.1% of 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 BI is weak to moderate and for USE the value is very weak. For use behavior

Table 2. Discriminant Validity with AVEs and Construct Correlations

Constructs (AVE)	AWA	BI	COLL	CONTROL	IUIPC	RB	TB	TB_{Tor}	USE
AWA (0.825)	0.908								
BI (0.780)	0.240	0.883							
COLL (0.748)	0.309	0.395	0.865						
CONTROL (0.642)	0.291	0.228	0.393	0.801					
IUIPC (1.000)	0.691	0.404	0.837	0.685	1,000				
RB (0.675)	0.215	0.291	0.486	0.242	0.451	0.822			
TB (0.658)	-0.143	-0.244	-0.480	-0.283	-0.431	-0.434	0.811		
TB_{Tor} (0.803)	0.075	0.599	0.249	0.152	0.226	0.216	-0.109	0.896	
USE (1.000)	-0.128	0.177	0.073	0.008	-0.009	0.010	-0.059	-0.026	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.

Table 3. Heterotrait-Monotrait Ratio (HTMT)

Constructs	AWA	BI	COLL	CONTROL	IUIPC	RB	TB	TB_{Tor}	USE
BI	0.274								
COLL	0.343	0.452							
CONTROL	0.346	0.290	0.486						
IUIPC	0.728	0.436	0.888	0.798					
RB	0.238	0.337	0.541	0.294	0.478				
TB	0.159	0.278	0.528	0.336	0.439	0.449			
TB_{Tor}	0.084	0.681	0.280	0.192	0.240	0.244	0.131		
USE	0.138	0.186	0.077	0.060	0.009	0.021	0.058	0.029	

several participants answered that they never use Tor (21 participants answered "never") although they stated to use the service several years (answers to the question: How many years are you using Tor? with a median of 6 years and an average of 6.87 years on a seven-point Likert scale). The correlation coefficient between the years of using Tor and the use frequency is very small, negative and statistically insignificant with -0.0222 and a p-value of 0.8066. These 21 answers massively bias the results for the relationship between behavioral intention and actual use behavior (the median value of use frequency is 5). However, we cannot explain why the participants answered like this. They either misunderstood the question, answered it intentionally like this to disguise their activity with Tor or found the scale for use behavior inappropriate. This might be due to the fact that the scale only contains "once a month" as the lowest use frequency besides "never". It might be possible that these 21 users use Tor only a few times per year or that they used Tor some years ago and have not used it again since then. Therefore, they might have chosen never as an answer. However, we used an established scale to measure use behavior [29], but recommend to consider this issue in future research studies with a similar context.

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. We chose this p-value range since p-values tend to be larger if the sample size is comparable small and we wanted to capture also significant effects above the 5% level. 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 shown by the relative size of the coefficient compared to the other explanatory variables [16].

It can be seen that IUIPC has a relatively large statistically significant negative effect on trusting beliefs and a positive effect on risk beliefs. The effect of IUIPC on trusting beliefs in Tor is significant, positive and relatively weak compared to the other significant effects in the model. The construct trusting beliefs has a statistically significant medium-sized negative effect on risk beliefs. The effects of trusting beliefs and risk beliefs on behavioral intention are not statistically significant (for both $p \geq 0.10$). In contrast, the effect of trusting beliefs in Tor on behavioral intention is highly statistically significant, positive and large with 0.560.

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 [30], 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, values

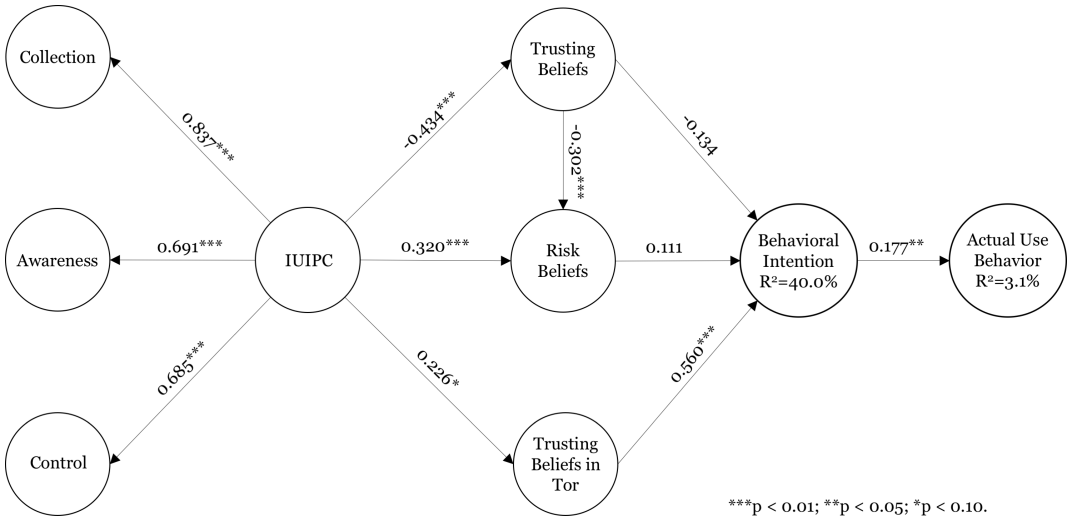

Figure 1. Path Estimates and Adjusted R^2 values of the Structural Model

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

Variables	f^2	q^2
Endogenous / Exogenous	BI	BI
RB	0.016	0.018
TB	*0.025*	*0.025*
TB_{Tor}	***0.499***	***0.766***

in bold indicate medium effects and values in bold and italics indicate large effects. All other values have no substantial effect. The results correspond to those of the previous analysis of the path coefficients whereas trusting beliefs have a small effect on the behavioral intention to use tor. As the path estimates have shown, trust in tor has a large effect on the behavioral intention.

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 [31]. Values above 0 indicate that the model has the property of predictive relevance. In our case, the Q^2 value is equal to 0.278 for BI and 0.002 for USE. Since they are larger than zero, 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 [16]. 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 [30]. 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 Tor has a large effect, implying the highest predictive power of all included exogenous variables.

5. Discussion and Conclusion

Based on our results, hypotheses H1 to H5 and H8 can be confirmed, whereas H6 and H7 cannot be confirmed (cf. Table 5). The results for H6 and H7 are surprising, considering that they are in contrast to the rationale explained in Sect. 3.1 and the results from previous literature [5]. However, it must be said that when effect sizes are rather small it is possible that the relatively small sample size of 124 leads to a statistical non-significance. Thus, we cannot rule out that the effects of risk beliefs and trusting beliefs on behavioral intention would be significant with a larger sample size. Thus, only the degree of trust in the PET (Tor) has a direct significant effect on the intention to use the PET. This result shows that a reputation of being trustworthy is crucial for a PET provider. 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

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 Tor (TB_{Tor})	✓
H5:	Trusting beliefs in Tor (TB_{Tor}) have a positive effect on the behavioral intention to use Tor (BI)	✓
H6:	Trusting beliefs (TB) have a negative effect on the behavioral intention to use Tor (BI)	✗
H7:	Risk beliefs (RB) have a positive effect on the behavioral intention to use Tor (BI)	✗
H8:	The behavioral intention to use Tor (BI) has a positive effect on the actual use behavior (USE)	✓

would have been beneficial. However, in general, a sample of 124 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 and if they are highly privacy sensitive which might repel them to disclose any kind of information (even if it is anonymous). Second, the combination of the results of the German and the English questionnaire can be a potential source of errors. German participants might have understood questions differently than the English participants. 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. Lastly, possible self-report biases (e.g. social desirability) might exist. We addressed this possible issue by gathering the data fully anonymized. As discussed earlier, we had issues with certain data sets of participants with regard to actual use behavior (cf. Sect. 4.2.). Although it might be more beneficial in certain settings to directly refer to actual use behavior as the sole target variable, we decided to include behavioral intention as an antecedent because of these issues.

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 research 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 Tor), risk beliefs associated with online firms data processing and the actual use behavior of Tor. By adapting and extending the IUIPC model by Malhotra et al. [5], we could show that several of the assumptions for regular online services do not hold for PETs.

References

[1] L. Mineo, "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.

[2] E. E. David and R. M. Fano, "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] M. Bédard, "The underestimated economic benefits of the internet," regulation series, The Montreal Economic Institute, 2016. Economic Notes.

[4] T. Singh and M. E. Hill, "Consumer privacy and the Internet in Europe: a view from Germany," *Journal of consumer marketing*, vol. 20, no. 7, pp. 634–651, 2003.

[5] 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, pp. 336–355, dec 2004.

[6] P. E. Naeini, S. Bhagavatula, H. Habib, M. Degeling, L. Bauer, L. Cranor, and N. Sadeh, "Privacy expectations and preferences in an iot world," in *Symposium on Usable Privacy and Security (SOUPS)*, 2017.

[7] J. Heales, S. Cockcroft, and V.-H. Trieu, "The influence of privacy, trust, and national culture on internet transactions," in *Social Computing and*

Social Media. Human Behavior (G. Meiselwitz, ed.), (Cham), pp. 159–176, Springer International Publishing, 2017.

[8] F. Raber and A. Krueger, "Towards understanding the influence of personality on mobile app permission settings," in *IFIP Conference on Human-Computer Interaction*, pp. 62–82, 2017.

[9] The Tor Project. https://www.torproject.org, 2018.

[10] J. J. Borking and C. Raab, "Laws, PETs and Other Technologies for Privacy Protection," *Journal of Information, Law and Technology*, vol. 1, pp. 1–14, 2001.

[11] L. Lee, D. Fifield, N. Malkin, G. Iyer, S. Egelman, and D. Wagner, "A Usability Evaluation of Tor Launcher," *Proceedings on Privacy Enhancing Technologies*, no. 3, pp. 90–109, 2017.

[12] Z. Benenson, A. Girard, and I. Krontiris, "User Acceptance Factors for Anonymous Credentials: An Empirical Investigation," *14th Annual Workshop on the Economics of Information Security (WEIS)*, pp. 1–33, 2015.

[13] F. Brecht, B. Fabian, S. Kunz, and S. Mueller, "Are You Willing to Wait Longer for Internet Privacy?," in *ECIS 2011 Proceedings*, 2011.

[14] 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.

[15] J. Hair, C. M. Ringle, and M. Sarstedt, "PLS-SEM: Indeed a Silver Bullet," *The Journal of Marketing Theory and Practice*, vol. 19, no. 2, pp. 139–152, 2011.

[16] J. Hair, G. T. M. Hult, C. M. Ringle, and M. Sarstedt, *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*. SAGE Publications, 2017.

[17] K. A. Stewart and A. H. Segars, "An Empirical Examination of the Concern for Information Privacy Instrument," *Information Systems Research*, vol. 13, no. 1, pp. 36–49, 2002.

[18] P. A. Pavlou, "Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model," *International Journal of Electronic Commerce*, vol. 7, no. 3, pp. 101–134, 2003.

[19] D. H. Mcknight, M. Carter, J. B. Thatcher, and P. F. Clay, "Trust in a specific technology: An investigation of its components and measures," *ACM Transactions on Management Information Systems (TMIS)*, vol. 2, no. 2, p. 12, 2011.

[20] N. K. Lankton, D. H. McKnight, and J. Tripp, "Technology, humanness, and trust: Rethinking trust in technology," *Journal of the Association for Information Systems*, vol. 16, no. 10, p. 880, 2015.

[21] M. Fishbein and I. Ajzen, *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*. Reading, MA: Addison-Wesley, 1975.

[22] B. H. Sheppard, J. Hartwick, and P. R. Warshaw, "The Theory of Reasoned Action: A Meta-Analysis of Past Research with Recommendations for Modifications and Future Research," *Journal of Consumer Research*, vol. 15, no. 3, pp. 325–343, 1988.

[23] C. Schmitz, "LimeSurvey Project Team." http://www.limesurvey.org, 2015.

[24] C. M. Ringle, S. Wende, and J. M. Becker, "SmartPLS 3." http://www.smartpls.com, 2015.

[25] J. Henseler, C. M. Ringle, and M. Sarstedt, "A new criterion for assessing discriminant validity in variance-based structural equation modeling," *Journal of the Academy of Marketing Science*, vol. 43, no. 1, pp. 115–135, 2015.

[26] N. K. Malhotra, S. S. Kim, and A. Patil, "Common Method Variance in IS Research: A Comparison of Alternative Approaches and a Reanalysis of Past Research," *Management Science*, vol. 52, no. 12, pp. 1865–1883, 2006.

[27] 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.

[28] C. Blome and A. Paulraj, "Ethical Climate and Purchasing Social Responsibility: A Benevolence Focus," *Journal of Business Ethics*, vol. 116, no. 3, pp. 567–585, 2013.

[29] L. Rosen, K. Whaling, L. Carrier, N. Cheever, and J. Rokkum, "The Media and Technology Usage and Attitudes Scale: An empirical investigation," *Comput Human Behav.*, vol. 29, no. 6, pp. 2501–2511, 2013.

[30] J. Cohen, *Statistical Power Analysis for the Behavioral Sciences*. 1988.

[31] W. W. Chin, "The Partial Least Squares Approach to Structural Equation Modeling," in *Modern Methods for Business Research* (G. A. Marcoulides, ed.), pp. 295–336, Mahwah, NJ: Lawrence Erlbaum, 1998.

A. Distribution Channels of the Tor Online Survey

1. Mailinglists:
   (a) tor-talk[2]
   (b) liberationtech[3]
   (c) IFIP TC 11[4]
   (d) FOSAD[5]
   (e) GI PET[6]
   (f) GI FBSEC[7]
2. Twitter with #tor and #privacy
3. Boards:
   (a) reddit (sub-reddits: r/TOR, r/onions, r/privacy)
   (b) ubuntuusers.de
4. Tor Hidden Service Boards, Sections posted into:
   (a) Darknet Avengers[8], Off Topic
   (b) The Hub[9], Beginners
   (c) Onion Land[10], Off Topic
   (d) 8chan[11], /tech/
   (e) IntelExchange[12], Unverified Users
   (f) Code Green[13], Discussions
   (g) Changolia[14], overchan.random
   (h) Atlayo[15], Posting
5. Personal Announcements at Workshops

B. Questionnaire

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

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.

Trusting Beliefs in Tor (TB_{Tor})

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

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.

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.

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.

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.

Behavioral Intention (BI)

1. I intend to continue using Tor in the future.
2. I will always try to use Tor in my daily life.
3. I plan to continue to use Tor frequently.

Use Behavior (USE)

1. Please choose your usage frequency for Tor[16]

- 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

[2] https://lists.torproject.org/cgi-bin/mailman/listinfo/tor-talk/
[3] https://mailman.stanford.edu/mailman/listinfo/liberationtech
[4] https://dlist.server.uni-frankfurt.de/mailman/listinfo/ifip-tc11
[5] http://www.sti.uniurb.it/events/fosad/
[6] http://mail.gi-fb-sicherheit.de/mailman/listinfo/pet
[7] http://mail.gi-fb-sicherheit.de/mailman/listinfo/fbsec
[8] http://avengersdutyk3xf.onion/
[9] http://thehub7xbw4dc5r2.onion
[10] http://onionlandbakyt3j.onion
[11] http://oxwugzccvk3dk6tj.onion
[12] http://rrcc5uuudhh4oz3c.onion
[13] http://pyl7a4ccwgpxm6rd.onion
[14] http://jewsdid.oniichanylo2tsi4.onion
[15] http://atlayofke5rqhsma.onion/
[16] The frequency scale is adapted from Rosen et al. [29].