HOW PRIVACY CONCERNS, TRUST AND RISK BELIEFS AND PRIVACY LITERACY 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

Dr. Sebastian Pape
Chair of Mobile Business and Multilateral Security, Goethe University Frankfurt am Main

Acknowledgments

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

Accepted at: ACM SIGMIS The DATA BASE for Advances in Information Systems (forthcoming 2020)

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 trusting beliefs in the anonymization service itself as well as a measure for privacy literacy. A survey among 124 users of the anonymization service Tor shows that trust in Tor has a statistically significant effect on the actual use behavior of the PET. In addition, the results indicate that privacy literacy has a negative impact on trusting beliefs in general and a positive effect on trust in Tor.

Keywords: Privacy Concerns; Tor; Privacy-Enhancing Technologies; Privacy Literacy; Technology Use

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." (Mineo, 2017). Privacy and the related concerns have been discussed since the very beginning of computer sharing (David & Fano, 1965). Due to a raising economic interest in personal data during the last years (Bédard, 2016), 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 (Singh & Hill, 2003).

However, technologies which are able to protect users' privacy (PETs) are not widely adopted yet (Rossnagel, 2010). Among others, privacy concerns (Angst & Agarwal, 2009; Slyke, Johnson, Jiang, & Shim, 2006) and trust-risk-relationships (Harborth & Pape, 2018b, 2019; Smith, Dinev, & Xu, 2011) are assumed to have an important effect on the adoption of technologies. We argue that privacy concerns might have an important effect in the case of PETs, too. 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, Kim, & Agarwal (2004). 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 (Naeini et al., 2017), internet transactions (Heales, Cockcroft, & Trieu, 2017) and mobile apps (Raber & Krueger, 2017). 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. (The Tor Project, 2018)). Besides users' concerns and trust, it is also important to consider the users' knowledge and capabilities. Users' attitudes often differ from the decisions they make ('privacy paradox') (Dienlin & Trepte, 2015). One way to explain the privacy paradox is that users balance between potential risks and benefits they gain from the service (privacy calculus) (Dinev & Hart, 2006). Another way to explain it is that users are concerned but lack knowledge to react in a way that would reflect their needs (Trepte et al., 2015).

Since we are surveying active users of Tor, both argumentations do not fit. In the former case, we have already explained that PETs are different than regular internet services since their primary goal is to protect the users' privacy. In the latter case, users have already installed the PET and use it. However, we still argue that it is important to consider the users' capabilities since users need a certain amount of knowledge in order to adequately evaluate the given level of privacy (Masur, Teutsch, & Trepte, 2017; Park, 2013). Thus, their knowledge might influence the users' trusting and risk beliefs in online companies and in particular the users' trusting beliefs in Tor. For that purpose, we measured the users' privacy literacy with the "Online Privacy Literacy Scale" (OPLIS) developed by Trepte et al. (2015).

To the best of our knowledge the OPLIS instrument in combination with 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?
3. What influence does privacy literacy (measured with the OPLIS scale) have on trusting beliefs, risk beliefs and trusting beliefs in Tor?

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) (The Tor Project, 2018). 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: Section 2 introduces Tor and lists related work on PETs. In Section 3, we present research hypotheses and the data collection process. We assess the reliability and validity of our results in Section 4. In Section 5, we discuss the implications and limitations of our work and suggest future work. We conclude the article in Section 6.

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" (Borking & Raab, 2001, p. 1).

Privacy Enhancing Technologies and Tor

In this paper, we investigate the privacy, trust and risk beliefs associated with PETs for the case of the anonymity service Tor. Tor is a free-to-use anonymity service that is based on the onion routing principle. The development of Tor started in 1995 in the Naval Research Lab (NRL). At that time the general idea was that one should be able to communicate over the Internet without revealing oneself to the other party (The Tor Project, 2018). 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 (The Tor Project, 2018).

Related work on PETs considers mainly usability studies and to the best of our knowledge only two articles exist which focus on privacy concerns and related trust and risk beliefs of users of the PETs Tor and JonDonym (JonDos Gmbh, 2018). The two articles extend the IUIPC model by adding trust in the respective PET and find that the PET-specific trust (in Tor and JonDonym, respectively) has a large statistically significant positive effect on usage (Harborth & Pape, 2018b, 2019). Lee et al. (2017) assess the usability of the Tor Launcher and propose recommendations to overcome the found usability issues. Benenson, Girard, & Krontiris (2015) 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). This hypothesis is supported by other research on technology acceptance factors of Tor which finds that trust in Tor is a highly relevant factor driving the use intention of the PET (Harborth & Pape, 2018a). Other research results indicate that trust in a PET has a positive effect on the willingness to pay money for this PET (Harborth, Cai, & Pape, 2019).

Privacy Concerns

A highly relevant study for our research is the one by Brecht et al. (2011), 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. (2011) use another operationalization of privacy concerns (Dinev & Hart, 2006) and they do not investigate it in the nomological network with trust and risk beliefs. However, it is highly relevant for constructs such as IUIPC and OPLIS to establish nomological validity (Straub, Boudreau, & Gefen, 2004). Therefore, we contribute to the theoretical discourse about privacy literacy and privacy concerns by including an operationalization of privacy literacy (OPLIS) and privacy concerns (IUIPC) in one nomological network with the trust-risk relationships discussed before. We decided to use the operationalization for privacy concerns as in the original IUIPC paper (Malhotra et al., 2004). Thus, IUIPC is a second-order variable consisting of the constructs collection, control and awareness.

Online Privacy Literacy

Park (2013) defines online privacy literacy as a "principle to support, encourage, and empower users to undertake informed control of their digital identities". Trepte et al. (2015) give an exhaustive summary on the development of (online) privacy literacy. Several studies exist which aim to measure users' privacy literacy. Hoofnagle et al. (2010) ask users to answer whether five given statements about information handling of providers are true.

Brecht et al. (2012) find that users generally have a low knowledge about privacy issues on the Internet. They also find a negative correlation between a users' stated and their actual knowledge of privacy issues. Morrison (2013) investigates the same questions and asks ten objective questions and compares the results to three subjective questions (self-assessments). He finds that the users' self-assessment differs greatly from their objective knowledge about privacy. This cognitive bias where people mistakenly assess their cognitive ability as greater as than it is, is called Dunning-Kruger effect (Kruger & Dunning, 1999). As a consequence, users' statements on their knowledge about privacy cannot be trusted and other scales with users' self-assessments (cf. Park, 2013) are not further discussed here. Trepte et al. (2015) define online privacy literacy as "a combination of factual or declarative (knowing that) and procedural (knowing how) knowledge about online privacy" and implemented a scale based on "objective knowledge" to measure privacy literacy: the online privacy literacy scale (OPLIS). OPLIS consists of 20 questions divided into the following four knowledge groups:

4. practices of organizations, institutions and online service providers
5. technical aspects of data protection;
6. data protection law in Germany and Europe;
7. data protection strategies.

Since the constructs for data protection laws were specific for Germany and Europe and we surveyed Tor users worldwide, we needed to remove them (cf. Section 3.3).

Trepte and Masur (2017) apply a short version of OPLIS for a descriptive study. Joeckel and Dogruel (2019) investigate OPLIS, too. They find two correlations with the OPLIS score: a medium-sized with age (older participants know more about online privacy), and a weaker with privacy concerns (more privacy literate users were more concerned about their privacy). However, their correlation analysis does not offer any causality. Thus, it is unclear if more concerned users know more about privacy or users who know more are more concerned.

Methodology

We base our research on the Internet Users Information Privacy Concerns (IUIPC) model by Malhotra et al. (2004). 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 (Hair, Hult, Ringle, & Sarstedt, 2017; Hair, Ringle, & Sarstedt, 2011) and not covariance-based SEM. In the following subsections, we discuss the hypotheses based on the IUIPC model (Malhotra et al., 2004), the questionnaire and the data collection process.

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. IUIPC is operationalized as a second-order construct 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" (Malhotra et al., 2004, 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" (Malhotra et al., 2004, 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 (Malhotra et al., 2004). 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:

> Hypothesis 1 (H1): Internet Users Information Privacy Concerns (IUIPC) have a negative effect on Trusting Beliefs (TB).
>
> Hypothesis 2 (H2): Internet Users Information Privacy Concerns (IUIPC) have a positive effect on Risk Beliefs (RB).
>
> Hypothesis 3 (H3): 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 (2003). 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:

> Hypothesis 4 (H4): Internet Users Information Privacy Concerns (IUIPC) have a positive effect on the trusting beliefs in Tor (TB_{Tor}).

Privacy literacy is not a widely used concept in the information systems domain when investigating information privacy. Based on a representative selection of literature, Smith, Dinev, & Xu (2011) derive the "APCO" macro model summarizing related concepts and their relations to privacy concerns. However, no variable is or is related to privacy literacy. To the best of our knowledge, the construct we use in our analysis (OPLIS) is also not investigated in a nomological network with privacy concerns and outcome variables as behavioral intention or use. Therefore, we searched primarily for "privacy literacy" on Google Scholar as we argue that OPLIS operationalizes this concept. We find different applications and definitions of the concept "privacy literacy" in the literature. For example, online privacy literacy is defined as "[...] users' knowledge of privacy control tools (passive), and their actual application (active) to obscure the users' identity and protect his/her personal information on the internet" (Weinberger, Zhitomirsky-Geffet, & Bouhnik, 2017, p. 656). This definition is very focused on PETs and the research model is primarily looking at the antecedents of privacy literacy and the interrelations between the variables. For example, the results of the research indicate that online privacy concerns have a statistically significant positive effect on privacy literacy. However, due to a lack of a theoretical underlying we refrain from hypothesizing this relation since we argue that online privacy literacy is independent from IUIPC. Park (2013) investigates a closely related conceptualization of privacy literacy to OPLIS and the effect on corresponding behaviors in the digital sphere. The author finds that technical privacy knowledge, although very heterogenous amongst different demographic groups, has a positive correlation with users' ability to exert information control, i.e. decide about their personal information disclosure. OPLIS (Masur et al., 2017) was partially developed from skill items of the study by Park (2013) whereas the authors do not investigate OPLIS in a nomological network. "Social privacy literacy" as a sub-concept of privacy literacy for the case of social network is investigated in an article by Bartsch & Dienlin (2016). They find a positive effect of social privacy literacy on social privacy behavior. In summary, prior research suggests that privacy literacy might influence online behaviors positively in a way that individuals who are more literate behave in a more privacy-aware manner. However, privacy literacy is a context-independent variable comparable to IUIPC (Malhotra et al., 2004). Therefore, we argue that it behaves similar in its effects on the context-specific factors trusting beliefs, risk beliefs and trusting beliefs in Tor. As discussed before, previous research suggests that people with more privacy knowledge tend to be more aware about privacy threats (Bartsch & Dienlin, 2016), we argue that a higher level of online privacy literacy leads to less trust in online companies with respect to handling personal information. In contrast, risk beliefs will increase with a higher level of knowledge. Therefore, we hypothesize:

> Hypothesis 5 (H5): Online Privacy Literacy (OPLIS) has a negative effect on Trusting Beliefs (TB).
>
> Hypothesis 6 (H6): Online Privacy Literacy (OPLIS) has a positive effect on Risk Beliefs (RB).

The relationship of privacy literacy and trusting beliefs in Tor is not as clear as for hypotheses 5 and 6 because the OPLIS instrument does not contain any specific questions related to Tor. Thus, the assumption that trust in Tor is built upon the knowledge of certain specific features of Tor is difficult to make. However, since we asked active users of Tor, we argue that there is a certain level of trust in the service in place which is positively correlated with their relatively high knowledge related to privacy. We hypothesize this type of self-selection in hypothesis 7:

Hypothesis 7 (H7): Online Privacy Literacy (OPLIS) has a positive effect on the trusting beliefs in Tor (TB_{Tor}).

Trust is an important factor in the acceptance decision of users (Pavlou, 2003). McKnight, Carter, Thatcher, & Clay (2011) show that trust in a specific technology will positively affect individual's 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, Mcknight, & Tripp (2015). We hypothesize that:

Hypothesis 8 (H8): 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:

Hypothesis 9 (H9): Trusting beliefs (TB) have a negative effect on the behavioral intention to use Tor (BI).

Hypothesis 10 (H10): 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 & Ajzen (1975). Later research indicates a positive link between the two constructs (Sheppard, Hartwick, & Warshaw, 1988). Thus, we hypothesize that:

Hypothesis 11 (H11): The behavioral intention to use Tor (BI) has a positive effect on the actual use behavior (USE).

The resulting structural model is shown in Figure 1.

Insert Figure 1 About Here

Data Collection

The questionnaire constructs are adapted from the original IUIPC paper. The trust construct for trust in Tor is adapted from Pavlou (2003). Privacy literacy is operationalized with the online privacy literacy scale (OPLIS) (Masur et al., 2017). 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) (Schmitz, 2015). 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 past research which does not find a statistically significant differences across gender, income groups, educational levels, or political affiliation in the desire to protect one's privacy (Singh & Hill, 2003).

Descriptive Statistics and OPLIS Adaption

The descriptive statistics for our quantitative analysis can be found in Table 1. The OPLIS value is calculated as a relative value (i.e. ratio of correctly answered questions divided by total number of questions).

As already mentioned in Section 2.3, we had to adapt the OPLIS score. The original questionnaire aimed at the German population. Thus, it contains questions about German and European data protection laws. Since our sample consists of Tor users possibly spread from all over the world, it does not make sense to ask them for German or even European law. As a consequence, we omitted the respective questions about national laws. This is straight forward since we consider the ratio of correctly answered questions. For a comparison with the reference group (cf. Figure 2), we extrapolate our results from 15 to 20 questions.

It can be seen that on average participants answered 78.78% of the questions correctly (with a median of 0.8). It can be seen that the participants are highly privacy-sensitive (median values for collection, awareness and control range from 6 to 7). This view is reinforced by a relatively low median value for trusting beliefs in online companies and an above neutral median value for risk beliefs. Trusting beliefs in Tor are relatively high with a median of 5.6667 indicating that most participants agree that they trust Tor. The descriptive statistics for the three covariates show that participants have on average almost 7 years of experience with Tor and almost 18 years of internet experience. This insight combined with the high privacy literacy implies that the sample is relatively knowledgeable and experienced compared to the general population of internet users. A median value of 4 indicates that participants perceive to be a victim of privacy breaches "occasionally".

Insert Table 1 About Here

The distribution of the cumulative relative frequency for correctly answered privacy literacy questions is illustrated in Figure 2.

As discussed in Section 2, we extrapolate our results for Tor users in order to make it comparable to results of a representative German sample of regular Internet users (Masur et al., 2017). The distribution graph clearly shows that the Tor users are more literate with respect to online privacy compared to regular German internet users. For example, 60% of the participants in our sample answered 12 out of 15 questions correctly (i.e. 80% correctly answered questions). In contrast, roughly 60% of the regular internet users in the reference group answered 12 out of 20 questions correctly (i.e. 60%).

Insert Figure 2 About Here

Results

We tested the model using SmartPLS version 3.2.7 (Ringle, Wende, & Becker, 2015). 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.

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.

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 (Hair et al., 2017). Table 2 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 (Hair et al., 2017). In sum, ICR is established for our variables. Since IUIPC and USE are single-item constructs they have ICR values of 1.

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). Loadings above 0.7 imply that the indicators have much in common, which is desirable for reflective measurement models. Table 2 shows the outer loadings in bold on the diagonal. All loadings were higher than 0.7, except for TRUST4 with a value of 0.289. 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 (Hair et al., 2017). The diagonal values of Table 3 present the AVE of our constructs. All values are well above 0.5, demonstrating convergent validity.

Insert Table 2 About Here

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. Table 2 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) (Hair et al., 2017). Table 3 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.

Insert Table 3 About Here

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 (Henseler, Ringle, & Sarstedt, 2015). 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 (Hair et al., 2017). Values close to 1 for HTMT indicate a lack of discriminant validity. A conservative threshold is 0.85. Table 4 contains the values for HTMT and no value, except for the correlation between IUIPC and COLL (with 0.888), is above the 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.

Insert Table 4 About Here

Common method bias (CMB) can occur if data is gathered with a self-reported survey at one point in time in one questionnaire (Malhotra, Kim, & Patil, 2006). 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 (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003). 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. The test shows that eight factors have eigenvalues larger than 1 which account for 72.86% of the total variance. The first factor explains 26.76% of the total variance. Based on the results of previous literature (Blome & Paulraj, 2013), we argue that CMB is not likely to be an issue in the data set.

Assessment and Results of the Structural Model

To assess the structural model, we evaluate possible collinearity problems, path coefficients, the level of adjusted R^2, the effect size f^2, 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 (Hair et al., 2017).

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 1.380. Thus, collinearity is apparently not an issue.

Figure 3 shows the results of the path estimations and the adjusted R^2-values of the endogenous variables BI and USE. The adjusted R^2 is 0.412 for BI and 0.055 for USE. Thus, our model explains 41.2% of the variance of BI and 5.5% 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. (2011), 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 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 (Rosen, Whaling, Carrier, Cheever, & Rokkum, 2013), 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 3. 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 (Hair et al., 2017).

Insert Figure 3 About Here

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 0.588. The second newly added construct OPLIS has a statistically significant negative impact on trusting beliefs in online companies and a positive effect on trusting beliefs in Tor. The effect on risk beliefs is not statistically significant.

The results for the covariates experience with Tor, internet experience and privacy victim experience are not depicted in Figure 3 due to clarity reasons. The results with the respective significance level are shown in Table 5. The results indicate that experience with Tor has no immediate effect on the five context-specific variables. Internet experience has a slightly significant negative effect on risk beliefs implying that experienced internet users tend to associate less risk with online companies handling their personal data. Personal privacy victim experiences exert statistically significant effects on trusting beliefs, trusting beliefs in Tor, behavioral intention as well as on the actual use behavior. The results indicate that a higher number of negative past experiences with privacy breaches lead to less trust in online companies. The same negative effect is in place for trust in Tor. Apparently, Tor users in our sample are well aware about the technical limitations of the PET with respect to protecting their anonymity. Therefore, they do not blindly assume that they are completely protected when using Tor. There is even the possibility that certain privacy breaches occurred while using a PET. Interestingly, at the same time there are positive effects on BI and USE. Thus, the overall result of the relations between privacy victim experiences, trust in Tor and behavioral intention and actual use behavior are rather ambiguous.

Insert Table 5 About Here

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. The values are assessed based on thresholds by Cohen (1988), who defines effects as small, medium and large for values of 0.02, 0.15 and 0.35, respectively. Table 6 shows the results of the f^2 evaluation. Values in italics indicate small effects, values 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 in Tor have a large effect on the behavioral intention.

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. We used an omission distance d=7. Recommended values for d are between five and ten (Hair et al., 2011). 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. Values above 0 indicate that the model has the property of predictive relevance. In our case, the Q^2 value is equal to 0.306 for BI and 0.007 for USE. Since they are larger than zero, predictive relevance of the model is established.

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 (Hair et al., 2017). All individual values for q^2 are calculated with an omission distance d of seven. The results are shown in Table 6. The thresholds for the f^2 interpretation can be applied here, too. Values in italics indicate small effects, values in bold indicate medium effects and values in bold and italics indicate large effects. All other values have no substantial effect. As before, only the trusting beliefs in Tor have a medium-sized effect, implying the highest predictive power of all included exogenous variables. Risk beliefs have a small q^2 effect size.

Insert Table 6 About Here

Discussion

In this section, we interpret and summarize our findings of the statistical analysis, elaborate on limitations of our work and present future work opportunities.

Interpretation of the Results

Based on our results, all hypotheses except for H6, H9 and H10 can be confirmed (cf. Table 7). The results for H9 and H10 are surprising, considering that they are in contrast to the rationale explained in Section 3.1 and the results from previous literature (Malhotra et al., 2004). 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 and their privacy literacy. Thus, the results imply that users with a higher level of privacy concerns and privacy literacy rather tend to trust a PET.

Insert Table 7 About Here

Hypothesis 6 cannot be confirmed, too. As for H9 and H10, the effect is not statistically significant. The hypotheses for the effects of privacy literacy on the two other context-specific factors trusting beliefs and risk beliefs can only be confirmed for the negative effect of OPLIS on trusting beliefs (H5). Thus, users who are more literate with respect to privacy tend to trust online companies less regarding the handling of their personal information. The effect of OPLIS on risk beliefs is not statistically significant.

Limitations

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 124 participants is acceptable for our kind of statistical analysis 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. Third, we cannot rule out a non-response bias since especially in the privacy context people might not answer the questionnaire due to privacy concerns. Fourth, possible self-report biases (e.g. social desirability) might exist. We addressed these possible biases 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. Section 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. Lastly, our calculation of the OPLIS value is not based on all 20 questions of the original instrument since five questions are specific to law in the European Union. Thus, our results might not be comparable to the extent as we did in Figure 2. However, it is not possible to further break down the sample without the demographic information which we did not ask for mandatorily. Another limitation related to OPLIS concerns the validity of the instrument. OPLIS might have certain flaws since it is relatively new and not widely tested yet.

Future Work

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 would be required to include this relationship in such a research model. Furthermore, our work only investigates online literacy, especially online privacy literacy, in a specific context, i.e. with respect to the influence on specific variables and with respect to PETs. Thus, there is a lot of potential for future work to analyze this concept within different theories applied to different information systems. Interpreting privacy literacy as a kind of personal disposition might yield interesting results and might enable researchers to frame existing and new research questions based on another perspective. We also encourage building a more sophisticated model which not only includes privacy literacy but also closely related dimensions such as privacy awareness and the users' attitudes to investigate the users' intention and behavior.

Conclusions

In this paper, we contribute 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, general privacy literacy and the actual use behavior of Tor. By adapting and extending the IUIPC model by Malhotra et al. (2004), we could show that several of the assumptions for regular online services do not hold for PETs. Furthermore, we contribute to the practical work on PETs, especially Tor, by providing insights into factors influencing use intentions and behaviors of actual users. Trust in Tor is one of the major drivers of use intentions. Thus, companies or non-profits like 'The Tor Project' should focus on building a strong reputation and a trustful relationship with its users. We contribute to the literature on online literacy, by analyzing a relatively new instrument for measuring online privacy literacy (OPLIS) in two ways. First, our descriptive results of the OPLIS scores for Tor users indicate that they are more privacy literate than an average reference group of regular internet users (Masur et al., 2017). Second, we derived research hypotheses following the notion that online privacy literacy is similar to a personal disposition influencing the context-specific factors within the IUIPC model. Our results indicate that a higher level of online privacy literacy leads to less trust in online companies with respect to handling personal information. In contrast, more literate users tend to trust Tor to a larger extent. Thus, we argue that online privacy literacy is an important factor to consider when investigating relationships with privacy-related factors like concerns or risks.

References

Angst, C. M., & Agarwal, R. (2009). Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion. MIS Quarterly, 33(2), 339–370.

Bartsch, M., & Dienlin, T. (2016). Control your Facebook: An analysis of online privacy literacy. Computers in Human Behavior, 56, 147–154. https://doi.org/10.1016/j.chb.2015.11.022

Bédard, M. (2016). The underestimated economic benefits of the internet. In Regulation series, The Montreal Economic Institute.

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

Blome, C., & Paulraj, A. (2013). Ethical Climate and Purchasing Social Responsibility: A Benevolence Focus. Journal of Business Ethics, 116(3), 567–585. https://doi.org/10.1007/s10551-012-1481-5

Borking, J. J., & Raab, C. (2001). Laws, PETs and Other Technologies for Privacy Protection. Journal of Information, Law and Technology, 1, 1–14.

Brecht, F., Fabian, B., Kunz, S., & Mueller, S. (2011). Are You Willing to Wait Longer for Internet Privacy? In ECIS 2011 Proceedings. Retrieved from http://aisel.aisnet.org/ecis2011/236

Brecht, F., Fabian, B., Kunz, S., & Müller, S. (2012). Communication Anonymizers: Personality, Internet Privacy Literacy and Their Influence on Technology Acceptance. In ECIS 2012 Proceedings (pp. 1–13). Retrieved from http://aisel.aisnet.org/ecis2012/214

Cohen, J. (1988). Statistical Power Analysis for the Behavioral Sciences. HillsDale, NJ.

David, E. E., & Fano, R. M. (1965). Some thoughts about the social implications of accessible computing. In Proceedings 1965 Fall Joint Computer Conference.

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. European Journal of Social Psychology, 45(3), 285–297. https://doi.org/10.1002/ejsp.2049

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. Information Systems Research, 17(1), 61–80. https://doi.org/10.1287/isre.1060.0080

Fishbein, M., & Ajzen, I. (1975). Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research. Reading, MA: Addison-Wesley. https://doi.org/10.2307/2065853

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

Hair, J., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a Silver Bullet. The Journal of Marketing Theory and Practice, 19(2), 139–152. https://doi.org/10.2753/MTP1069-6679190202

Harborth, D., Cai, X., & Pape, S. (2019). Why Do People Pay for Privacy-Enhancing Technologies? The Case of Tor and JonDonym. In G. Dhillon, F. Karlsson, K. Hedström, & A. Zúquete (Eds.), ICT Systems Security and Privacy Protection. SEC 2019. IFIP Advances in Information and Communication Technology, vol 562 (pp. 253–267). Springer, Cham. https://doi.org/https://doi.org/10.1007/978-3-030-22312-0_18

Harborth, D., & Pape, S. (2018a). Examining Technology Use Factors of Privacy-Enhancing Technologies: The Role of Perceived Anonymity and Trust. In Twenty-fourth Americas Conference on Information Systems. New Orleans, USA.

Harborth, D., & Pape, S. (2018b). JonDonym Users' Information Privacy Concerns. In L. Janczewski & M. Kutyłowski (Eds.), ICT Systems Security and Privacy Protection. SEC 2018. IFIP Advances in Information and Communication Technology, vol 529 (pp. 170–184). Poznan, Poland: Springer, Cham. https://doi.org/https://doi.org/10.1007/978-3-319-99828-2_13

Harborth, D., & Pape, S. (2019). How Privacy Concerns and Trust and Risk Beliefs Influence Users' Intentions to Use Privacy-Enhancing Technologies - The Case of Tor. In Hawaii International Conference on System

Sciences (HICSS) Proceedings (pp. 4851–4860). Hawaii, US.

Heales, J., Cockcroft, S., & Trieu, V.-H. (2017). The influence of privacy, trust, and national culture on internet transactions. In G. Meiselwitz (Ed.), Social Computing and Social Media. Human Behavior (pp. 159–176). Springer International Publishing.

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. Journal of the Academy of Marketing Science, 43(1), 115–135. https://doi.org/10.1007/s11747-014-0403-8

Hoofnagle, C. J., King, J., Li, S., & Turow, J. (2010). How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies? https://repository.upenn.edu/asc_papers/399. https://doi.org/10.2139/ssrn.1589864

Joeckel, S., & Dogruel, L. (2019). Default effects in app selection: German adolescents' tendency to adhere to privacy or social relatedness features in smartphone apps. Mobile Media & Communication, 1–20. https://doi.org/10.1177/2050157918819616

JonDos Gmbh. (2018). Official Homepage of JonDonym. Retrieved January 16, 2018, from https://www.anonym-surfen.de

Kruger, J., & Dunning, D. (1999). Unskilled and Unaware of It: How Difficulties in Recognizing One's Own Incompetence Lead to Inflated Self-Assessments. Journal of Personality and Social Psychology, 77(6), 1121–1134. https://doi.org/10.1037/0022-3514.77.6.1121

Lankton, N. K., Mcknight, D. H., & Tripp, J. (2015). Technology, Humanness, and Trust: Rethinking Trust in Technology. Journal of the Association for Information Systems, 16(10), 880–918.

Lee, L., Fifield, D., Malkin, N., Iyer, G., Egelman, S., & Wagner, D. (2017). A Usability Evaluation of Tor Launcher. Proceedings on Privacy Enhancing Technologies, (3), 90–109. https://doi.org/10.1515/popets-2017-0030

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. Information Systems Research, 15(4), 336–355. https://doi.org/10.1287/isre.1040.0032

Malhotra, N. K., Kim, S. S., & Patil, A. (2006). Common Method Variance in IS Research: A Comparison of Alternative Approaches and a Reanalysis of Past Research. Management Science, 52(12), 1865–1883. https://doi.org/10.1287/mnsc.1060.0597

Masur, P. K., Teutsch, D., & Trepte, S. (2017). Entwicklung und Validierung der Online-Privatheitskompetenzskala (OPLIS) [Development and validation of the Online Privacy Literacy Scale (OPLIS)]. Diagnostica, 63(4), 256–268. https://doi.org/10.1026/0012-1924/a000179

McKnight, D. H., Carter, M., Thatcher, J. B., & Clay, P. F. (2011). Trust in a Specific Technology: An Investigation of Its Components and Measures. ACM Transactions on Management Information Systems (TMIS), 2(2), 1–25. https://doi.org/10.1145/1985347.1985353

Mineo, L. (2017). On internet privacy, be very afraid (Interview with Bruce Schneier). Retrieved February 20, 2018, from https://news.harvard.edu/gazette/story/2017/08/when-it-comes-to-internet-privacy-be-very-afraid-analyst-suggests/

Morrison, B. (2013). Do We Know What We Think We Know? An Exploration of Online Social Network Users' Privacy Literacy. Workplace Review, April 2013.

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

Park, Y. J. (2013). Digital Literacy and Privacy Behavior Online. Communication Research, 40(2), 215–236. https://doi.org/10.1177/0093650211418338

Pavlou, P. A. (2003). Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model. International Journal of Electronic Commerce, 7(3), 101–134. https://doi.org/10.1080/10864415.2003.11044275

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: a critical review of the literature and recommended remedies. Journal of Applied Psychology, 88(5), 879–903. https://doi.org/10.1037/0021-9010.88.5.879

Raber, F., & Krueger, A. (2017). Towards understanding the influence of personality on mobile app permission settings. In IFIP Conference on Human-Computer Interaction (pp. 62–82).

Ringle, C. M., Wende, S., & Becker, J. M. (2015). SmartPLS 3. Boenningstedt: SmartPLS GmbH, http://www.smartpls.com. Retrieved from http://www.smartpls.com

Rosen, L. D., Whaling, K., Carrier, L. M., Cheever, N. A., & Rokkum, J. (2013). The Media and Technology Usage and Attitudes Scale: An empirical investigation. Comput Human Behav., 29(6), 2501–2511. https://doi.org/10.1016/j.pestbp.2011.02.012.Investigations

Rossnagel, H. (2010). The market failure of anonymity services. Lecture Notes in Computer Science (Incl.

Subseries Lecture Notes in AI and Lecture Notes in Bioinformatics), 6033 LNCS, 340–354. https://doi.org/10.1007/978-3-642-12368-9_28

Schmitz, C. (2015). LimeSurvey Project Team. Retrieved from http://www.limesurvey.org

Sheppard, B. H., Hartwick, J., & Warshaw, P. R. (1988). The Theory of Reasoned Action: A Meta-Analysis of Past Research with Recommendations for Modifications and Future Research. Journal of Consumer Research, 15(3), 325–343.

Singh, T., & Hill, M. E. (2003). Consumer privacy and the Internet in Europe: a view from Germany. Journal of Consumer Marketing, 20(7), 634–651.

Slyke, C. V., Johnson, R., Jiang, J., & Shim, J. T. (2006). Concern for Information Privacy and Online Consumer Purchasing. Journal of the Association for Information Systems, 7(6), 415–444.

Smith, H. J., Dinev, T., & Xu, H. (2011). Theory and Review Information Privacy Research: An Interdisciplinary Review. MIS Quarterly, 35(4), 989–1015.

Straub, D., Boudreau, M. C., & Gefen, D. (2004). Validation Guidelines for IS Positivist Research. Communications of the Association for Information Systems, 13, 380–427.

The Tor Project. (2018). Tor. Retrieved February 20, 2018, from https://www.torproject.org

Trepte, S., & Masur, P. K. (2017). Privacy attitudes, perceptions, and behaviors of the German population. Forum Privatheit Und Selbstbestimmung in Der Digitalen Welt.

Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., & Lind, F. (2015). Do People Know About Privacy and Data Protection Strategies? Towards the “Online Privacy Literacy Scale” (OPLIS). In S. Gutwirth, R. Leenes, & P. de Hert (Eds.), Reforming European Data Protection Law (Vol. 20). Springer Netherlands. https://doi.org/10.1007/978-94-017-9385-8

Weinberger, M., Zhitomirsky-Geffet, M., & Bouhnik, D. (2017). Factors affecting users’ online privacy literacy among students in Israel. Online Information Review, 41(5), 582–597. https://doi.org/10.1108/OIR-05-2016-0127

About the Authors

David Harborth holds a Master's degree in Management with specialization in Finance and Information Management and a Bachelor's degree in Business Administration and Economics with specialization in Finance and Accounting from Goethe University Frankfurt. He worked for three years in the consulting industry in the strategy and financial services sector. David Harborth started to work at the Chair of Mobile Business & Multilateral Security as a research and teaching assistant in December 2015. His major areas of research are the socio-economic and technical issues related to privacy in Augmented Reality (AR), as well as user perceptions and business models for privacy-enhancing technologies (PETs). His research has appeared in conferences such as *International Symposium on Mixed and Augmented Reality (ISMAR), Hawaii International Conference on System Sciences (HICSS), European Conference on Information Systems (ECIS), Americas Conference on Information Systems (AMCIS), Wirtschaftsinformatik (WI)* and *IFIP SEC.*

Dr. Sebastian Pape Sebastian Pape is a senior researcher working at the Chair of Mobile Business & Multilateral Security at Goethe University Frankfurt. He successfully completed diplomas in mathematics (Dipl.-Math.) and computer science (Dipl.-Inform.) at Darmstadt University of Technology and holds a doctoral degree (Dr. rer. nat.) from the University of Kassel. From 2005 to 2011, he worked as research and teaching assistant at the Database Group (lead by Prof. Dr. Lutz Wegner) of the Department of Electrical Engineering and Computer Science of the University of Kassel. From 2011 to 2015, he was a senior researcher and teaching assistant at the Software Engineering for Critical Systems Group (lead by Prof. Dr. Jan Jürjens) of the Department of Computer Science Department of TU Dortmund University. From October 2014 to January 2015, he also was a visiting researcher (of Prof. Dr. Fabio Massacci) at the security group of the Department of Information Engineering and Computer Science of University of Trento. From 2018 to 2019 he was standing in as a professor at the Chair of Information Systems of the Faculty of Business, Economics and Management Information Systems at Regensburg University.

Appendix A - Distribution Channels of the Tor Online Survey

1. *Mailinglists:*

(a) tor-talk (https://lists.torproject.org/cgi-bin/mailman/listinfo/tor-talk/)
(b) liberationtech (https://mailman.stanford.edu/mailman/listinfo/liberationtech)
(c) IFIP TC 11 (https://dlist.server.uni- frankfurt.de/mailman/listinfo/ifip-tc11)
(d) FOSAD (http://www.sti.uniurb.it/events/fosad/)
(e) GI PET (http://mail.gi-fb-sicherheit.de/mailman/listinfo/pet)
(f) GI FBSEC (http://mail.gi-fb-sicherheit.de/mailman/listinfo/fbsec)

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, Off Topic (http://avengersdutyk3xf.onion/)
(b) The Hub, Beginners (http://thehub7xbw4dc5r2.onion)
(c) Onion Land, Off Topic (http://onionlandbakyt3j.onion)
(d) 8chan, /tech/ (http://oxwugzccvk3dk6tj.onion)
(e) IntelExchange, Unverified Users (http://rrcc5uuudhh4oz3c.onion)
(f) Code Green, Discussions (http://pyl7a4ccwgpxm6rd.onion)
(g) Changolia, overchan.random (http://jewsdid.oniichanylo2tsi4.onion)
(h) Atlayo, Posting (http://atlayofke5rqhsma.onion/)

5. *Personal Announcements at Workshops*

Appendix 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. (reverse-scored item)

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. I'm 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)
Please choose your usage frequency for Tor (the frequency scale is adapted from Rosen et al. (2013)):
1. Never
2. Once a month
3. Several times a month
4. Once a week
5. Several times a week
6. Once a day
7. Several times a day
8. Once an hour
9. Several times an hour
10. All the time

Internet Experience (in years)
1. How many years of experience do you have with computers?

Answer options range from 0 years to “more than 20 years”.

Experience with Tor (in years)
1. How many years are you using Tor?

Answer options range from 0 years to “more than 20 years”.

Privacy Victim Experience
1. How frequently have you personally been the victim of what you felt was an improper invasion of privacy?

Item measured with a seven-point frequency scale (“Never”, “Very infrequently”, “Infrequently”, “Occasionally”, “Sometimes”, “Frequently”, “Very frequently”).

Online Privacy Literacy Scale (OPLIS)
Part 1: Knowledge about institutional practices
1. The National Security Agency (NSA) accesses only public user data, which are visible for anyone. (True/**false**/don’t know)
2. Social network site operators (e.g. Facebook) also collect and process information about non-users of the social network site. (**True**/false/don’t know)
3. User data that are collected by social network site operators (e.g. Facebook) are deleted after five years. (True/**false**/don’t know)
4. Companies combine users’ data traces collected from different websites to create user profiles. (**True**/false/don’t know)
5. E-mails are commonly passed over several computers before they reach the actual receiver. (**True**/false/don’t know)

Part 2: Knowledge about technical aspects of data protection (correct answers randomized)
1. What does the term “browsing history” stand for? In the browsing history...
   A. ...the URLs of visited websites are stored.
   B. ...cookies from visited websites are stored.
   C. ...potentially infected websites are stored separately.
   D. ...different information about the user are stored, depending on the browser type.
2. What is a “cookie”?
   A. A text file that enables websites to recognize a user when revisiting.
   B. A program to disable data collection from online operators.
   C. A computer virus that can be transferred after connecting to a website.
   D. A browser plugin that ensures safe online surfing.

3. What does the term “cache” mean?
    A. A buffer memory that accelerates surfing on the Internet.
    B. A program that specifically collects information about an Internet user and passes them on to third parties.
    C. A program, that copies data on an external hard drive to protect against data theft.
    D. A browser plugin that encrypts data transfer when surfing online.
4. What is a “trojan”? A trojan is a computer program, that...
    A. ...is disguised as a useful application, but fulfills another function in the background.
    B. ...protects a computer from viruses and other malware.
    C. ... was developed for fun an d has no specific function.
    D. ... caused damage as computer virus in the 90ies but doesn’t exist anymore.
5. What is a “firewall”?
    A. A fallback system that will protect the computer from unwanted web attacks.
    B. An outdated protection program against computer viruses.
    C. A browser plugin that ensures safe online surfing.
    D. A new technical development that prevents data loss in case of a short circuit.

Part 3: Knowledge about data protection strategies

1. Tracking of one’s own internet is made more difficult if one deletes browser information (e.g. cookies, cache, browser history) regularly. (**True**/false/don’t know)
2. Surfing in the private browsing mode can prevent the reconstruction of your surfing behavior, because no browser information is stored. (**True**/false/don’t know)
3. Using false names or pseudonyms can make it difficult to identify someone on the Internet. (**True**/false/don’t know)
4. Even though It-experts can crack difficult passwords, it is more sensible to use a combination of letters, numbers and signs as passwords than words, names or simple combinations of numbers. (**True**/false/don’t know)
5. In order to prevent the access to personal data, one should use various passwords and user names for different online applications and change them frequently. (**True**/false/don’t know)

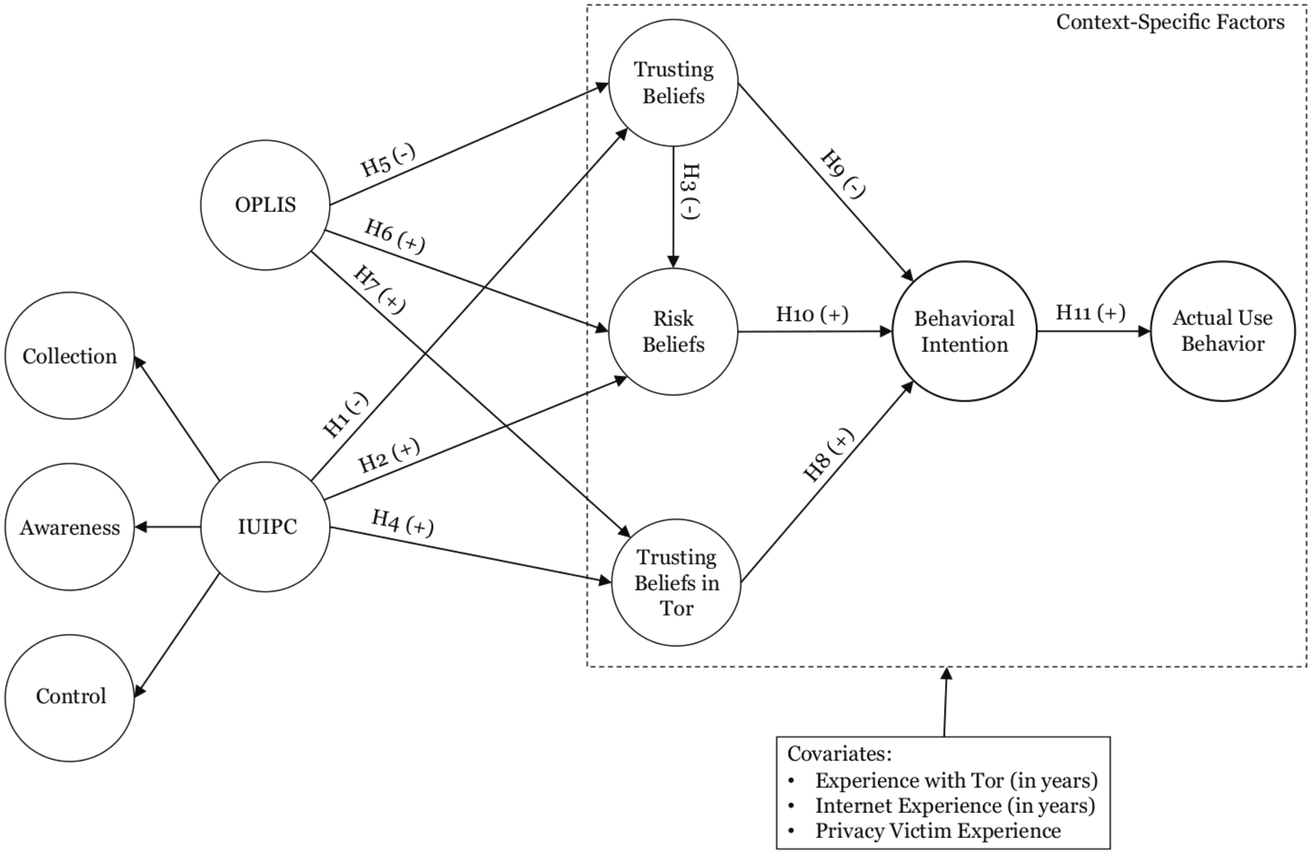

Figure 1. Research Model

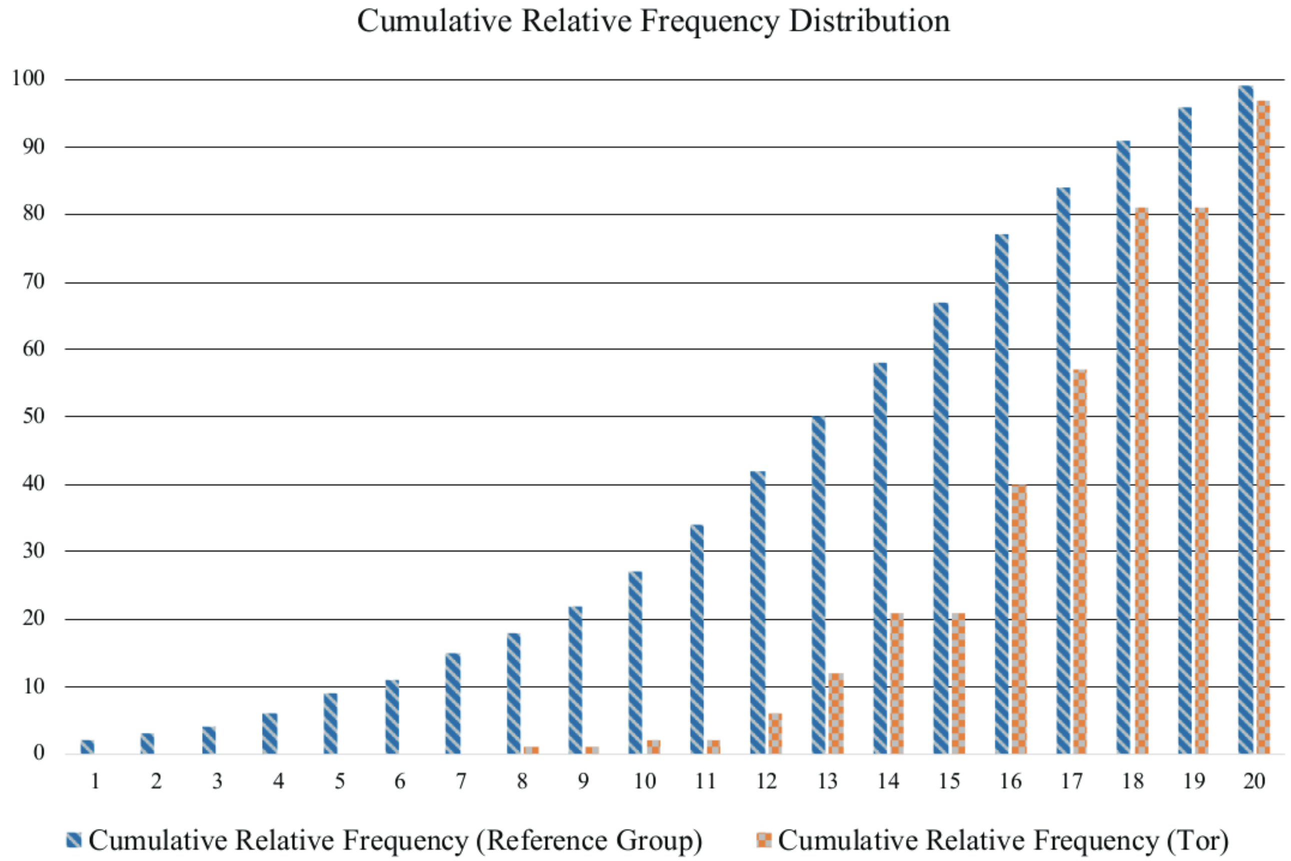

Figure 2. Differences in the Distributions between the Cumulative Relative Frequency of Correctly Answered OPLIS Questions between the Reference Group (Masur et al., 2017) and the Tor Users in our Sample

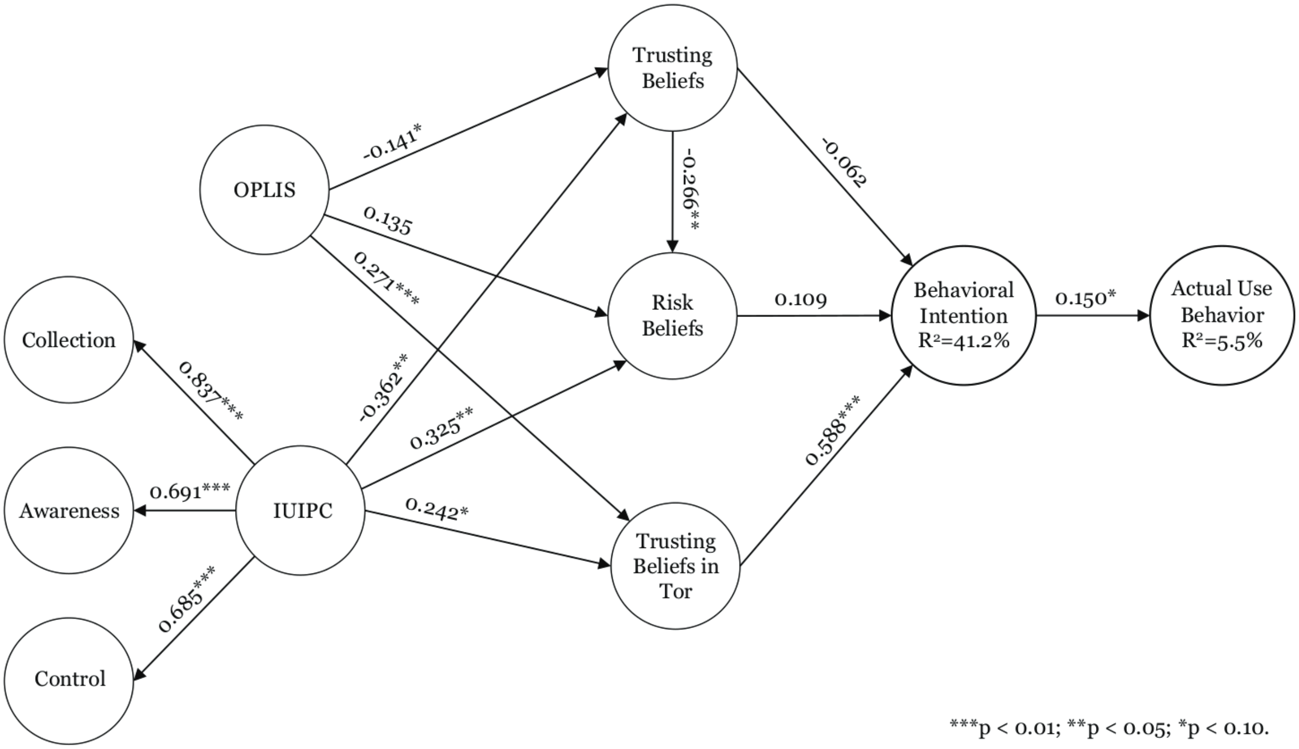

Figure 3. Path Estimates and Adjusted R^2 Values of the Structural Model

Table 1. Descriptive Statistics for the Used Variables (cf. Appendix A2 for Measurement Scales of the Constructs)

Statistics					
Variable	**Mean**	**Median**	**Min.**	**Max.**	**Std. Dev.**
OPLIS (relative)	0.7876	0.8	0.3333	1	0.1259
Collection	6.3810	6.5	4	7	0.7053
Awareness	6.5457	7	1	7	0.7500
Control	5.9435	6	1	7	1.0038
Trusting Beliefs	2.2694	2.2	1	5.8	0.9429
Risk Beliefs	5.3242	5.5	1.6	7	1.1048
Trusting Beliefs in Tor	5.3548	5.6667	1	7	1.1892
Behavioral Intention	5.7043	6	1	7	1.2971
Actual Use Behavior	4.0726	5	0	9	2.6692
Experience with Tor	6.8710	6	0	20	4.6416
Internet Experience	17.7984	21	2	21	5.0429
Privacy Victim Experience	4.2742	4	1	7	1.6297

Table 2. Loadings and Cross-Loadings of the Reflective Items and Internal Consistency Reliability

Construct	**AWA**	**Control**	**COLL**	**RB**	**TB**	**$\text{Trust}_{\text{Tor}}$**	**BI**
AWA1	**0.911**	0.234	0.302	0.222	-0.136	0.066	0.201
AWA2	**0.923**	0.230	0.219	0.136	-0.153	0.072	0.197
AWA3	**0.891**	0.323	0.315	0.220	-0.102	0.066	0.249
CONTROL1	0.095	**0.825**	0.271	0.107	-0.163	0.137	0.214
CONTROL2	0.405	**0.821**	0.226	0.245	-0.149	0.132	0.237
CONTROL3	0.174	**0.756**	0.438	0.214	-0.340	0.098	0.098
COLL1	0.264	0.358	**0.888**	0.546	-0.462	0.176	0.301
COLL2	0.206	0.332	**0.812**	0.204	-0.337	0.232	0.374
COLL3	0.292	0.359	**0.906**	0.443	-0.442	0.272	0.375
COLL4	0.304	0.309	**0.850**	0.466	-0.399	0.182	0.317
RISK1	0.196	0.200	0.487	**0.879**	-0.446	0.217	0.258
RISK2	0.170	0.160	0.326	**0.832**	-0.292	0.156	0.233
RISK3	0.155	0.252	0.364	**0.861**	-0.346	0.233	0.221
RISK4	0.245	0.231	0.374	**0.826**	-0.255	0.257	0.327
RISK5	-0.105	-0.145	-0.427	**-0.700**	0.396	-0.003	-0.144
TRUST1	-0.149	-0.261	-0.455	-0.417	**0.894**	-0.097	-0.265
TRUST2	-0.118	-0.186	-0.410	-0.376	**0.890**	-0.033	-0.195
TRUST3	-0.107	-0.339	-0.397	-0.396	**0.768**	-0.131	-0.153
TRUST5	-0.069	-0.009	-0.219	-0.069	**0.682**	-0.109	-0.166
$\text{TRUST}_{\text{Tor}}1$	0.064	0.149	0.257	0.159	-0.091	**0.880**	0.559
$\text{TRUST}_{\text{Tor}}2$	0.077	0.121	0.236	0.244	-0.124	**0.924**	0.552
$\text{TRUST}_{\text{Tor}}3$	0.059	0.138	0.169	0.179	-0.078	**0.883**	0.486
BI1	0.236	0.240	0.355	0.228	-0.252	0.586	**0.858**
BI2	0.262	0.202	0.322	0.318	-0.149	0.465	**0.864**
BI3	0.143	0.158	0.363	0.233	-0.231	0.522	**0.926**
Cronbach's α	0.894	0.722	0.887	0.567	0.831	0.877	0.859
Comp. Reliability	0.934	0.843	0.922	0.817	0.885	0.924	0.914

Table 3. Discriminant Validity with AVEs and Construct Correlations

Constructs (AVE)	AWA	BI	COLL	Control	IUIPC	OPLIS	RB	TB	Trust$_{\text{Tor}}$	USE
AWA (0.825)	0.908									
BI (0.780)	0.239	0.883								
COLL (0.748)	0.309	0.394	0.865							
Control (0.642)	0.291	0.226	0.393	0.801						
IUIPC (1.000)	0.691	0.403	0.837	0.685	1.000					
OPLIS (1.000)	-0.071	0.143	0.111	0.110	0.071	1.000				
RB (0.675)	0.214	0.290	0.485	0.243	0.450	0.198	0.822			
TB (0.662)	-0.142	-0.242	-0.476	-0.276	-0.426	-0.155	-0.426	0.813		
Trust$_{\text{Tor}}$ (0.803)	0.075	0.597	0.249	0.152	0.226	0.300	0.217	-0.110	0.896	
USE (1.000)	-0.128	0.177	0.073	0.008	-0.009	0.006	0.010	-0.058	-0.026	1.000

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

Table 4. Heterotrait-Monotrait Ratio (HTMT)

Constructs	**AWA**	**BI**	**COLL**	**Control**	**IUIPC**	**OPLIS**	**RB**	**TB**	**Trust$_{Tor}$**
BI	0.274								
COLL	0.343	0.452							
Control	0.346	0.290	0.486						
IUIPC	0.728	0.436	0.888	0.798					
OPLIS	0.075	0.155	0.119	0.127	0.071				
RB	0.238	0.337	0.541	0.294	0.478	0.212			
TB	0.159	0.278	0.528	0.336	0.439	0.171	0.449		
Trust$_{Tor}$	0.084	0.681	0.280	0.192	0.240	0.318	0.244	0.131	
USE	0.138	0.186	0.077	0.060	0.009	0.006	0.021	0.058	0.029

Table 5. Covariate Results (Significance Levels: ***p < 0.01; **p < 0.05; *p < 0.10)

Context-specific factors Covariate	TB	RB	TB_{Tor}	BI	USE
Experience with Tor	-0.047	-0.008	-0.012	0.092	-0.074
Internet experience	-0.001	-0.139*	0.003	0.016	0.065
Privacy victim experience	-0.245**	0.011	-0.163*	0.196**	0.225**

Table 6. f^2 and q^2 Effect Size Assessment Values

Variables	**f^2**	**q^2**
Endogenous Exogenous	BI	BI
TB	0.005	0.000
RB	0.016	*0.072*
TB_{Tor}	***0.567***	**0.334**

Table 7. 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	Online Privacy Literacy (OPLIS) has a negative effect on Trusting Beliefs (TB)	√
H6	Online Privacy Literacy (OPLIS) has a positive effect on Risk Beliefs (RB)	×
H7	Online Privacy Literacy (OPLIS) has a positive effect on the trusting beliefs in Tor (TB_{Tor})	√
H8	Trusting beliefs in Tor (TB_{Tor}) have a positive effect on the behavioral intention to use Tor (BI)	√
H9	Trusting beliefs (TB) have a negative effect on the behavioral intention to use Tor (BI)	×
H10	Risk beliefs (RB) have a positive effect on the behavioral intention to use Tor (BI)	×
H11	The behavioral intention to use Tor (BI) has a positive effect on the actual use behavior (USE)	√