Acceptance Factors of Privacy-Enhancing Technologies on the Basis of Tor and JonDonym

Sebastian Pape and David Harborth

1 Introduction and Background

Bruce Schneier states [49]: "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." One of the reasons for the surveillance of users is a rising economic interest in the Internet [3]. However, users are not helpless and can make use of privacy-enhancing technologies (PETs) to protect them. Examples of PETs include services that allow anonymous communication, such as Tor [68] or JonDonym [40].

Tor and JonDonym are low-latency anonymity services that redirect packets in a certain way to hide metadata (the sender's and optionally—in case of a hidden service—the receiver's Internet protocol (ip) address) from passive network observers. While Tor and JonDonym differ technically, they are highly comparable with respect to the general technical structure and the use cases. Tor offers an adapted browser including the Tor client for using the Tor network, the "Tor Browser." Similarly, the "JonDoBrowser" includes the JonDo client for using the JonDonym network.

However, the entities who operate the PETs are different. Tor is operated by a non-profit organization with thousands of voluntarily operated servers (relays) and an estimated 2 million daily users by the Tor Project [68] and an estimated 8 million daily users by Mani et al. [46]. Tor is free to use with the option that users can donate to the Tor project. JonDonym is run by a commercial company with servers (mix cascades) operated by independent and non-interrelated organizations or private individuals who all publish their identity. A limited service is available

S. Pape (✉) · D. Harborth
Chair of Mobile Business and Multilateral Security, Goethe University Frankfurt, Frankfurt, Germany
e-mail: sebastian.pape@m-chair.de; david.harborth@m-chair.de

N. Gerber et al. (eds.), *Human Factors in Privacy Research*,
https://doi.org/10.1007/978-3-031-28643-8_15

for free, and different premium rates allow to overcome the limitations. The actual number of users is not known since the service does not keep track of this. While the number of users of anonymization services is large enough to conduct studies and evaluate the running systems, it is quite low compared to the number of Internet users in total, which was estimated to 4.13 billion in 2019 [7]. Far less than 1% of the users use anonymization networks.

In order to investigate why there is not a broader adoption of anonymization services, some user research seems to be necessary: Investigating users' privacy concerns and their technology acceptance to find factors promoting the use of PETs. Since Tor is one of the most prominent PETs, the hope is that the insights can also be transferred to other PETs.

Besides the users' perspective, it is also important to investigate the economic side: Are users willing to pay for PETs and which incentives and hindrances exist for companies to implement PETs?

For PETs such as anonymization networks such as Tor [68] or JonDonym [40] that allow anonymous communication, there has been a lot of research [50, 64], but the large majority of it is of technical nature and does not consider the users and their perceptions. However, the number of users is essential for anonymization networks since an increasing number of (active) users also increases the anonymity set. The anonymity set is the set of all possible subjects who might be related to an action [58], and thus, a larger anonymity set may make it more difficult for an attacker to identify the sender or receiver of a message. Therefore, it is crucial to understand the reasons for the users' intention to use a PET or obstacles preventing it [1].

However, for the propagation of a PET, it is not only important to understand the users' intentions to use the PET, but also the users' willingness to pay for the service, which would allow companies to build a business model upon the provision of the service. The main challenge in motivating the user to pay for PET, i. e., an anonymization service, is that the user can barely notice a working PET directly. Noticing an anonymization network is in most cases the result of a limitation of throughput, performance, or response time. Indirect effects such as fewer profiling are also hard to detect, but even harder to connect to the PET in place. This makes it hard for a company as well as the user to sell or, respectively, understand the advantages for these types of PETs. As a consequence, it is hard for a company to come up with a business model, and thus the further distribution of PETs is prevented [52].

Therefore, besides investigating the users' intention to use a PET on the basis of Tor in Sect. 3.1 and JonDonym in Sect. 3.2, we also investigate in Sect. 3.4 the economic sides from the perspective of the users' willingness to pay for Tor or JonDonym and in Sect. 3.5 from the perspective of a business owner to provide a PET in general as service.

2 Methodology

In this section, we first describe how the questionnaire was built and how the data were collected and evaluated (cf. Sects. 2.1–2.3). In the second part, we briefly sketch how we conducted and evaluated experts' interviews (cf. Sects. 2.4 and 2.5).

2.1 Questionnaire Composition

To investigate the users intention to use Tor or JonDonym, we made use of two different popular structural equation [19] models:

Internet Users' Information Privacy Concerns (IUIPC) is a construct by Malhotra et al. [45] for measuring and explaining privacy concerns of online users that is embedded in a larger nomological net with other privacy-related variables. IUIPC is operationalized as a second-order construct[1] of the sub-constructs collection, awareness, and control (please refer also to the chapter "Toward Valid and Reliable Privacy Concern Scales: The Example of IUIPC-8" for a detailed discussion of the IUIPC). That means the user's concerns are determined by concerns about data on the user in relation to the value or received benefits, by concerns about the control users have over their own data, and by concerns about his or her awareness regarding organizational privacy practices. The privacy concerns then influence trusting beliefs and risk beliefs that in turn influence the user's behavior. The use behavior was the release of personal information to a marketing service provider in the original research. The trusting and risk beliefs refer to the users' perceptions about the behavior of online firms (in general) to protect or lose the users' personal information.

The IUIPC construct has been used in various contexts, such as Internet of Things [51], Internet transactions [39], and mobile apps [59]. Furthermore, it has recently been re-evaluated in several studies [54, 55]. But so far it had not been applied to a PET such as an anonymization service. There is a major difference between PETs and other services, i. e., apps [30, 35, 53] or games [24, 33] regarding the application of the IUIPC instrument. The other services had a certain use for their customer (primary use), and the users' privacy concerns were investigated for the use of the service. The concepts of trusting and risk beliefs matched that in a way that they were referring to "general companies" that may provide a service to the user based on data they receive. However, for anonymization services, providing privacy is the primary purpose. Therefore, it is necessary to distinguish between trusting and risk beliefs with respect to technologies that aim to protect personal data (PETs) and regular Internet

[1] For an extensive discussion on second-order constructs, see Steward [66].

services. As a consequence, the trust model within IUIPC's causal model was extended by trusting beliefs in Tor/JonDonym.

Technology Acceptance Model (TAM) was developed by Davis [9, 10] based on the the theory of reasoned action (TRA) by Fishbein and Ajzen [12] and the theory of planned behavior (TPB) by Ajzen [2] (see also the chapter "From the Privacy Calculus to Crossing the Rubicon: An Introduction to Theoretical Models of User Privacy Behavior"). According to the TRA, a person's behavioral intention determines that person's behavior. The behavioral intention itself is influenced by the person's subjective norms and attitude toward the behavior. The subjective norms refer to a person's normative beliefs and normative pressure to perform or not perform the behavior. The attitude relies on the person's beliefs about the behavior and its consequences. TPB is an extension of the TRA with the same overall structural process: the behavioral intention is influenced by several components and influences the behavior. However, the TPB adds perceived behavioral control that refers to a person's perception regarding the ease or difficulty of performing a given behavior in a given situation.

2.2 Questionnaire Data Collection

We conducted a *survey among users of the anonymization services JonDonym and Tor*. For both surveys, we conducted the study with German- and English-speaking users. Thus, we administered two questionnaires for each service. All items for the German questionnaire had to be translated into German since all of the constructs are adapted from the English literature [26, 27]. To ensure content validity of the translation, we followed a rigorous translation process [23, 24]. 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 of the questionnaire was then translated back to English by a second independent certified translator. 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.

Since we investigate the effects of privacy concerns, trust and risk beliefs on the use of JonDonym and Tor, we collected data of actual users of the PET. We installed the surveys on a university server. For JonDonym, the links to the surveys were distributed with the beta version of the JonDonym browser and published on the official JonDonym homepage. For Tor, the links to the English and German version were distributed over multiple channels on the Internet (cf. [29, Appendix A]). Surprisingly, although there are approximately two million active Tor users, it was more difficult to gather the necessary number of complete answers for a valid and reliable quantitative analysis for Tor users. After deleting all incomplete sets and sets from participants who answered a test question in the middle of the survey incorrectly, 124 usable data sets remained for Tor [29] and 141 usable data sets

remained for JonDonym [28] for our analysis. The questionnaires and the answers to Likert scale questions are available online [31, 32].

For both services, the demographic questions were not mandatory. 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 [65]. However, other studies also showed that technological knowledge is not equally distributed in different age groups [17, 53], and users with a better education are more likely to use PETs [60]. In the end, our decision is a trade-off between the ability to take demographic effects in consideration and the chance to have highly privacy-aware participants who might have aborted answering the questionnaire (or lied) if demographic questions had been mandatory.

2.3 Questionnaire Evaluation

We made use of a mixed method approach consisting of quantitative and qualitative methods. We start by describing the quantitative methods and then describe the qualitative part.

Quantitative Methods

We applied a standard statistical analysis approach called *structural equation modeling* (SEM) to assess our research model and the corresponding hypotheses regarding the cause–effect relationships among these constructs. SEM can reveal how much of the variance in the dependent variables (effects) can be explained by the independent variables (causes). There are two main approaches for SEM, namely covariance-based SEM (CB-SEM) and partial least squares SEM (PLS-SEM). Since our research goal is to predict the dependent variables (effects) *behavioral intention* and *actual use behavior* of PETs and maximize the explained variance for these dependent variables, we use PLS-SEM [19] for our analysis (Hair et al. extensively discuss on the use of PLS-SEM [18]). For that purpose, we first built our models for IUIPC-10 [28, 29, 34] and TAM [25, 37, 38] based on the existing literature. We then tested our model using SmartPLS [63]. To assess the quality of all different models, we investigated the structural model (e.g., possible collinearity problems) and the measurement model (internal consistency reliability, convergent validity, and discriminant validity). For all of the models, the structural model and the measurement model were consistent and checks were fine for reliability and validity on both data sets. For details, we refer to the respective papers [25, 28, 29, 34, 37, 38].

Since JonDonym and Tor are different with respect to the pricing schemes and the organizational structure of the providers, we are interested whether there are significant differences in the hypothesized relationships between the variables. To compare JonDonym and Tor users in the TAM, we split the data set into two parts and analyzed the results for Tor and JonDonym separately. For that, we conducted a *multigroup analysis* in SmartPLS and tested whether there are statistically significant differences for each of the hypotheses.

As a last step, we conducted a *logistic regression* [21] to find out which factors influence users' willingness to pay for privacy (in our case willingness to pay for JonDonym and willingness to donate to Tor). We used the logistics regression to build the model because our dependent variable is a binary variable. A linear regression is not an appropriate model here due to the violation of the assumption that the dependent variable (WTP) is continuous, with errors that are normally distributed [48]. Willingness to pay for JonDonym is defined as the binary classification of JonDonym users' actual behavior. The regression was conducted with the open-source statistic software R.

We use a less conservative level of statistical significance of 10% here since the p value is sensitive to the relatively small sample sizes when comparing results for Tor and JonDonym. Thus, we provide this level of statistical significance in this analysis to indicate potential statistically significant differences between the effects for Tor and JonDonym. In addition, the oftentimes referenced statistical significance level of 5% only indicates a "convenient" threshold for judging statistical significance [13] and can be considered a rule of thumb.

Qualitative Methods

The questionnaire contained four open questions from which we aimed to get deeper insights into certain aspects of the quantitative analysis described above. We asked if users have any concerns, which additional features they would like, and why they would (not) recommend JonDonym or Tor. JonDonym users were additionally asked under which circumstances they would choose one of the premium tariffs. Two researchers analyzed the statements independently from each other and abstracted the individual answers to codes. Codes summarize the data and present different dimensions of a concept. For example, we find that *usability* is an important concept for both technologies. However, the results indicate that the code *usability* can be found with a negative as well with a positive characteristic depending on the user and the respective context (e. g., users praising or complaining about the usability of the PETs depending on what they intend to achieve).

Altogether 626 statements were collected. The coding was done in two stages, following a method from sociology [6, 16], which comprises two or three coding phases, namely initial coding, axial coding, and focused coding. We only used initial and focused coding since this level of structuring is sufficient for our data [6]. First, we initially coded each of the statements. These initial codes in itself provide a sorting and structuring for the data. Initial codes represent topics that occur

frequently in the data, i. e., topics often mentioned by participants. In our case, we decided to name these codes "Subconcepts" in our results since they already provide one level of abstraction. After the initial coding phase, we compared the different codings of the researchers and discussed the individual codes. Thereby, we agreed upon certain subconcepts that were similar or the same but expressed differently by the coders. In a next step, we calculated the intercoder reliability. We did not use a common codebook or a predefined set of codes to do the initial coding. Therefore, the known reliability measures such as Cohen's Kappa [8] are not usable for our case since these measures are relying on predefined categories. Consequently, we used a very simple calculation in order to provide a reliability measure dividing the number of equally coded statements by the total number of statements to be coded. We had 226 matches for Tor and 242 matches for JonDonym, which yield intercoder reliabilities of 68.69% and 81.48%, respectively, for the total number of statements for each PET. Thus, the intercoder reliability is equal to 74.76% for both PETs. These numbers are relatively large considering that we coded independently from each other without agreeing to fixed subconcepts beforehand. We also counted the incidents in which one of the coders had at least one more code assigned to a statement than the other coder in order to provide more transparency of our coding process. This happened 52 times (coder 1 had 29 times more codes, coder 2 had 23 times more codes) for Tor and 44 times for JonDonym (coder 1 had 27 times more codes, coder 2 had 17 times more codes). These instances are counted toward the mismatches in the intercoder reliability measures. In the second step, we structured the most occurring themes in these initial codes and came up with the focused codes. We name these codes "Concepts" and find that users primarily make statements about either technical issues, their beliefs and perceptions, or economic issues.

2.4 Interview Data Collection

For the *interviews of privacy experts*, we designed a semi-structured interview guide that we used to conduct the interviews. Semi-structured in this context means that the interview is significantly influenced by the respondent's interaction and answers. The questionnaire only records particularly relevant questions that definitely need to be addressed from the researcher's point of view. This has the advantage of being able to obtain the deepest possible insights and most detailed answers from the participant. The questionnaire can be divided into three main topics. First, general questions about the person and the company are asked. This is followed by questions about privacy and PETs. The second part covers technical questions about the status quo and possible future developments. The third part covers economic and societal issues. We interviewed experts and professionals who are involved with privacy-enhancing technologies (PETs) in their companies or in whose products or services privacy plays a special role. The experts are from companies that directly offer PETs or in which privacy plays an important role in the value proposition. Examples include the telecommunications sector, payment providers, or eCommerce solution

providers. We conducted and analyzed ten interviews, varying in duration from 44 to 180 min. The demographic information can be found in our respective article [20].

2.5 Interview Evaluation

The *expert interviews* were all recorded and then transcribed word for word. The transcripts were then analyzed using what is known as open coding and selective coding [6, 16, 67]. Open coding is the first step of data analysis and is closely oriented to the data (the transcripts). In the next step, codes are summarized and abstracted (selective coding). These steps are performed separately for each interview and then between interviews. This so-called comparative method [6, 16, 67] is an elementary component of the qualitative research methodology. By constantly comparing across interviews, we derived abstract categories from the data that provide a diverse picture of incentives and disincentives. These coding steps were performed by two authors to identify and resolve any discrepancies in the analysis of the data.

3 Results

We first present the results for the two different structural equation models based on IUIPC (cf. Sect. 3.1) and TAM (cf. Sect. 3.2). Then, we briefly discuss the evaluation of the open questions (cf. Sect. 3.3). Besides users' concerns and factors influencing their technology use acceptance, it is also important to consider factors for a successful business model built on a PET. For that purpose, we additionally investigated the users' willingness to pay or donate for a PET (cf. Sect. 3.4) and also considered the perspective of companies by investigating their incentives and hindrances to implement PETs (cf. Sect. 3.5).

3.1 Internet Users Information Privacy Concerns

The basic idea of investigating users' privacy concerns was to learn how they influence users' behavioral intention to use the service. Figure 1 shows the SEM for JonDonym users and Fig. 2 for Tor users. The models for JonDonym and Tor users turned out to be very similar. Most of the relations were as expected, somewhat surprising was the result that general trusting and risk belief had no significant effect on the use behavior. However, for the rather small effect sizes, it might be that the sample size was simply not large enough to show a significant relationship. In any case, the trust in JonDonym or Tor had by far a larger influence on the use behavior, respectively, the behavioral intention. The result shows that the reputation of being

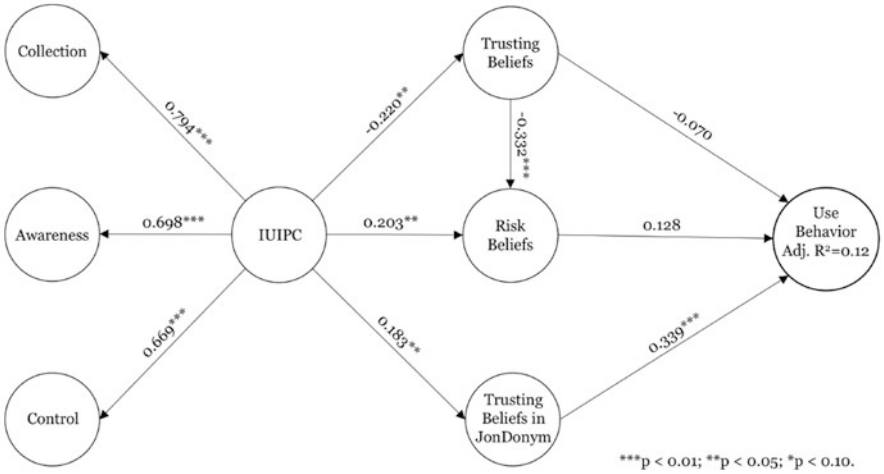

Fig. 1 JonDonym users, IUIPC, path estimates, and adjusted R^2 values of the structural model [28]

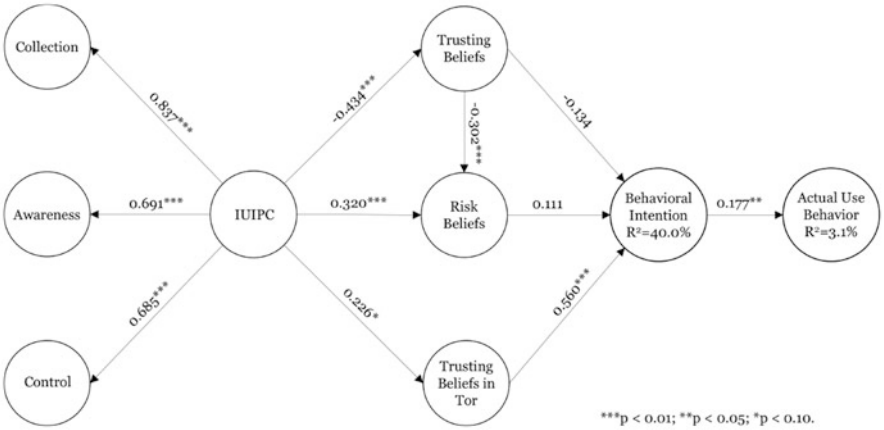

Fig. 2 Tor users, IUIPC, path estimates, and adjusted R^2 values of the structural model, figure taken from Harborth and Pape [29] licensed under CC BY-NC-ND 4.0

a trustworthy provider, respectively, service, is crucial for an anonymization service provider. The results also show that users with a higher level of privacy concerns rather tend to trust their anonymization service provider, which might be affected by the fact that we only asked users of the respective PET.

In general, if there is a reliable measure of the use behavior, it is a better indicator than the users' behavioral intention to use a service. Since we questioned actual users, we could use their use frequency of the services. However, the results indicate

that the influence of the behavioral intention on the actual use behavior was rather small for Tor users.

Users' attitudes and behavioral intention can differ from the decisions they make. This phenomenon is often denoted as the "privacy paradox" [15]. Two possible explanations come to mind to explain the privacy paradox: (i) users balance between potential risks and benefits they gain from the service (privacy calculus) [11] and (ii) users are concerned but lack knowledge to react in a way that would reflect their needs [69]. However, since we surveyed active users of Tor, both argumentations do not fit. Regarding the privacy paradox, we have already discussed how PETs differ from regular Internet services. Regarding the lack of knowledge, users have already installed the PET and use it. However, it is still important to investigate the users' capabilities since users need a certain amount of knowledge in order to adequately evaluate the given level of privacy [57, 69]. For that purpose, we added the users' privacy literacy measured with the *Online Privacy Literacy Scale* (OPLIS) [47] to the model. For that purpose, we slightly adapted the original questionnaire since it aimed at the German population and contains questions about German and European data protection laws. With our sample of Tor users possibly spread from all over the world, it does not make sense to ask them for German or even European privacy laws. As a consequence, we omitted the respective questions about national laws, and we extrapolated our results from 15 to 20 questions for a comparison with the reference group [34]. The results showed that users' privacy literacy positively influences trusting beliefs in Tor (cf. Fig. 3). Therefore, educating users and increasing their privacy literacy should add to the behavioral intention of using Tor. Built on our work, Lux and Platzer [44] investigated the relation between

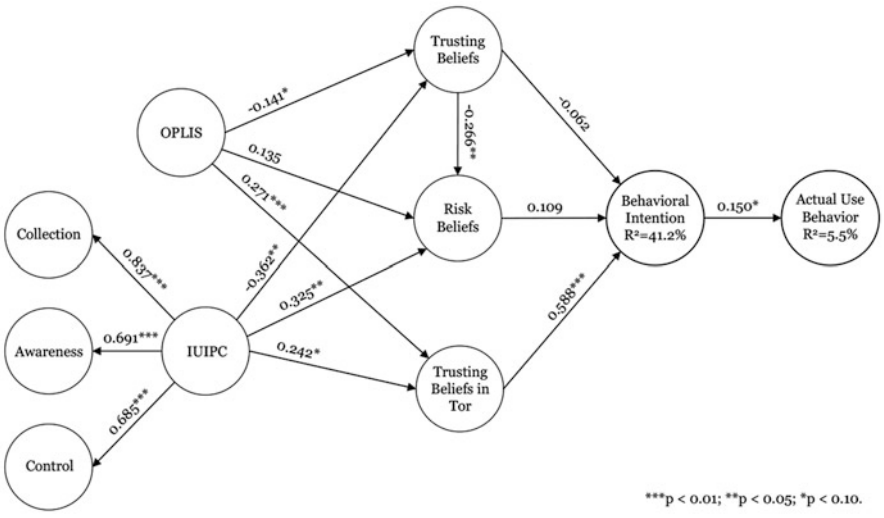

Fig. 3 Tor users, IUIPC and OPLIS, path estimates, and adjusted R^2 values of the structural model [34]

online privacy literacy and the usage of Tor in more detail following our approach to use only 15 items and to extrapolate the result. We will further investigate the influence of the behavioral intention on the actual use behavior by making use of the TAM model in the next subsection.

3.2 Technology Acceptance Model

Within the same survey, we also asked the participants about certain constructs we could use in a TAM model [27]: How they perceived the usefulness, the ease of use, and the anonymity of the PET. Since we had already identified trust in the PET as a major driver for the behavioral intention, we included it too. The resulting model is shown in Fig. 4 including JonDonym and Tor users [37].

The model shows significant relationships for all paths as already known from the TAM model with three noteworthy observations:

- There are three main drivers of the PETs' perceived usefulness: perceived anonymity, trust, and perceived ease of use that explain almost two-thirds of its variance. This demonstrates that for PETs the two newly added variables perceived anonymity and trust in the PETs can be important antecedents in technology acceptance models for PETs.
- Similar than in the IUIPC model, trust in the PET is the most important factor for behavioral intention. This underlines the importance of trust in the PETs as

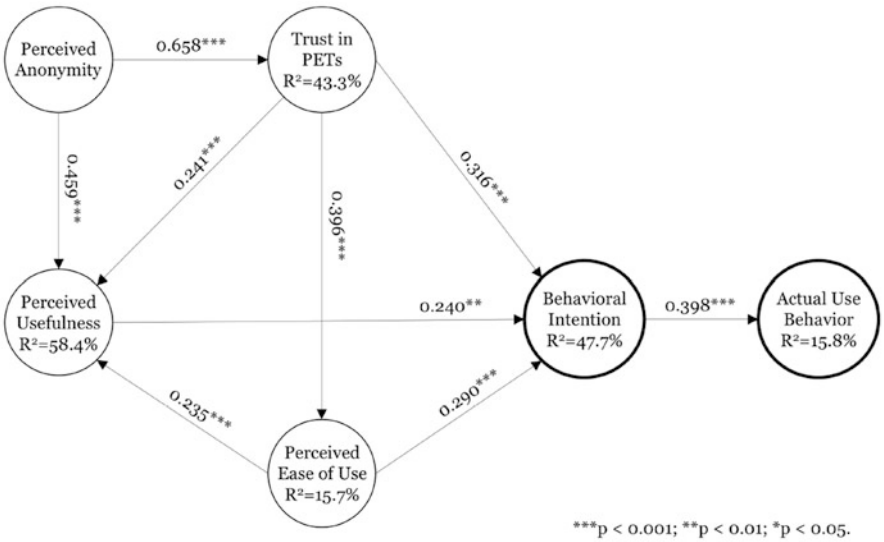

Fig. 4 TAM-based research model with path estimates and R^2 values of the structural model for PETs, figure taken from Harborth et al. [37] licensed under CC BY-NC-ND 3.0

a highly relevant concept when determining the drivers of users' use behavior of PETs.

- Since the effects of perceived anonymity and trust in the PETs on behavioral intention and actual use behavior were partially indirect, we calculated the total effects. All of the effects were highly statistically significant (p value <0.001), and the total effects on behavioral intention are relatively large (PA → BI: 0.446; Trust_{PETs} → BI: 0.511), while the effects on the actual use are as expected smaller (PA → USE: 0.177; Trust_{PETs} → USE: 0.203).

To investigate the differences between JonDonym and Tor and also to further investigate the small effect of behavioral intention on actual use behavior, we conducted a multigroup analysis to test whether there are statistically significant differences between JonDonym and Tor users as shown in Table 1. The table also shows the path coefficients for both PETs individually.

These results indicate that the most significant difference between JonDonym and Tor users was the effect size between behavioral intention and actual use, which is 0.679 for JonDonym and 0.179 for Tor. Less significant observations were that the effects of trust on behavioral intention and perceived anonymity on perceived usefulness were slightly larger for JonDonym users. A possible explanation could be the structure of the two services, as JonDonym is a profit-oriented company that charges for the unlimited use of the PET [40], while Tor is a community-driven project based on donations.

Table 1 Results of the MGA analysis (gray background indicates statistical significance at least at the 10% level) [37]

	Original path coefficient		P values		Path coefficient difference	P value
Relationships	JonDonym	Tor	JonDonym	Tor	JonDonym vs Tor	
PA → Trust_{PETs}	0.597	0.709	<0.001	<0.001	0.112	0.865
PA → PU	0.543	0.369	<0.001	<0.001	0.174	0.088
Trust_{PETs} → BI	0.416	0.232	<0.001	0.010	0.184	0.064
Trust_{PETs} → PU	0.173	0.304	0.035	0.008	0.131	0.823
Trust_{PETs} → PEOU	0.378	0.431	<0.001	<0.001	0.053	0.657
PU → BI	0.183	0.300	0.046	0.002	0.117	0.805
PEOU → BI	0.206	0.371	0.011	<0.001	0.165	0.929
PEOU → PU	0.182	0.300	0.039	<0.001	0.118	0.830
BI → USE	0.679	0.179	<0.001	0.029	0.500	<0.001

BI behavioral Intention, *PEOU* perceived ease of use, *PA* perceived anonymity, *USE* actual use frequency, *PU* perceived usefulness

3.3 Evaluation of Open Questions

To gather some reasons for the observed differences and possibly identify other differences of the services from a user perspective, we included five open questions in the survey. The results of their coding are shown in Table 2. In the left column, we have the three concepts technical issues, beliefs and perceptions, and economical issues. Each of them includes several subconcepts. The results were then clustered into statements common to both PETs, such as feature requests (**Tor.1**, **Jon.1**), statements only referring to Tor, such as statements about malicious exit nodes (**Tor.2**), and statements only referring to JonDonym, such as concerns about the location of mix cascades (**Jon.2**). For each statement, we selected at least one quote shown at the bottom of the table.

The result for user perceptions shows that both services differ not that much with respect to technical issues but in the users' beliefs. Unsurprisingly, economical issues were only concerning JonDonym. Three main differences might be able to explain the observed different effect sizes in the structural equation model. As already discussed, trust models between the services were different in the way that for JonDonym, users have to trust a company (**Jon.13**), while Tor users have to trust their community (**Tor.12**). While the concept for both technologies is that the users' anonymity does not rely on a single malicious server, there is still trust necessary since only a minority of the users will inspect the programs they are running. For JonDonym users, the size of the user base was also an issue (**Jon.11**). However, the most interesting observation also in terms of explaining the weak effect of behavioral intention on actual use behavior for Tor users was that many Tor users were concerned about looking like a criminal (**Tor.13**, **Tor.14**).

3.4 Customers' Willingness to Pay or Donate

Within the same survey as already described in the previous subsection, we also asked JonDonym users about their recent tariff and Tor users if they ever have donated to Tor [21]. It showed that the majority of users was not willing to pay or donate for the services: 85 out of 141 users (60%) used JonDonym's free tariff and 93 out of 124 (75%) Tor users have never donated to Tor.

For JonDonym, we also compared the users' preferences for certain tariff structures depending on factors such as data volume, pricing, and contract duration. We were comparing users' preferences toward existing tariffs: a high-data-volume tariff, a low-price tariff, and a low-anonymity tariff and two newly created tariffs adding a lower data volume than the low-price tariff and a higher volume than the high-data-volume tariff. Free users were neutral to all tariffs but showed a slight preference to the newly created low-traffic tariff. Already paying users preferred the existing and newly created high-data-volume tariffs over the others. This indicates that free users would prefer the cheapest tariff if they decide to pay at all. This

Table 2 Results of the coding for the open questions including quotes [37]

Concepts	Subconcepts	Common to both PETs	Specific Subconcepts for Tor	Specific Subconcepts for JonDonym
Technical Issues	PET design	Feature Requests (**Tor.1**, **Jon.1**)	Malicious exit nodes (**Tor.2**)	Location of mix cascades (**Jon.2**)
	Compatibility	Accessibility of websites (**Tor.3**, **Jon.3**)		
	Usability	Documentation (**Tor.4**, **Jon.4**) Ease of use (**Tor.5**, **Jon.5**) Missing knowledge to use it correctly (**Tor.6**,**Jon.6**)		
	Performance	Latency (**Tor.7**, **Jon.7**, **Jon.8**)		
Beliefs and Perceptions	Anonymity	Concerns about deanonymization (**Tor.8**, **Jon.9**) Reason of use (**Tor.9**, **Jon.10**)		Size of the user base (**Jon.11**)
	Consequences	Fear of investigations (**Tor.10**, **Tor.11**, **Jon.12**)	Beliefs about social effects (**Tor.13**, **Tor.14**)	
	Trust		Trust in the community (**Tor.12**)	Trust in technology (**Jon.13**)
	Substitute technologies	Best available tool (**Tor.15**, **Jon.14**)		Tor as reference technology (**Jon.3**, **Jon.8**, **Jon.11**)
Economical Issues	Costs			Lower costs, other pricing schemes (**Jon.15**)
	Payment methods			Easy, anonymous payment options (**Jon.15**)
	Use cases		Circumvent Censorship (**Tor.16**)	Willingness to pay in certain scenarios (**Jon.16**, **Jon.17**)

Tor.1 *TCP support for name resolution via Tor's DNSPort [. . .]*
Tor.2 *Many exit nodes are run by governmental intelligence organizations. Exit notes can collect unencrypted data.*
Tor.3 *It can't be used on all websites; therefore it is of limited use to me*
Tor.4 *Easy to understand instructions for users with different levels of knowledge.*
Tor.5 *Tor protects privacy while on the web and is easy to use.*
Tor.6 *An unexperienced user may not understand the technical limitations of Tor and end up losing [. . .] privacy.*
Tor.7 *Increased latency makes the experience painful at times*
Tor.8 *It may fail to provide the expected level of anonymity because of attacks which may not even be known at the time they are performed (or commonplace).*
Tor.9 *It is a key component to maintaining one's privacy when browsing on the Internet.*
Tor.10 *Tor usage "Stands out"*
Tor.11 *[. . .] having a cop boot at my door because of Tor.*
Tor.12 *An end user needs to trust the network, the persons running Tor nodes and correct implementations [. . .]*
Tor.13 *Only social backlash from people thinking that Tor is mostly used for illegal activities.*
Tor.14 *For the same reason I don't hang out in brothels, using Tor makes you look like a criminal*
Tor.15 *While not perfect, Tor is the best option for reliable low-latency anonymization*
Tor.16 *It can be used as a proxy / VPN to get past censorship*
Jon.1 *Larger number of Mix Cascades, more recent software, i.e. pre-configured browser, faster security updates*
Jon.2 *First and last server of the mix cascade should not be located in the same country*
Jon.3 *Unlike Tor, JonDonym is not blocked by some websites. (Google for example among others)*
Jon.4 *Clearer explanations and instructions for JonDoFox*
Jon.5 *Easy to use, outside the mainstream like i.e. Tor*
Jon.6 *Privacy is less than expected because of wrong configuration settings.*
Jon.7 *[. . .] Even if it is quite slow without a premium tariff*
Jon.8 *[. . .] sometimes it's a little bit to slow, but compared with Tor...*
Jon.9 *Defeat of your systems by government agencies.*
Jon.10 *It provides a minimum level of personal data protection and online safety.*
Jon.11 *Tor is better due to having a much larger user base. More users results in greater anonymity*
Jon.12 *By using the service, am I automatically marked by intelligence authorities as a potential terrorist, supporter of terrorist organizations, user [. . .] for illegal things?*
Jon.13 *How can I trust JonDonym? How can JonDonym proof that servers are trustworthy?*
Jon.14 *It appeared to be the least worst option for anonymization when I researched anonymization services*
Jon.15 *Fair pricing, pre-paid is an easy payment option.*
Jon.16 *For use it in a country where it's difficult surf the net*
Jon.17 *If I would use the computer for work-related tasks*

suggests that providers of PETs should offer tariffs with a low monetary barrier to convert free users into paying users. However, even with a low monetary barrier, there would still be the need to resolve the payment barrier, which regularly shows in e-commerce when customers are abandoning their shopping cart before the payment process [61].

We also built a regression model to identify significant factors contributing to the willingness to pay. For that purpose, we defined a binary classifier for the willingness to pay (JonDonym), being 0 if the respondent was using a free tariff and being 1 if the respondent was using a premium tariff. Analogous, we defined the willingness to donate (Tor), being 0 if the respondent has never donated and being 1 if the respondent has donated at least once. As independent variables, we considered risk propensity (RP), frequency of improper invasion of privacy (VIC), trusting beliefs in online companies (TRUST), trusting beliefs in JonDonym ($TRUST_{PET}$), and knowing of Tor / JonDonym (TOR/JD) and derived the following research model:

$$\begin{aligned} WTP/WTD_i = \beta_0 + \beta_1 \cdot RP_i + \beta_2 \cdot VIC_i + \beta_3 \cdot TRUST_i \\ + \beta_4 \cdot TRUST_{PET,i} + \beta_5 \cdot TOR/JD_i + \epsilon_i. \end{aligned}$$

The results are shown in Table 3, and one more time indicates that trust in the PET is the prevalent factor. On a highly significant level, the regression model suggests that a one unit increase in trust results in a roughly 12% higher likelihood that users choose a premium tariff (JonDonym) or donate (Tor). Besides that, the only significant variables were risk propensity for JonDonym and past privacy victim experiences for Tor. Surprisingly, risk propensity had a negative coefficient, indicating that more risk-averse users are less likely to choose a premium tariff for JonDonym. This contradicts previous findings [14] that risk aversion can act as a driver to protect an individual's privacy. For Tor, bad experiences with privacy breaches lead to a higher probability of donating money, even though on a more marginal level of roughly 5% per unit.

Table 3 Results of the logistic regression model for users' willingness to pay/donate [21]

	WTP for JonDonym		WTD for Tor		
	Coeff	Avg. marg. effects	Coeff	Avg. marg. effects	Difference
(Intercept)	−0.0376	−0.0081	6.1455***	−0.9768	0.9687
RP	−0.4967**	−0.1067	−0.1492	−0.0237	−0.083
VIC	−0.0397	−0.0085	0.3352**	0.0533	−0.0618
TRUST	−0.0868	−0.0187	−0.1222	−0.0194	0.0007
$TRUST_{PET}$	0.5661***	0.1217	0.7835***	0.1245	−0.0028
TOR/JD	−0.5792	−0.1245	0.488	0.0776	−0.2021

*$p < 0.1$, **$p < 0.01$, ***$p < 0.001$

3.5 Companies' Incentives and Hindrances to Implement PETs

Equally important to the user perspective for the broad distribution of PETs is the perspective of the companies since users can only order services if they are offered. Therefore, we investigated the incentives and hindrances of companies to implement PETs either in their existing products or as a stand-alone product.

For that purpose, we conducted semi-structured interviews with 12 experts and managers from companies dealing with privacy and PETs in their daily business [20]. Our interview guide consisted of three relevant parts about general questions on the interviewees and their companies, technical questions on the status quo, and questions on economic and societal issues. The interviews were recorded, transcribed, openly coded, and in a second round selectively coded. The selective coding was done first separately and then among all interviews to consolidate the developed codings [6, 16]. We identified the following categories:

Technical Optimization: PETs help to optimize the company within an organization and technical dimension and can get the company a technological lead. For that purpose, the *integration into the business process* was named as a necessary condition, and it was criticized that it is in general hard to get information about the practical use of PETs. PETs were also seen as a tool for *data management and avoidance* to improve business processes.

Business model: The category considering business models was by far the largest. Here, the interviewees saw the largest incentives but also the largest hindrances. With the implementation of PETs, companies intend to *further develop their services*. How and if that works depends on the customers' requirements, on the level of convenience for the existing service (if it depends on customer data) as well as on the PET's handling. Customers' awareness of privacy was also seen as an important factor. However, the interviewees were discordant if raising it should be the task of the company. PETs were also seen as a chance to *enlarge the company's clientele* by addressing "nerds." The mass market was seen from the viewpoint that most customers do not request PETs but would accept them and that there is a chance to implement PETs in existing products that are already widespread. Interviewees also did not agree on the *development of new business models* in terms of offering privacy as a premium feature. While some considered it as naturally to ask for a fee for the additional effort on the company's side, others questioned that approach by referring to the perception of the "non-premium" customers that they do not have sufficient security and privacy levels when using the company's service. As a last incentive, a better *positioning for the future* was named, which could gain the company an advantage over its competitors.

Corporate perception: The particular technology was considered to be less important, but a positive perception by business partners was considered to be highly useful to gain *trust*. Using PETs to have a communicable unique selling point enables the company to *profile itself through PETs*. *Business ethics* was considered from multiple viewpoints. Based on the assumption that anonymity

and the use of PETs are independent of moral value positions, the question was raised if informative awareness campaigns are morally defensible or a way of using the customer's fear to sell them PETs. On the other hand, it was advocated for integrating PETs independently of the economic value but rather because it seems to be the right thing to do.

Our results do not draw a clear picture in some areas since the perceptions differ a lot, i. e., on the question if privacy can be sold to the customers as a premium service. This shows that more research is necessary to determine underlying factors and elaborate precise recommendations to companies on how they can integrate PETs in their products while having a proper business model in mind.

4 Discussion and Conclusion

Our results indicate that for models based on IUIPC the traditional influence of trusting and risk beliefs is overruled by trust in the respective PET. With the newly introduced constructs perceived anonymity and trust in the PET, technology acceptance models are applicable for PETs also. Most of the existing variables in the TAM were also found in the participants' statements (e. g., usability, performance, anonymity, and trust). Trust in the PET also plays a major role when it comes to paying for or donating to the service. For companies, the introduction of PETs offers a huge chance but also rises challenges, in particular about a profitable business model. However, our results can only be a first insight into issues of hindering a broader adoption of PETs, where more details have to be brought to light in future work.

Future work could also investigate PETs that are integrated into regular services, e. g., the use of machine learning to help users with the privacy preferences [42], integration of PETs into physical services such as payment and shipment for e-commerce [56], or the integration of PETs into the Internet infrastructure eliminating the users' effort to set up PETs themselves [22]. However, this would raise additional challenges as it needs to be clearly investigated if users refer to the PET part of the service or the traditional part. Moreover, as already discussed in the introduction, an ideal PET would be barely noticeable, which would raise questions regarding suitable business models and the opportunity to "sell" privacy as a feature. It has also been shown that if users are aware that a tool should protect their privacy, they are getting biased and tend toward being more concerned about potential privacy issues of the tool than for non-privacy tools [4, 5]. Further problems of integrating PETs into existing services are that, on the one hand, it is hard to decide which of the many PETs is the best choice [43, 62] and that, on the other hand, it is hardly possible to ask the users about their preferences since in most cases the users do not notice the main achievement of the PET to protect their privacy, but rather things such as increased latency, more complex processes, or similar side effects.

While the adding of online privacy literacy did not improve the explanatory power of the model a lot, research in other areas such as the Corona Warning App [36, 53] (please refer to the chapter "Privacy Research on the Pulse of Time: COVID-19 Contact-Tracing Apps" for an overview of research in this area) or inferences of voice recordings [41] suggests that knowledge and awareness play a fundamental role in the users' perception. Thus, in this case, the used OPLIS construct might not have been specific enough to relate the users' knowledge with their concerns and behavior.

Summing up, while there has been lots of progress on the cryptographic side and the technical implementation of PETs, there is still a gap concerning the understanding of factors influencing users to use PETs. From a company perspective, it is equally important to address the question on how to embed which PET in a service and which business model supports a monetization strategy of this privacy feature.

Acknowledgments This work was supported by the European Union's Horizon 2020 research and innovation program from the project CyberSec4Europe (grant agreement number 830929).

References

1. Abu-Salma, R., Sasse, M. A., Bonneau, J., Danilova, A., Naiakshina, A., & Smith, M. (2017). Obstacles to the adoption of secure communication tools. In *IEEE security & privacy* (pp. 137–153).
2. Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179–211.
3. Bédard, M. (2016). The underestimated economic benefits of the Internet. Regulation series, The Montreal Economic Institute. Economic Notes.
4. Bracamonte, V., Pape, S., & Kiyomoto, S. (2021). Investigating user intention to use a privacy sensitive information detection tool. In *Symposium on Cryptography and Information Security (SCIS)*.
5. Bracamonte, V., Pape, S., & Löbner, S. (2022). "All apps do this": Comparing privacy concerns towards privacy tools and non-privacy tools for social media content. *Proceedings on Privacy Enhancing Technologies (PoPETs), 2022*(3), 57–78.
6. Charmaz, K. (2014). *Constructing grounded theory* (2nd ed.) Sage Publications.
7. Clement, J. (2020). Number of Internet users worldwide 2005–2019. https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/
8. Cohen, J. (1968). Weighted kappa: Nominal scale agreement provision for scaled disagreement or partial credit.
9. Davis, F. D. (1985). *A technology acceptance model for empirically testing new end-user information systems: Theory and results*. Massachusetts Institute of Technology.
10. Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319–340.
11. Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17*(1), 61–80.
12. Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention and behavior: An introduction to theory and research*. Addison-Wesley.
13. Fisher, R. A. (1970). *Statistical methods for research workers* (14th ed.). Oliver & Boyd.

14. Frik, A., & Gaudeul, A. (2016). The relation between privacy protection and risk attitudes, with a new experimental method to elicit the implicit monetary value of privacy. *CEGE Discussion Papers, Number*.
15. Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security, 77*, 226–261.
16. Glaser, B. G., & Strauss, A. L. (1967). *The discovery of grounded theory*. Aldine Publishing.
17. Graeff, T. R., & Harmon, S. (2002). Collecting and using personal data: Consumers' awareness and concerns. *Journal of Consumer Marketing, 19*(4), 302–318.
18. 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.
19. Hair, J., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing Theory and Practice, 19*(2), 139–152.
20. Harborth, D., Braun, M., Grosz, A., Pape, S., & Rannenberg, K. (2018). Anreize und Hemmnisse für die Implementierung von Privacy-Enhancing Technologies im Unternehmenskontext. In *Sicherheit 2018: Sicherheit, Schutz und Zuverlässigkeit, Beiträge der 9. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI), 25.-27. April 2018, Konstanz* (pp. 29–41).
21. Harborth, D., Cai, X., & Pape, S. (2019). Why do people pay for privacy-enhancing technologies? The case of Tor and JonDonym? In *ICT Systems Security and Privacy Protection—34th IFIP TC 11 International Conference, SEC 2019, Lisbon, Portugal, June 25–27, 2019, Proceedings* (pp. 253–267).
22. Harborth, D., Herrmann, D., Köpsell, S., Pape, S., Roth, C., Federrath, H., Kesdogan, D., & Rannenberg, K. (2017). Integrating privacy-enhancing technologies into the Internet infrastructure. https://arxiv.org/abs/1711.07220. Also available via https://epub.uni-regensburg.de/36346/
23. Harborth, D., & Pape, S. (2017). Exploring the hype: Investigating technology acceptance factors of Pokémon GO. In W. Broll, H. Regenbrecht, & J. E. Swan II (Eds.), *2017 IEEE International Symposium on Mixed and Augmented Reality, ISMAR 2017, Nantes, France, October 9–13, 2017* (pp. 155–168).
24. Harborth, D., & Pape, S. (2017). Privacy concerns and behavior of Pokémon GO players in Germany. In M. Hansen, E. Kosta, I. Nai-Fovino, & S. Fischer-Hübner (Eds.), *Privacy and Identity Management. The Smart Revolution—12th IFIP WG 9.2, 9.5, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Ispra, Italy, September 4–8, 2017, Revised Selected Papers*, volume 526 of *IFIP Advances in Information and Communication Technology* (pp. 314–329). Springer.
25. Harborth, D., & Pape, S. (2018). Examining technology use factors of privacy-enhancing technologies: The role of perceived anonymity and trust. In *24th Americas Conference on Information Systems, AMCIS 2018, New Orleans, LA, USA, August 16–18, 2018*. Association for Information Systems.
26. Harborth, D., & Pape, S. (2018). German translation of the concerns for information privacy (CFIP) construct. Technical report, SSRN.
27. Harborth, D., & Pape, S. (2018). German translation of the unified theory of acceptance and use of technology 2 (UTAUT2) questionnaire. Technical report, SSRN.
28. Harborth, D., & Pape, S. (2018). JonDonym users' information privacy concerns. In *ICT Systems Security and Privacy Protection—33rd IFIP TC 11 International Conference, SEC 2018, Held at the 24th IFIP World Computer Congress, WCC 2018, Poznan, Poland, September 18–20, 2018, Proceedings* (pp. 170–184).
29. 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 *52nd Hawaii International Conference on System Sciences (HICSS) 2019* (pp. 4851–4860).
30. Harborth, D., & Pape, S. (2019). Investigating privacy concerns related to mobile augmented reality applications. In H. Krcmar, J. Fedorowicz, W. F. Boh, J. M. Leimeister, & S. Wattal (Eds.), *Proceedings of the 40th International Conference on Information Systems ICIS 2019, Munich, Germany, December 13–15, 2019*.

31. Harborth, D., & Pape, S. (2020). Dataset on actual users of the privacy-enhancing technology JonDonym.
32. Harborth, D., & Pape, S. (2020). Dataset on actual users of the privacy-enhancing technology Tor.
33. Harborth, D., & Pape, S. (2020). Empirically investigating extraneous influences on the "APCO" model—childhood brand nostalgia and the positivity bias. *Future Internet, 12*(12), 220.
34. Harborth, D., & Pape, S. (2020). How privacy concerns, trust and risk beliefs and privacy literacy influence users' intentions to use privacy-enhancing technologies—the case of Tor. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 51*(1), 51–69.
35. Harborth, D., & Pape, S. (2021). Investigating privacy concerns related to mobile augmented reality apps—a vignette based online experiment. *Computers in Human Behavior, 122*, 106833.
36. Harborth, D., & Pape, S. (2022). A privacy calculus model for contact tracing apps: Analyzing the German corona-Warn-App. In *ICT Systems Security and Privacy Protection—37th IFIP TC 11 International Conference, SEC 2022*, volume 648 of *IFIP Advances in Information and Communication Technology* (pp. 3–19).
37. Harborth, D., Pape, S., & Rannenberg, K. (2020). Explaining the technology use behavior of privacy-enhancing technologies: The case of Tor and JonDonym. *Proceedings on Privacy Enhancing Technologies (PoPETs), 2020*(2), 111–128.
38. Harborth, D., Pape, S., & Rannenberg, K. (2021). Explaining the technology use behavior of privacy-enhancing technologies: The case of Tor and JonDonym (poster). In *17th Symposium on Usable Privacy and Security (SOUPS 2021)*.
39. 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.
40. JonDos Gmbh. (2018). Official Homepage of JonDonym. https://www.anonym-surfen.de
41. Kröger, J. L., Gellrich, L., Pape, S., Brause, S. R., & Ullrich, S. (2022). Personal information inference from voice recordings: User awareness and privacy concerns. *Proceedings on Privacy Enhancing Technologies (PoPETs), 2022*(1), 6–27.
42. Löbner, S., Tesfay, W. B., Nakamura, T., & Pape, S. (2021). Explainable machine learning for default privacy setting prediction. *IEEE Access, 9*, 63700–63717.
43. Löbner, S., Tronnier, F., Pape, S., & Rannenberg, K. (2021). Comparison of de-identification techniques for privacy preserving data analysis in vehicular data sharing. In B. Brücher, C. Krauß, M. Fritz, H. Hof, & O. Wasenmüller (Eds.), *CSCS '21: ACM Computer Science in Cars Symposium, Ingolstadt, Germany, November 30th, 2021* (pp. 7:1–7:11). ACM.
44. Lux, A., & Platzer, F. (2022). Online-Privatheitskompetenz und Möglichkeiten der technischen Umsetzung mit dem Anonymisierungsnetzwerk Tor. In *Selbstbestimmung, Privatheit und Datenschutz* (pp. 129–149). Springer Vieweg.
45. 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.
46. Mani, A., Wilson-Brown, T., Jansen, R., Johnson, A., & Sherr, M. (2018). Understanding Tor usage with privacy-preserving measurement. In *2018 Internet Measurement Conference (IMC'18)* (pp. 1–13).
47. Masur, P. K., Teutsch, D., & Trepte, S. (2017). Entwicklung und Validierung der Online-Privatheitskompetenzskala (OPLIS). *Diagnostica*.
48. McKelvey, R. D., & Zavoina, W. (1975). A statistical model for the analysis of ordinal level dependent variables. *Journal of Mathematical Sociology, 4*(1), 103–120.
49. Mineo, L. (2017). 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/
50. Montieri, A., Ciuonzo, D., Aceto, G., & Pescapé, A. (2017). Anonymity services Tor, I2P, JonDonym: Classifying in the dark. In *Teletraffic Congress (ITC 29), 2017 29th International* (Vol. 1, pp. 81–89). IEEE.

51. 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)*.
52. Pape, S. (2020). Requirements engineering and tool-support for security and privacy. Habilitation thesis, submitted to the Faculty of Computer Science and Mathematics of the Johann Wolfgang Goethe University, Frankfurt am Main, Germany in September 2020.
53. Pape, S., Harborth, D., & Kröger, J. L. (2021). Privacy concerns go hand in hand with lack of knowledge: The case of the German Corona-Warn-App. In A. Josang, L. Futcher, & J. Hagen (Eds.), *ICT Systems Security and Privacy Protection—36th IFIP TC 11 International Conference, SEC 2021*, volume 625 of *IFIP Advances in Information and Communication Technology* (pp. 256–269). Springer.
54. Pape, S., Ivan, A., Harborth, D., Nakamura, T., Kiyomoto, S., Takasaki, H., & Rannenberg, K. (2020). Open materials discourse: Re-evaluating Internet users' information privacy concerns: The case in Japan. *AIS Transactions on Replication Research, 6*(22), 1–7.
55. Pape, S., Ivan, A., Harborth, D., Nakamura, T., Kiyomoto, S., Takasaki, H., & Rannenberg, K. (2020). Re-evaluating Internet users' information privacy concerns: The case in Japan. *AIS Transactions on Replication Research, 6*(18), 1–18.
56. Pape, S., Tasche, D., Bastys, I., Grosz, A., Laessig, J., & Rannenberg, K. (2018). Towards an architecture for pseudonymous e-commerce—applying privacy by design to online shopping. In *Sicherheit 2018: Sicherheit, Schutz und Zuverlässigkeit, Beiträge der 9. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI), 25.-27. April 2018, Konstanz* (pp. 17–28).
57. Park, Y. J. (2013). Digital literacy and privacy behavior online. *Communication Research, 40*(2), 215–236.
58. Pfitzmann, A., & Hansen, M. (2010). A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management.
59. 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). Springer.
60. Rainie, L., Kiesler, S., Kang, R., Madden, M., Duggan, M., Brown, S., & Dabbish, L. (2013). Anonymity, privacy, and security online. *Pew Research Center, 5*.
61. Rajamma, R. K., Paswan, A. K., & Hossain, M. M. (2009). Why do shoppers abandon shopping cart? Perceived waiting time, risk, and transaction inconvenience. *Journal of Product & Brand Management, 18*(3), 188–197.
62. Rannenberg, K., Pape, S., Tronnier, F., & Löbner, S. (2021). Study on the technical evaluation of de-identification procedures for personal data in the automotive sector. Technical report, Goethe University Frankfurt.
63. Ringle, C. M., Wende, S., & Becker, J. M. (2015). SmartPLS 3. www.smartpls.com
64. Saleh, S., Qadir, J., & Ilyas, M. U. (2018). Shedding light on the dark corners of the Internet: A survey of Tor research. *Journal of Network and Computer Applications, 114*, 1 – 28.
65. 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.
66. Stewart, K. A., & Segars, A. H. (2002). An empirical examination of the concern for information privacy instrument. *Information Systems Research, 13*(1), 36–49.
67. Strübing, J. (2013). Zum Verhältnis von Theorien und Methoden. *Qualitative Sozialforschung. Eine Einführung* (pp. 27–52).
68. The Tor Project. (2018). https://www.torproject.org
69. 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 *Reforming European Data Protection Law* (pp. 333–365). Springer.