David Harborth*, Sebastian Pape, and Kai Rannenberg

Explaining the Technology Use Behavior of Privacy-Enhancing Technologies: The Case of Tor and JonDonym

Abstract: Today's environment of data-driven business models relies heavily on collecting as much personal data as possible. Besides being protected by governmental regulation, internet users can also try to protect their privacy on an individual basis. One of the most famous ways to accomplish this, is to use privacy-enhancing technologies (PETs). However, the number of users is particularly important for the anonymity set of the service. The more users use the service, the more difficult it will be to trace an individual user. There is a lot of research determining the technical properties of PETs like Tor or JonDonym, but the use behavior of the users is rarely considered, although it is a decisive factor for the acceptance of a PET. Therefore, it is an important driver for increasing the user base.

We undertake a first step towards understanding the use behavior of PETs employing a mixed-method approach. We conducted an online survey with 265 users of the anonymity services Tor and JonDonym (124 users of Tor and 141 users of JonDonym). We use the technology acceptance model as a theoretical starting point and extend it with the constructs *perceived anonymity* and *trust in the service* in order to take account for the specific nature of PETs. Our model explains almost half of the variance of the *behavioral intention* to use the two PETs. The results indicate that both newly added variables are highly relevant factors in the path model. We augment these insights with a qualitative analysis of answers to open questions about the users' concerns, the circumstances under which they would pay money and choose a paid premium tariff (only for JonDonym), features they would like to have and why they would or would not recommend Tor/JonDonym. Thereby, we provide additional insights about the users' attitudes and perceptions of the services and propose new use factors not covered by our model for future research.

Keywords: Privacy-Enhancing Technologies, Tor, JonDonym, user study, technology acceptance

DOI 10.2478/popets-2020-0020
Received 2019-08-31; revised 2019-12-15; accepted 2019-12-16.

***Corresponding Author: David Harborth:** Goethe University Frankfurt, Germany, E-mail: david.harborth@m-chair.de

Sebastian Pape: Goethe University Frankfurt, Germany, E-mail: sebastian.pape@m-chair.de

Kai Rannenberg: Goethe University Frankfurt, Germany, E-mail: kai.rannenberg@m-chair.de

1 Introduction

Perry Barlow [6] states: "The internet is the most liberating tool for humanity ever invented, and also the best for surveillance. It's not one or the other. It's both." One of the reasons for surveilling users is a rising economic interest in the internet [7]. However, users who have privacy concerns and feel a strong need to protect their privacy are not helpless, they can make use of privacy-enhancing technologies (PETs). PETs allow users to improve their privacy by eliminating or minimizing personal data disclosure to prevent unnecessary or unwanted processing of personal data [58]. Examples of PETs include services which allow anonymous communication, such as Tor [56] or JonDonym [35].

There has been lots of research on Tor and JonDonym [43, 50], but the large majority of it is of technical nature and does not consider the user. However, the number of users is crucial for this kind of services. Besides the economic point of view which suggests that more users allow a more cost-efficient way to run those services, the quality of the offered service is depending on the number of users 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 [46], thus a larger anonymity set may make it more difficult for an attacker to identify the sender or receiver of a message [2]. As a consequence, it's crucial to learn about the users' intention to use a PET and investigate the factors it depends on. Thus, our research is in line with related work on the obstacles of using secure communication tools [1] with the recommendation to "understand the target population" and research suggesting zero-effort privacy [28, 32] by improving the usability of the service.

In this paper, we investigate how the users' perceived anonymity and their trust in the service influence the intention to use PETs. Privacy protection is usually not the primary goal of the users, but only their secondary goal [17]. The user's

aims become more indistinct if the PET is integrated in the regular service (e.g. anonymous credentials [8]). In contrast to PETs integrated in services, "standalone" PETs are not integrated into a specific service and can be used for several purposes. Thus, examining standalone PETs allows us to focus on the usefulness of the PET with regard to privacy protection and avoids interference with other goals of the user. Therefore, we conducted a survey of the users of the (standalone) anonymity services Tor and JonDonym. The similarities and differences of the two considered PETs are sketched in the next section.

To determine the use factors of Tor and JonDonym, we extend the classical technology acceptance factors by Davis [18, 19] with relevant factors for the specific nature of PETs. We focus on *perceived anonymity* and *trust* because the perception about anonymity is a key variable for users to decide whether to use a such services or not. This perception is closely related to the trust which users might have in services. For example, there are vivid discussions with people claiming that Tor is essentially a big honeypot controlled by the US government. Opposing voices argue that anonymity is never achievable to 100% and that Tor is among the better solutions we have for certain scenarios (e.g. see a recent discussion which developed after a Twitter tweet by Edward Snowden on Tails [57]).

Since most users do not base their decisions on any kind of formal (technical or mathematical) anonymity measurement, we decided to measure the perceived anonymity. The resulting research question is:

RQ1: Does perceived anonymity influence the behavioral intention to use a PET?

However, *perceived anonymity* is a subjective perception of each user. Since we assume, that most users will not dig into mathematical proofs of the assured anonymity or challenge the implementation of the service provider, we conclude that it is important to also consider the *trust in the service provider and the service* itself:

RQ2: Does trust in the PET influence the behavioral intention to use it?

We further refine the two research questions and in particular the relation between *perceived anonymity*, *trust in the service* (Tor/JonDonym), *perceived usefulness*, *perceived ease of use*, *behavioral intention* and *actual use behavior* in Section 3. Consequently, the question arises whether the relationships between the variables of the model differ for the two PETs. We address this question by comparing the results based on a multigroup analysis. To augment and generalize the findings, we also asked users open questions about their concerns, their willingness to donate to Tor or use JonDonym's (paid) premium service, features they would like to have and why they would or would not recommend Tor/JonDonym.

The remainder of the paper is structured as follows: Section 2 briefly introduces the anonymization services Tor and JonDonym, provides information on the technology acceptance model and lists related work on PETs and technology acceptance. In Section 3, we present the research hypotheses, describe the questionnaire and the data collection process. We assess the quality of our quantitative empirical results with regard to reliability and validity in Section 4. We present the results for the research model for PETs and the multigroup analysis to compare Tor and JonDonym in Section 5 and for the qualitative analysis of the open questions in Section 6. In Section 7, we discuss the implications of the results, elaborate on limitations of our work and present possible future work. Section 8 concludes the paper with a summary of the findings.

2 Theoretical Background

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

PETs have a property that is not characteristic for many other technology types. Privacy protection is usually not the primary goal of the users, but only their secondary goal [17]. It is important to understand that in many cases PET users make use of the PET while they pursue another goal like browsing the internet or using instant messengers. These aims become more indistinct if the PET is integrated in the regular service (e.g. anonymous credentials [8]). In contrast to PETs integrated in services, standalone PETs (e.g. overlay networks like Tor [56] or JonDonym [35]) are not integrated into a specific service and can be used for several purposes.

In this paper, we investigate the role of *perceived anonymity* and *trust* in the context of a technology acceptance model for the case of standalone PETs, namely the anonymity services Tor and JonDonym.

2.1 Tor and JonDonym

Tor and JonDonym are low latency anonymity services which redirect packets in a certain way in order 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. In contrast to anonymity services with higher latency such as anonymous remailers low latency anonymity services can be used for interactive services such as messen-

gers. Due to network overheads this still leads to increased latency which was evaluated by Fabian et al. [21] who found associated usability issues when using Tor.

Technically, Tor – the onion router – is an overlay network where the users' traffic is encrypted and directed over several different servers (relays). The Tor client gets a file with a list of relays and follows a certain algorithm to select some relays for a circuit. The aim of the algorithm is to avoid to have two relays in one circuit which are run by the same entity. Selected routes through the circuit should be difficult for an adversary to observe. Consequently, unpredictable routes through the Tor network are chosen. The relays where the traffic leaves the Tor network are called "exit nodes" and for an external service the traffic seems to originate from those. JonDonym is based on user selectable mix cascades (a group of anonymization proxies), with two or three mix servers in one cascade. For mix networks route unpredictability is not important so within one cascade always the same sequence of mix servers is used. Thus, for an external service the traffic seems to originate from the last mix server in the cascade. As a consequence, other usability issues may arise when websites face some abusive traffic from the anonymity services [53] and decide to restrict access for users of the anonymity service. Restrictions range from outright rejection to limiting the users' access to a subset of the service's functionality or imposing hurdles such as CAPTCHA-solving [36] and for the user it appears that the website is not function properly.

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.

Although the specific technical functioning differ, JonDonym and Tor are highly comparable with respect to the general technical structure and the use cases. However, the entities who operate the PETs are different. Tor is operated by a non-profit organization with thousands of voluntarily operated servers (relays) over which the encrypted traffic is directed. Tor is free to use with the option that users can donate to the Tor project. The actual number of users is estimated with approximately 2,000,000 daily users by the Tor Project [56]. However, a recent study using another measurement technique found 8,000,000 daily users [42]. JonDonym is run by a commercial company. The mix servers used to build different mix cascades are operated by independent and non interrelated organizations or private individuals who all publish their identity. The service is available for free with several limitations, like the maximum download speed. In addition, there are different premium rates without these limitations that differ with regard to duration and included data volume. Thus, JonDonym offers several different tariffs and is not based on donations. The actual number of users is not predictable since the service does not keep track of this.

Thus, we assume that users' perceptions are equal with respect to technical characteristics, but may be different with respect to trust in the services.

From a research perspective, there are some papers about JonDonym, e.g. a user study on user characteristics of privacy services [55]. However, the majority of work is about Tor. Most of the work is technical [50], e.g. on improvements such as relieved network congestion, improved router selection, enhanced scalability or reduced communication/computational cost of circuit construction [4]. Naturally, there is also lots of work about the security and anonymity properties [33, 37] and traffic correlation [34].

2.2 Research on Technology Acceptance

The field of technology adoption and use has been the subject of a multitude of previous research, yielding several competing concepts, theories, and models. Some of the most prominent models will be briefly introduced in order to create a common understanding for the following analysis and our choice for using the technology acceptance model (TAM) as the base model.

The Theory of Reasoned Action (TRA) provides the theoretical starting point of TAM. It falls back on empirical research conducted by the social psychologists Fishbein and Ajzen [22]. According to TRA, a person's behaviour is determined by that person's intention to perform this particular behaviour. The behavioural intention (BI), in turn, is influenced by his or her subjective norms (SN) and attitude toward the given behaviour (A). BI can also be viewed as a function of certain beliefs. On the one hand, attitude is related to a person's beliefs about and evaluation of the consequences of the behaviour. On the other hand, the subjective norms concerning a given behaviour are affected by normative beliefs and normative pressure. Subjective norms refer to a person's motivation to comply with persons saying whether he or she should perform the behaviour or not. Feedback loops can arise at various stages of the process, as the performance of a given behaviour can have an impact on beliefs, which in turn influences BI and hence the behaviour itself.

The Theory of Planned Behavior (TPB) by Ajzen [3] is based on the TRA. The overall structural process remains unchanged, i.e. BI is influenced by several components and in turn influences the performance of a behaviour. Nevertheless, it was created as an extension of the TRA integrating the addition of perceived behavioural control (PBC). In practical terms, this denotation refers to a person's perception regarding the ease or difficulty of performing a given behaviour in a given

situation. Consequently, PBC is assumed to depend on the extent to which required resources and opportunities are available. PBC can have an impact on behaviour in two ways. First, indirectly through its influence on BI and its relationship with A and SN. Secondly, together with BI, PBC can be used directly for predicting behavioural achievement.

Based on the TRA and TPB, TAM was developed in 1985 by Davis [18]. The model specifically focuses on the user acceptance of information systems. Similar to TRA, TAM hypothesizes that system use is determined by BI to use. However, it differs from the former model, as BI is jointly influenced by a person's overall attitude towards the use of the technology (A) and the perceived usefulness (PU). Subjective perceptions regarding the system's ease of use are theorized to be fundamental determinants of the system use, too. They directly influence A and PU. Again, PU refers to the extent to which a system would enhance a person's job performance within an organizational context. Perceived ease of use (PEOU) is the degree of effort needed to use the system. Furthermore, external variables affect one's attitude and behaviour indirectly through their impact on PU and PEOU [20]. TAM has been the subject of various studies and extensions whereas PETs were, to the best of our knowledge, seldom considered as a research object in the context of TAM (e.g. the paper by Benenson et al. [8] is based on TAM for the case of anonymous credentials). However, the model is well suited for our case of explaining the behavioral intention and actual use behavior of PETs due to the following reasons. First, the model and the respective constructs are widely tested in the literature and the base model provides valid and reliable measures of the above mentioned variables. Thus, we argue that these constructs provide an appropriate basis for explaining technology acceptance of PETs. Second, the model is parsimonious, i.e. there are relatively few constructs necessary to explain a relatively large share of the variance in the target constructs. This makes it possible to add technology-specific variables (in our case for PETs) without overspecifying the model and minimizing an overspecification bias. We adapt the original constructs of TAM to the case of PETs by specifying perceived usefulness as the usefulness of a PET to protect the user's privacy. We argue that this definition is reasonable for our examplary PETs (Tor and JonDonym) since they enable users to do multiple tasks while privacy protection is the evident goal when using them. This perception regarding the usefulness to protect the user's privacy is therefore theorized to be crucial when deciding to use a PET. In summary, we argue that our adapted TAM model serves as an appropriate theoretical underlying for answering our research questions and contribute to our understanding regarding the main factors influencing individuals' use behavior of PETs.

2.3 Related Work

Previous non-technical work on PETs mainly considers usability studies and does not primarily focus on technology acceptance of these technologies. For example, Lee et al. [39] assess the usability of the Tor Launcher and propose recommendations to overcome the found usability issues. In a qualitative study, Forte et al. [24] examine perceived risks and privacy concerns of Tor users and Wikipedia editors who are concerned about their privacy. Previous related work investigates privacy concerns and trust with respect to JonDonym [30] and Tor [31] based on Internet users' information privacy concerns (IUIPC) [40]. Comparable studies to the study at hand with respect to the underlying theory of technology acceptance are the ones by Benenson et al. [8, 9] and Krontiris et al. [38] who investigate acceptance factors for an anonymous credential service. However, in their case the anonymous credential service is integrated into a course evaluation system. Thus, the users of their anonymous credential service had a clearly defined primary task (evaluation of the course system) and a secondary task (ensure privacy protection). Benenson et al. focused on the measurement of the perceived usefulness of the anonymous credential system (the secondary goal), but state that considering the perceived usefulness for the primary goals as well, may change the relationship between the variables in their model [8]. In contrast to their study, we examine a standalone PET, and thus can focus on privacy protection as the primary goal of the users with respect to the PET. Compared to the previous studies, Brecht et al. [11] focus on no specific anonymization service in their analysis on acceptance factors. In addition, they do not base their model on classical technology acceptance variables like we do in this paper.

3 Methodology

In the following subsections, we discuss the research model and hypotheses based on the extended TAM, the questionnaire and the data collection process. In addition, we provide a brief overview of the employed quantitative statistical analysis approach.

3.1 Research Model and Hypotheses

PETs are structurally different compared to technologies used in the job context or pleasure-oriented (hedonic) information systems like games. Therefore, the research hypotheses and the model must be derived according to the properties of the specific technology (see Table 3 for the differences of the results between Tor and JonDonym [29]).

In general, it is obvious to users what a certain technology does. For example, if users employ a spreadsheet program in their job environment, they will see the immediate result of their action when the program provides them a calculation. The same holds for pleasure-oriented technologies which provide an immediate feedback to the user during the interaction. However, this interaction and feedback structure is different with PETs. Anonymity is the main goal which a user can achieve by using PETs. However, most PETs are designed to not harm the user experience. Besides some negative side effects such as a loss of speed during browsing the internet or an increasing occurrence of CAPTCHAs [15], the user may not be able to detect the running of the PET at all (which would be the optimal characteristic of a PET). The direct effects of the increased anonymity in general go undetected since they consist of long term consequences, e.g. different advertisements, unless the user visits special websites with anonymity tests or showing the internet address of the request. In summary, the main impact of a PET is not immediately tangible for the user.

Therefore, perceptions about the achieved impact of using the technology should be specifically incorporated in any model dealing with drivers of *use behavior*. This matches the observation that most users do not base their decisions on any kind of formal (technical or mathematical) anonymity measurement. Thus, we adapted a formerly tested and validated construct named "perceived anonymity" to the case of the PETs Tor and JonDonym [8]. The construct mainly asks for the perceptions of users about their level of anonymity achieved by the use of the PET. Due to the natural importance of anonymity for a PET, we argue that these perceptions will have an important effect on the *trust in the technology*. Thus, the more users think that the PET will create anonymity during their online activities, the more they will trust the PET (H1a). Creating anonymity for its users is the main purpose of a PET. Thus, we hypothesize that the *perceived anonymity* has a positive effect on the *perceived usefulness of the PET to protect the users' privacy* (H1b).

H1a: Perceived anonymity when using PETs has a positive effect on trust in PETs.

H1b: Perceived anonymity when using PETs has a positive effect on the perceived usefulness of PETs to protect the users' privacy.

Trust is a diverse concept integrated in several models in the Information Systems (IS) domain. It is shown that different trust relationships exist in the context of technology adoption of information systems [54]. Trust can refer to the technology (in our case PETs (Tor and JonDonym)) as well as to the service provider. Since the non-profit organization of Tor evolved around the service [56], it is rather difficult for users to distinguish which label refers to the technology itself and which refers to the organization. The same holds for JonDonym since JonDonym is the only main service offered by the commercial company JonDos. Therefore, we argue that it is rather difficult for users to distinguish which label refers to the technology itself and which refers to the company. Thus, we decided to ask for *trust in the PET* (Tor and JonDonym, respectively), assuming that the difference to ask for trust in the organization / company is negligible.

Literature shows that trust in services enables positive attitudes towards interacting with these services [44]. Applying this logic to the case of technologies, we hypothesize that a higher level of trust in a given technology causes a stronger *behavioral intention to use* this technology (H2a). Besides this direct effect on use intentions, trust influences the perceived usefulness of a given technology. Thus, we argue that the higher the trust in the PET, the higher is the level of *perceived usefulness of protecting the user's privacy* (H2b). Lastly, we hypothesize that *trust in PETs* has a positive effect on the *perceived ease of use of PETs* (H2c). Previous literature supports this hypothesis, indicating that a higher level of trust in a given technology decreases the need to understand each and every detail of the technology [14]. This is especially relevant for the case of PETs since they represent a kind of technology with a relatively high level of complexity (e.g. compared to pleasure-oriented information systems).

H2a: Trust in PETs has a positive effect on the behavioral intention to use the technology.

H2b: Trust in PETs has a positive effect on the perceived usefulness of protecting the user's privacy.

H2c: Trust in PETs has a positive effect on the perceived ease of use of PETs.

The theoretical underlying of hypotheses H3, H4a, H4b and H5 is adapted from the original work on TAM by Davis [18, 19] since PETs are not different to other technologies with regard to the relationships of *perceived usefulness*, *perceived ease*, *behavioral intention to use* and *actual use behavior*. However, *perceived usefulness* refers explicitly to privacy protection as it is the sole purpose of the technology. The rationale for hypotheses 3 and 4a are straightforward. The higher the *perceived usefulness* and *ease of use* of a given technology, the stronger the *behavioral intention to use* this technology. Literature indicates that *perceived ease of use* itself has a positive effect on the *perceived usefulness* of a technology (H4b). Improvements in *ease of use* contribute to efficiency gains and enable users of a given technology to accomplish the same goals with less effort [18, 19]. We argue that this rationale also holds for PETs, since a PET which is easy to use requires less mental effort to fulfill the goal of protecting user's privacy. Research on the relationship between *behavioral intention* and *actual use behavior* consistently indicates

that there is a positive relationship between the two variables, where *behavioral intention* has a positive effect on *actual use behavior* [22, 52]. We assume that this relationship is also apparent for the case of PETs (H5). In summary, we hypothesize:

H3: The perceived usefulness of protecting the user's privacy has a positive effect on the behavioral intention to use the technology.

H4a: Perceived ease of use has a positive effect on the behavioral intention to use the technology.

H4b: Perceived ease of use has a positive effect on the perceived usefulness of protecting the user's privacy.

H5: The behavioral intention to use PETs has a positive effect on the actual use behavior.

These hypotheses constitute the research model illustrated in Figure 1.

3.2 Questionnaire and Data Collection

The questionnaire constructs are adapted from different sources. *Perceived ease of use* (PEOU) and *perceived usefulness* are adapted from Venkatesh and Davis [59], *behavioral intention* (BI) is adapted from Venkatesh et al. [60], *trust in the PET service* is adapted from Pavlou [44] and *perceived anonymity* is adapted from Benenson et al. [8]. The former constructs are measured based on a seven-point Likert scale, ranging from "strongly disagree" to "strongly agree". The *actual use behavior* is measured with a ten-item frequency scale [49]. The adapted questionnaire items can be found in Table 1. These items are solely used for the quantitative analysis in Section 5. Besides these questions, we asked participants for their age, education and gender. However, we cannot present a reliable overview of these variables since they 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 and could potentially react to mandatory demographic questions by terminating the survey. Consequently, the demographics are incomplete to a large extent. Therefore, we had to resign from a discussion of the demographics in our research context.

We conducted the studies with German and English-speaking users of Tor and JonDonym. For each service, 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: We translated the English questionnaire into German with the help of a certified translator (translators are standardized by 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. Last, a group of five academic colleagues checked the equivalence of the two English versions. All items were found to be equivalent.

Since we investigate the drivers of the *use behavior of PETs*, we collected data from actual users of the PETs. We installed the surveys on a university server and managed it with the LimeSurvey [51]. For Tor, we distributed the links to the English and German version over multiple channels on the internet. Although there are 2,000,000 to 8,000,000 active users of the service, it was relatively difficult to gather the necessary number of complete answers for a quantitative analysis. Thus, to foster future research about Tor users, we provide an overview of every distribution channel in the appendix. 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 participants who answered a test question in the middle of the survey incorrectly, 124 usable data sets remained for the following analysis. The test question simply asked participants to select a specified answer in a given set. Questions like this are usually added to questionnaires to check for the awareness of the participants and avoid participants just clicking through the survey without carefully reading the questions.

For JonDonym, we distributed the links to the English and German version with the beta version of the JonDonym browser and published them on the official JonDonym homepage. This made it possible to address the actual users of the PET in the most efficient manner. 416 participants started the questionnaire (173 for the English version and 243 for the German version). Of those 416 approached participants, 141 (53 for the English version and 88 for the German version) remained after deleting unfinished sets and all participants who answered a test question in the middle of the survey incorrectly. In total, our sample consists of 265 complete answers.

We also addressed potential ethical issues of the user survey. The ethics board of the authors' university provides an extensive checklist which qualifies our study as exempt for an ethics review. However, in order to inform participants about our data collection process we provided information about the related research project and the goal of the study (improve PETs and investigate their acceptance factors). Furthermore, we stated that all answers are anonymous (e.g. no saving of IP addresses), that all answers are stored on a German server and that by participating in the survey, participants agree that their answers are used for scientific publications, research publications and a PhD thesis. We provided an open-text-field for

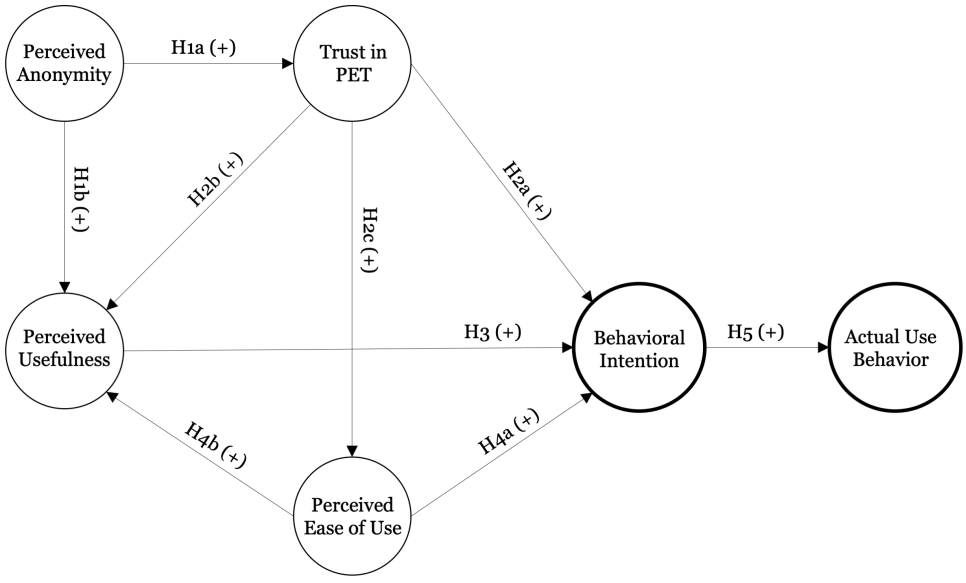

Fig. 1. Research model showing the structural model with the research hypotheses

feedback and a researcher's e-mail address for further questions and requests at the end of the survey.

3.3 Statistical Analysis Approach

We hypothesize that perceived anonymity and trust in the PET, along with the standard variables drawn from the TAM (cf. Section 2.2), are measurable underlying constructs that influence the adoption of Tor and JonDonym. To test this, we use the questionnaire described in Section 3.2 to measure these constructs, and apply a standard statistical analysis approach called structural equation modelling (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 [27] for our analysis (Hair et al. extensively discuss on the use of PLS-SEM [26]).

4 Validity and Reliability Testing

We tested our model (cf. Section 3) using SmartPLS version 3.2.7 [48]. 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 chose the suggested path weighting scheme with a maximum of 300 iterations and a stop criterion of 10^{-7}. For the bootstrapping procedure, we used 5000 bootstrap subsamples and no sign changes as the method for handling sign changes during the iterations of the bootstrapping procedure [26]. We met the suggested minimum sample size with 265 datasets considering the threshold of ten times the number of structural paths headed towards a latent construct in the model [27].

4.1 Measurement Model Assessment

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 [27]. 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 [26]. Table 1 includes the ICR of the variables in the last two rows. It can be seen that all values for Cronbach's α and the composite

reliability are above the lower threshold of 0.7 and no value is above 0.95. In sum, ICR is established for our variables.

In a next step, we assess the convergent validity to determine the degree to which indicators of a certain reflective construct are explained by that construct. For that, we calculate the outer loadings of the indicators of the constructs (indicator reliability) and evaluate the average variance extracted (AVE) [26]. Loadings above 0.7 imply that the indicators have much in common, which is desirable for reflective measurement models. Table 1 shows the outer loadings with grey background on the diagonal. All loadings are higher than 0.7. 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 indicators' variance. The first column of Table 2 presents the constructs' AVE. All values are above 0.5, demonstrating convergent validity.

The next step for assessing the measurement model is the evaluation of discriminant validity. It measures the degree of uniqueness of a construct compared to other constructs. 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 [26]. Table 1 illustrates the cross-loadings as off-diagonal elements. All cross-loadings are smaller than the outer loadings, fulfilling the first assessment approach of discriminant validity. In the second approach, we compare 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). Table 2 contains the square root of the AVE as on-diagonal values. All values fulfill the Fornell-Larcker criterion, indicating discriminant validity.

The last step of the measurement model assessment is to check for common method bias (CMB). CMB can occur if data is gathered with a self-reported survey at one point in time in one questionnaire [41]. Since this is the case in our research design, we test for CMB. 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 [47]. 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 four factors have eigenvalues larger than 1 which account for 72.04% of the total variance. The first factor explains 46.51% of the total variance. Thus, no single factor emerged and the first factor does not explain the majority of the variance. Hence, we argue that CMB is not likely to be an issue.

4.2 Structural Model Assessment

We first test for possible collinearity problems before discussing the results of the structural model. Collinearity is present if two predictor variables are highly correlated with each other. This is important since collinearity can otherwise bias the results heavily. To address this issue, we assess the inner variance inflation factor (inner VIF). All VIF values above 5 indicate that collinearity between constructs is present [26]. For our model, the highest VIF is 1.892. Thus, collinearity is apparently not an issue.

We also assessed the predictive relevance of the two added variables for *behavioral intention* and *actual use behavior* in order to assess whether they are important enough to be included in the model. A simple measure for the relevance of *perceived anonymity* and *trust* is to delete both variables and run the model again. The results show that the R^2-value for *behavioral intention* decreases to 41.9% (= 5.8 percentage points less). Thus, without the two new variables the explained variance for *behavioral intention* decreases by 12.2%. A more advanced measure for predictive relevance is the Q^2 measure. It indicates the out-of-sample predictive relevance of the structural model with regard to the endogenous latent variables based on a blindfolding procedure [26]. We used an omission distance d=7. Recommended values for d are between five and ten. 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. Detailed information about the calculation is given by Chin [13]. For our model, Q^2 is calculated for *behavioral intention* and *use behavior*. Values above 0 indicate that the model has the property of predictive relevance. Omitting both new variables leads to a decrease of Q^2 for *behavioral intention* from 0.336 to 0.293. R^2 as well as Q^2 did not change for *actual use* when deleting the new variables, since there is no direct relation from these constructs to *actual use*.

5 Quantitative Analysis Results

We present the results of our quantitative analysis in this section. First, we discuss the path estimates and the R^2-values for our extended technology acceptance model. Second, we conduct a multigroup analysis in order to investigate potential differences in the path estimates between Tor and JonDonym.

Constructs	BI	PEOU	PA	Trust$_{PETs}$	PU	USE
BI1. I intend to continue using the PET[1] in the future.	0.884	0.499	0.537	0.573	0.602	0.322
BI2. I will always try to use the PET[1] in my daily life.	0.830	0.409	0.350	0.408	0.372	0.319
BI3. I plan to continue to use the PET[1] frequently.	0.931	0.487	0.439	0.545	0.534	0.408
PEOU1. My interaction with the PET[1] is clear and understandable.	0.503	0.825	0.281	0.386	0.410	0.153
PEOU2. Interacting with the PET[1] does not require a lot of my mental effort.	0.390	0.826	0.232	0.259	0.361	0.178
PEOU3. I find the PET[1] to be easy to use.	0.450	0.911	0.233	0.316	0.386	0.211
PEOU4. I find it easy to get the PET[1] to do what I want it to do.	0.468	0.882	0.338	0.382	0.473	0.232
PA1. The PET[1] is able to protect my anonymity in during my online activities.	0.488	0.311	0.899	0.593	0.641	0.103
PA2. With the PET[1] I obtain a sense of anonymity in my online activities.	0.437	0.259	0.885	0.609	0.616	0.143
PA3. The PET[1] can prevent threats to my anonymity when being online.	0.418	0.276	0.871	0.544	0.582	0.126
Trust$_{PETs}$1. The PET[1] is trustworthy.	0.513	0.348	0.642	0.891	0.608	0.115
Trust$_{PETs}$2. The PET[1] keeps promises and commitments.	0.557	0.386	0.581	0.921	0.568	0.139
Trust$_{PETs}$3. I trust the PET[1] because they keep my best interests in mind.	0.509	0.335	0.556	0.895	0.545	0.166
PU1. Using the PET[1] improves the performance of my privacy protection.	0.349	0.338	0.459	0.442	0.782	0.130
PU2. Using the PET[1] increases my level of privacy.	0.559	0.433	0.668	0.626	0.934	0.210
PU3. Using the PET[1] enhances the effectiveness of my privacy.	0.439	0.429	0.604	0.499	0.882	0.136
PU4. I find the PET[1] to be useful in protecting my privacy.	0.628	0.456	0.662	0.627	0.896	0.225
USE. Please choose your use frequency[2] of the PET[1].	0.398	0.225	0.140	0.155	0.206	1.000
Cronbach's α	0.859	0.885	0.862	0.886	0.898	-
Composite Reliability	0.914	0.920	0.916	0.929	0.929	-

BI: Behavioral Intention PEOU: Perceived Ease of Use PA: Perceived Anonymity USE: Actual Use Frequency
PU: Perceived Usefulness of Protecting Users' Privacy [1]Tor/JonDonym [2]10-point scale from "Never" to "All the time"

Table 1. Loadings and cross-loadings of the reflective items and ICR measures

Constructs (AVE)	BI	PA	PEOU	PU	Trust$_{PETs}$
BI (0.780)	0.883				
PA (0.783)	0.507	0.885			
PEOU (0.743)	0.530	0.319	0.862		
PU (0.766)	0.579	0.693	0.477	0.875	
Trust (0.814)	0.583	0.658	0.396	0.636	0.902
USE	0.398	0.140	0.225	0.206	0.155

Table 2. Discriminant validity and construct correlations

5.1 Technology Acceptance Factors of PETs

Figure 2 presents the results of the path estimations and the R^2-values of the target variables *behavioral intention* and *actual use behavior*. In addition, we provide the R^2-values for *trust*, *perceived ease of use* and *perceived usefulness*. R^2-values are weak with values around 0.25, moderate with 0.50 and substantial with 0.75 [27]. Based on this classification, the R^2-value for *behavioral intention* is moderate in size and weak for the variable *actual use behavior*. Our model explains 47.7% of the variance in the *behavioral intention to use the PET* and 15.8% of the variance of the *actual use behavior*.

In the Tor survey, several participants answered that they never use Tor (21 participants answered "never" to the question about their use frequency of Tor). This statement of these 21 participants is in contrast to their answer to a question in which we asked participants how many years they are using Tor. Here, the respective participants stated that they used Tor for six years (median of 6 years and an average of 6.87 years). The correlation coefficient between the years of using Tor and the use frequency is very small and negative with -0.0222. 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 [49], but recommend to consider this issue in future research with a similar context. For JonDonym, we did not observe this issue. The respective path coefficients are shown in Table 3. The effect size between *behavioral intention* and *actual use* is 0.679 for JonDonym and 0.179 for Tor.

Three main drivers of perceived usefulness of PETs

The explained variance of *perceived usefulness* is 58.4%, indicating that the three variables, *perceived anonymity*, *trust* and *perceived ease of use* explain almost two-thirds of the variance of this construct. Thus, we identified three major drivers of users' perceptions with regard to the usefulness of a privacy-enhancing technology. This result shows that the two

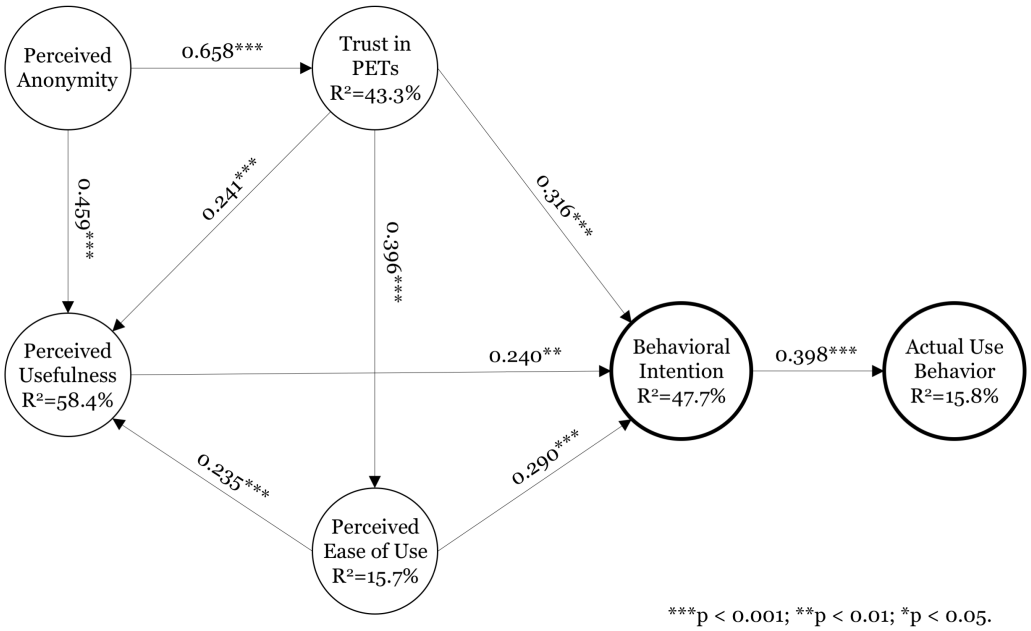

Fig. 2. Research model with path estimates and R^2 values of the structural model for PETs

	Relationships	Path coeff. original (JonDonym)	Path coeff. original (Tor)	P-values (JonDonym)	P-values (Tor)	Diff. path coeff. (| JonDonym - Tor |)	P-values (JonDonym vs Tor)
H1a	PA → Trust_{PETs}	0.597	0.709	< 0.001	< 0.001	0.112	0.865
H1b	PA → PU	0.543	0.369	< 0.001	< 0.001	0.174	0.088
H2a	Trust_{PETs} → BI	0.416	0.232	< 0.001	0.010	0.184	0.064
H2b	Trust_{PETs} → PU	0.173	0.304	0.035	0.008	0.131	0.823
H2c	Trust_{PETs} → PEOU	0.378	0.431	< 0.001	< 0.001	0.053	0.657
H3	PU → BI	0.183	0.300	0.046	0.002	0.117	0.805
H4a	PEOU → BI	0.206	0.371	0.011	< 0.001	0.165	0.929
H4b	PEOU → PU	0.182	0.300	0.039	< 0.001	0.118	0.830
H5	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 of Protecting Users' Privacy

Table 3. Results of the MGA-analysis (grey background indicates statistical significance at least at the 10% level)

newly added variables are important antecedents in the technology acceptance model which should be considered in future work on this topic. The strongest effect is exerted by the users' *perceived anonymity* provided by the service (H1b confirmed). This result is not surprising considering that providing anonymity is the main goal of a PET. In addition, *perceived anonymity* has a relatively strong and statistically significant effect on *trust* (H1a confirmed). Thus, users' *trust in PETs* is mainly driven by their perceptions that the service can create anonymity (R^2-value of Trust_{PETs} equals 43.3%).

Trust in PETs is the most important factor

As hypothesized in H2a - H2c, *trust* has a significant positive effect on the *behavioral intention to use the PET*, the *perceived usefulness* and the *perceived ease of use*. Therefore, *trust* emerges as a highly relevant concept when determining the drivers of users' *use behavior of PETs*. Among the factors influencing *behavioral intention*, it has the strongest effect size (0.316). As discussed earlier, hypotheses H3 - H5 are adapted from the original work on TAM [18, 19] and can be confirmed for the case of PETs.

Significant total effects of trust and perceived anonymity

Since the effects of *perceived anonymity* and *trust* on *behavioral intention* and the *actual use behavior* are partially indirect, we determine and analyze the total effects for these variables (cf. Table 4). It can be seen that the total effects for *behavioral intention* are relatively large and highly statistically significant. Thus, *perceived anonymity* and *trust* strongly influence the target variable *behavioral intention*. Due to the

Total effect	Effect size	P-value
PA → BI	0.446	< 0.001
PA → USE	0.177	< 0.001
Trust_{PETs} → BI	0.511	< 0.001
Trust_{PETs} → USE	0.203	< 0.001

Table 4. Total effects for perceived anonymity and trust in PETs

discussed bias in the construct USE, the total effects for this variable are comparably small.

5.2 Multigroup Analysis

After the analysis of the whole data sample, we split the data set into two parts and analyze the results for Tor and JonDonym separately. For that, we conduct a multigroup analysis and test whether there are statistically significant differences for each of the hypotheses.

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. For that purpose, we conducted a multigroup analysis in SmartPLS (cf. Table 3). We use a less conservative level of statistical significance of 10% in this table 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 [23] and can be considered a rule of thumb.

Trust is less important for Tor than for JonDonym

The results indicate that all relationships are similar for both PETs with respect to direction of the effect and effect size (see the path coefficients for both PETs). This supports the assumption that Tor is comparable to JonDonym from a user's perspective. Only three relationships are significantly different for the two technologies (p-value of difference smaller than 0.1). First, the effect of *perceived anonymity* on *perceived usefulness* is weaker for Tor than for JonDonym. Furthermore, *trust in the PET* is significantly less important for Tor than for JonDonym.

Differences in these relationships can have many causes. Among others, Tor exists longer and has significantly more users. However, the results are especially interesting when considering the structures of the two organizations. Tor has a more community-oriented structure based on donations, whereas JonDonym is operated by a profit-oriented company which charges money for the unlimited use of the PET [35]. Thus, users possibly focus more on the trust in the PET if it is operated by a commercial company, which leads to a stronger influence of trust on the use intentions and behaviors.

In contrast to this, Tor might be perceived as a technology that is based on the community which operates the used servers voluntarily without financial intentions. This leads to a wide distribution of the infrastructure and trust in the service is not needed from a technical point of view since the communication can only be intercepted if each server is controlled by one attacker. Therefore, users might perceive that the need for trust is not as important as if a profit-oriented company operates the PET.

6 Qualitative Analysis Results

We augment our quantitative results from the previous section with a qualitative analysis of answers to five open questions included in the questionnaires. By that, we provide deeper insights into certain aspects of the quantitative analysis from Section 5 and hints to relevant questions for future work. We show the questions and the number of answers to them in Table 5. These numbers exclude answers as "I don't know", "no" and so on. Two researchers analyzed the statements independently from each other and abstracted the invidiual 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 *usability* can be both a negative as well as a positive characteristic, depending on the user and the respective context. For example, the code "usability" joins negative as well as positive perceptions of users.

We do the coding of the 626 statements to the open questions in two stages. We use a coding method from sociology [12, 25], which comprises two or three coding phases, namely initial coding, axial coding and focused coding. We only use initial and focused coding since this level of structuring is sufficient for our data [12]. First, we initially code 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 decide to name these codes "Subconcepts" in our results since they already provide one level of abstraction. After the initial coding phase, we compare the different codings of the researchers and discussed the individual codes. Thereby, we agreed upon certain subconcepts which 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, known reli-

Questions	Number of answers for	
	JonDonym	Tor
1. Do you have any concerns about using JonDonym / Tor?	56	85
2. Under which circumstances would you choose one of the premium tariffs? (JonDonym)	76	not applicable
3. Which additional features would you like to have at your current tariff? (JonDonym)	32	
3. Which additional features would you like to have for Tor?		124
4. Why would you recommend JonDonym / Tor?	122	102
5. Why would you not recommend JonDonym / Tor?	11	18
Σ	297	329

Table 5. Open-ended questions from the survey and number of answers

ability measures as Cohen's Kappa [16] are not usable for our case since these measures are relying on predefined categories. Consequently, we use 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 yields a intercoder reliablity of 68.69% and 81,48%, respectively (cf. Table 5 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 count 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 towards the mismatches in the intercoder reliability measures.

In the second step, we structured the most occuring themes in these initial codes and came up with the focused codes. We name these codes "Concepts" in Table 6 since we find that users primarily make statements about either technical issues, about their beliefs and perceptions or about economic issues.

During the coding, we saw that there are certain subconcepts that hold for both, Tor and JonDonym. However, there are also subconcepts which are different for both PETs or nonexistent in the data for either one of the technologies. Therefore, we illustrate these differences separately in columns four and five of Table 6. We provide quotes from the statements for each concept, except for "Costs" and "Payment methods" since they are rather straightforward and users just stated that JonDonym should be cheaper and offer certain payment methods mentioned in the table.

Similar subconcepts to quantitative model

The results include four subconcepts which can be found in the investigated model of the quantitative part (Section 5). Participants mention *usability*, *performance*, *anonymity* and *trust* oftentimes in the context of concerns or why they would or would not recommend the respective PET. As mentioned before, these concepts are not tied to a certain positive or negative interpretation. This becomes obvious when looking at the exemplary quotes in the table.

Usability positively influences use behavior

Usability is mentioned most of the times in the context of a positive factor influencing the use. This means, if a PET is easy to use, users will prefer to use it (**Tor.5**, **Jon.5**). In contrast, participants mentioned for both PETs that they would like to have a better documentation in order to enhance the usability (**Tor.4**, **Jon.4**). We also find another interesting dimension for *usability* in the data. Some participants stated that missing knowledge about the correct use of the PET can lead to worse results with respect to privacy than without using the PET at all. This implies that some users are concerned that the degree of *ease of use* is not as high as it should be, especially considering layman users. This could lead to situations in which layman users think that the PET works properly, while it indeed does not (**Tor.6**, **Jon.6**).

Limited performance in the free version of JonDonym

The concept *performance* is only partially equivalent to *perceived usefulness* since we defined it as usefulness to protect the user's privacy. However, we argue that a PET needs to fulfill the requirement of low latency in order to be useful in the sense of protecting the users privacy. Therefore, we argue that the concept *performance* can be seen as the equivalent to the variable *perceived usefulness* in the quantitative model. It slightly differs for Tor (**Tor.7**) and JonDonym since participants only mention the issue for JonDonym when talking about the free of charge option (**Jon.7**, **Jon.8**) (the decreased performance is implemented by default for this option as a feature of the tariff [35]).

Anonymity and concerns regarding deanonymization

The concept *anonymity* is mentioned in the context of representing the main purpose of why participants use a PET (**Tor.9**, **Jon.10**). However, another dimension of this concept is a concern of being deanonymized by a variety of attackers, espe-

Concepts	Subconcepts	Common to both PETs	Specific Subconcepts for Tor	Specific Subconcepts for JD
Statements about 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**)
Statements about 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 organisations. 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. preconfigured 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 anonymisation when I researched anonymisation 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*

Table 6. Results of the coding for the open questions including quotes

cially government agencies (**Tor.8**, **Jon.9**) and by the fact that the anonymity set is too small because of a user base which is too small. The small user base is only mentioned as a concern by users of JonDonym (**Jon.11**).

Trust as a use factor and reason for concerns

The last concept which can be found in the quantitative model is *trust in the technology*. As for *usability*, *trust* is mentioned as a concern but also as a reason for recommending both PETs in our sample. However, the qualitative analysis reveals that the trust dimensions are slightly different between Tor and JonDoym. For Tor, participants mainly mention trust in the community (**Tor.12**), whereas the community aspect is not existent for JonDonym. For JonDonym, participants mainly focus on trust in the company and the technology (**Jon.13**). In summary, our findings related to trust support the quantitative results and strengthen our claim that *trust in the technology* is a major factor in a user's decision to use a PET. However, the results also show that future work should consider to differentiate the concept of trust and adapt it to the specific context of the PET.

New concepts emerged in the qualitative analysis

The concepts "PET design", "compatibility", "social issues", "substitute technologies" and the "statements about economical issues" are not reflected in our quantitative model. Participants still mention these concepts several times and we argue that they might be interesting to consider for future work dealing with technology acceptance of PETs.

Technical design of PETs affect concerns

"PET design" describes mainly concerns about the technical structure of the PETs which is prone to attacks (especially by government agencies). Tor and JonDonym differ in their technical structure which is reflected in the statements. Several participants mention "malicious exit nodes" as a technical issue for Tor (**Tor.2**). For JonDonym, participants are mainly concerned about the location of the mix cascades (**Jon.2**). Related to "PET design" is the concept "substitute technologies". Here, several participants state for Tor and JonDonym that the respective PET is the "best option available" amongst the existing PETs (**Tor.15**, **Jon.14**). Thus, the concern about the technical design might be compensated partially by this opinion of users. Interestingly, several other JonDonym users mention Tor several times as a comparative technology to argue about advantages of JonDonym (**Jon.3**, **Jon.8**). Participants oftentimes make this comparison in the context of deciding when they would spend money for a JonDonym premium tariff. Here, they argue that they would only do this, if Tor was not existent. This is due to costs, but also due to the larger anonymity set provided by Tor (**Jon.11**). This result implies that there are very high market entry barriers for comparable commercial PETs due to the strong market position of Tor. Related to the design of Tor and JonDonym are feature requests mentioned by participants. For example, participants ask for TCP support for Tor (**Tor.1**) and faster security updates for JonDonym (**Jon.1**).

Compatibility of PETs with websites affects adoption

"Compatibility" describes concerns and statements why participants would not recommend the PETs. They primarily mention accessibility issues with websites when using the respective PET (**Tor.3**, **Jon.3**). This is an important factor to consider for future technical improvements of the PETs and closely linked to the usability. PET developers should address this issue to foster a wider market acceptance.

Fear of investigations and adverse social effects

"Consequences" are prevalent for Tor and JonDonym users. The subconcept represents the fear of PET users that their use of PETs causes them to "stand out" (**Tor.10**) and leads to investigations by police forces or other government agencies (**Tor.11**, **Jon.12**). In addition to concerns related to governmental agencies, Tor users mentioned adverse social effects due to the use of Tor. These adverse social effects describe the belief that other members of the society think negatively about Tor. For example, participants stated that Tor is oftentimes primarily associated with illegal activities by others (**Tor.13**, **Tor.14**). This subconcept is interesting for future work dealing with the acceptance of PETs in the mass market. Layman users might be susceptible to such perceptions and therefore, avoid using a PET. Thus, marketers of PETs should stress the benefits for the user's privacy and self-determination and cleary address and explain these concerns related to possible consequences and social issues.

Importance of pricing schemes and payment methods

The last part on statements about economical issues is mainly relevant for JonDonym. The concept "costs" indicates that JonDonym users would like to have other pricing schemes which are either cheaper or include more available high-speed traffic (**Jon.15**). The concept "payment methods" is showing that PET users want a variety of (mainly anonymous) payment methods like virtual currencies or paysafecards [45] (**Jon.15**). The last concept is about "use cases" which influence the decision to use a PET at all. Censorship in certain countries is the main use scenario represented in this subconcept for Tor (**Tor.16**) and JonDonym (**Jon.16**). In addition, we find that participants would pay money for JonDonym if they were required to do sensitive, work-related tasks (**Jon.17**).

7 Discussion

We found strong effects for the influence of the *perceived anonymity* on the *behavioral intention to use the PET* (RQ1). The participants mentioned anonymity several times as the main reasons why they are using Tor or JonDonym. Therefore,

the results indicate that anonymity is one of the most important factors in the use decisions of PETs. In contrast to the findings of Benenson et al. [8], who found that *trust in the PET* has no statistically significant impact on the *intention to use the service*, we found a significant medium-sized effect of *trust in the PET* on the *behavioral intention to use* it (0.316) (RQ2). One possible explanation for the difference between the literature and our results is that the trust in the service and the trust in the service provider are perceived as equivalent in our use case, whereas in the literature trust refers solely to the technology [8]. In addition, the results of the multigroup analysis revealed that *trust in the PET* has a much stronger effect on the *use intentions* if the technology is operated by a commercial company (effect stronger for JonDonym compared to Tor) [5, 35]. However, this is only one possible explanation and there could be several other omitted variables. Still, it is an interesting starting point for future work.

Our results indicate that the *use behavior of PETs* is mainly influenced by the variables *perceived usefulness* and *perceived ease of use* as well as the newly added variables *trust* and *perceived anonymity*. This result is in line with the given statements of the participants to the open questions as well as with previous studies showing that *usability* is an important aspect for the use of this PET [11, 21].

Although we checked for several reliability and validity issues, certain limitations might impact our results. First, the sample size of 265 participants (124 for Tor and 141 for JonDonym) is relatively small for a quantitative study. However, since we reached the suggested minimum sample size for the applied method, we argue that our results are still valid. In addition, it is very difficult to gather data of actual users of PETs since it is a comparable small population that we could survey. It is also relevant to mention that we did not offer any financial rewards for the participation. Secondly, our sample is likely to be biased since our sample is by default a subset of anomymity service users who are privacy sensitive individuals relative to the rest of the population. Moreover, since they answered our survey, it could be that the respondents are the least privacy sensitive of the individuals since the most privacy sensitive individuals might not even have considered to participate in our survey. Thus, certain findings from our research might not be generalizable to a potentially larger user base. A third limitation concerns possible self-report biases (e.g. social desirability). We addressed this possible issue by gathering the data fully anonymized. Fourthly, mixing results of the German and English questionnaire could be a source of errors. On the one hand, this procedure was necessary to achieve the minimum sample size. On the other hand, we followed a very thorough translation procedure to ensure the highest level of equivalence as possible. Thus, we argue that this limitation did not affect the results to a large extent. However, we cannot rule out that there are unobserved effects on the results due to running the survey in more than one country at all. In addition, we did not control for the participants' actual or former use of different standalone PETs. This experience might have an impact on their assessments of Tor and JonDonym. Furthermore, demographic questions were not mandatory to fill out due to our assumption that these types of individuals who use Tor or JonDonym are highly cautious with respect to their privacy. Thus, we decided to go for a larger sample size considering that we might have lost participants otherwise (if demographics had to be filled out mandatorily).

Future work can build on the proposed relationships and extensions of our model to investigate the acceptance and use of other PETs in more detail. We could explain more than half of the variance in the target construct *behavioral intention* with a rather parsimonious model. For the construct *actual use behavior*, we did not find comparable high values due to the issues with the answers mentioned in Section 5. Furthermore, the analysis of the open questions shows interesting new concepts to consider in future work on technology acceptance of PETs. These concepts are about the design of the respective PET, compatibility when using it (e.g. websites not working properly), social issues, negative privacy experiences, other available solutions for privacy protecting and economic factors (only relevant for commercial applications).

In addition, it would be interesting to investigate the perceptions of non-users about PETs and compare them to actual users to figure out how the perceptions of these groups differ with respect to their influence on the *use intentions* and *actual use behavior*.

8 Conclusion

Up to now research on privacy-enhancing technologies mainly focused on the technical aspects of the technologies. In addition, to the best of our knowledge, the anonymization services Tor and JonDonym were not compared in the context of technology acceptance. However, a successful implementation and adoption of PETs requires a profound understanding of the perceptions and behaviors of actual and possible users of the technologies. Thus, with this paper we investigated actual users of existing PETs as a first step to address this research problem. Our results indicate that the basic rationale of technology use models is applicable for PETs like Tor and JonDonym as well as for other comparable privacy-enhancing technologies providing a relatively strong level of anonymization. The newly introduced variables *perceived anonymity* and *trust* improved the explanatory power of the structural model for the case of PETs and can be considered as a starting point

for comparable research problems in future work. The analysis of the open questions shows that the existing variables in our technology acceptance model can also be found as relevant concepts in the statements by the participants (*usability*, *performance*, *anonymity* and *trust*). In addition, the new concepts can be considered for future studies in this area.

Our results are a first step towards a deeper understanding of the acceptance of privacy-enhancing technologies. The results provide insights for developers and marketers to specifically address issues hindering a broader diffusion of PETs. Research in this area is a real contribution for strengthening the personal right for privacy in times of ever-increasing personal data collection in the internet.

9 Acknowledgements

This work was partially supported by German Federal Ministry of Education and Research (BMBF) [grant number 16KIS0371] and by the European Union's Horizon 2020 research and innovation program from the project CyberSec4Europe [grant agreement number 830929].

References

[1] Ruba Abu-Salma, M Angela Sasse, Joseph Bonneau, Anastasia Danilova, Alena Naiakshina, and Matthew Smith. Obstacles to the Adoption of Secure Communication Tools. In *IEEE Security & Privacy*, pages 137 – 153, 2017.

[2] Alessandro Acquisti, Roger Dingledine, and Paul Syverson. On the Economics of Anonymity Alessandro. In *International Conference on Financial Cryptography*, pages 84–102. Springer Berlin Heidelberg, 2003.

[3] Icek Ajzen. The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes*, 50(2):179–211, 1991.

[4] Mashael Alsabah and Ian Goldberg. Performance and security improvements for tor: A survey. *ACM Comput. Surv.*, 49(2):32:1–32:36, September 2016.

[5] Anonymized. 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, 2018.

[6] James Ball. Hacktivists in the frontline battle for the internet. https://www.theguardian.com/technology/2012/apr/20/hacktivists-battle-internet, 2012.

[7] Mathieu Bédard. The underestimated economic benefits of the internet. Regulation series, The Montreal Economic Institute, 2016. Economic Notes.

[8] Zinaida Benenson, Anna Girard, and Ioannis Krontiris. User Acceptance Factors for Anonymous Credentials: An Empirical Investigation. *14th Annual Workshop on the Economics of Information Security (WEIS)*, pages 1–33, 2015.

[9] Zinaida Benenson, Anna Girard, Ioannis Krontiris, Vassia Liagkou, Kai Rannenberg, and Yannis C. Stamatiou. User Acceptance of Privacy-ABCs: An Exploratory Study. In *Human–Computer Interaction*, pages 375–386, 2014.

[10] John J. Borking and Charles Raab. Laws, PETs and Other Technologies for Privacy Protection. *Journal of Information, Law and Technology*, 1:1–14, 2001.

[11] Franziska Brecht, Benjamin Fabian, Steffen Kunz, and Sebastian Mueller. Are You Willing to Wait Longer for Internet Privacy? In *ECIS 2011 Proceedings*, 2011.

[12] Kathy Charmaz. *Constructing Grounded Theory*. Sage Publications, London, 2nd editio edition, 2014.

[13] Wynne W. Chin. The Partial Least Squares Approach to Structural Equation Modeling. In George A. Marcoulides, editor, *Modern Methods for Business Research*, pages 295–336. Lawrence Erlbaum, Mahwah, NJ, 1998.

[14] Alina M. Chircu, Gordon B. Davis, and Robert J. Kauffman. Trust, Expertise, and E-Commerce Intermediary Adoption. In *AMCIS 2000 Proceedings*, 2000.

[15] Richard Chirgwin. CloudFlare shows Tor users the way out of CAPTCHA hell, 2016.

[16] Jacob Cohen. Weighted kappa: Nominal scale agreement provision for scaled disagreement or partial credit., 1968.

[17] L. F. Cranor and S. Garfinkel. *Security and Usability: Designing Secure Systems that People Can Use*. O'Reilly, Farnham, 2008.

[18] F.D. Davis. A Technology Acceptance Model for Empirically Testing New End-User Information Systems: Theory and Results. *Massachusetts Institute of Technology*, 1985.

[19] F.D. Davis. Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, 13(3):319–340, 1989.

[20] F.D. Davis, Richard P. Bagozzi, and Paul R. Warshaw. User Acceptance of Computer Technology: a Comparison of Two Theoretical Models. *Management Science*, 35(8):982–1003, 1989.

[21] Benjamin Fabian, Florian Goertz, Steffen Kunz, Sebastian Müller, and Mathias Nitzsche. Privately Waiting – A Usability Analysis of the Tor Anonymity Network. In *AMCIS 2010 Proceedings*, 2010.

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

[23] R. A. Fisher. *Statistical Methods for Research Workers*. Oliver & Boyd, Edinburgh, 14 edition, 1970.

[24] Andrea Forte, Nazanin Andalibi, and Rachel Greenstadt. Privacy, anonymity, and perceived risk in open collaboration: A study of tor users and wikipedians. In *CSCW*, pages 1800–1811, 2017.

[25] Barney G. Glaser and Anselm L. Strauss. *The Discovery of Grounded Theory*. Aldine Pub., Chicago, 1967.

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

[27] J. Hair, Christian M. Ringle, and Marko Sarstedt. PLS-SEM: Indeed a Silver Bullet. *Journal of Marketing Theory and Practice*, 19(2):139–152, 2011.

[28] David Harborth, Dominik Herrmann, Stefan Köpsell, Sebastian Pape, Christian Roth, Hannes Federrath, Dogan Kes-

dogan, and Kai Rannenberg. Integrating privacy-enhancing technologies into the internet infrastructure. *arXiv preprint arXiv:1711.07220*, 2017.

[29] David Harborth and Sebastian Pape. Examining Technology Use Factors of Privacy-Enhancing Technologies: The Role of Perceived Anonymity and Trust. In *Twenty-fourth Americas Conference on Information Systems (AMCIS2018)*, pages 1–10, New Orleans, USA, 2018.

[30] David Harborth and Sebastian Pape. JonDonym Users' Information Privacy Concerns. In L. Janczewski and M. Kutyłowski, editors, *ICT Systems Security and Privacy Protection - 33rd IFIP TC 11 International Conference, SEC 2018*, pages 170–184, Poznan, Poland, 2018. Springer, Cham.

[31] David Harborth and Sebastian Pape. 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*, Hawaii, US, 2019.

[32] Dominik Herrmann, Jens Lindemann, Ephraim Zimmer, and Hannes Federrath. Anonymity online for everyone: What is missing for zero-effort privacy on the internet? In *International Workshop on Open Problems in Network Security*, pages 82–94. Springer, 2015.

[33] Rob Jansen, Marc Juarez, Rafael Galvez, Tariq Elahi, and Claudia Diaz. Inside Job: Applying Traffic Analysis to Measure Tor from Within. In *Network and Distributed Systems Security (NDSS) Symposium*, pages 1–15, 2018.

[34] Aaron Johnson, Chris Wacek, Rob Jansen, Micah Sherr, and Paul Syverson. Users get routed: Traffic correlation on tor by realistic adversaries. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, CCS '13, pages 337–348, New York, NY, USA, 2013. ACM.

[35] JonDos Gmbh. Official Homepage of JonDonym. https://www.anonym-surfen.de, 2018.

[36] Sheharbano Khattak, David Fifield, Sadia Afroz, Mobin Javed, Srikanth Sundaresan, Vern Paxson, Steven J. Murdoch, and Damon McCoy. Do you see what I see?: Differential treatment of anonymous users. In *Network and Distributed System Security Symposium*, 2016.

[37] R. Koch, M. Golling, and G. D. Rodosek. How anonymous is the tor network? a long-term black-box investigation. *Computer*, 49(3):42–49, Mar. 2016.

[38] Ioannis Krontiris, Zinaida Benenson, Anna Girard, Ahmad Sabouri, Kai Rannenberg, and Peter Schoo. Privacy-ABCs as a Case for Studying the Adoption of PETs by Users and Service Providers. In *APF*, pages 104–123, 2015.

[39] Linda Lee, David Fifield, Nathan Malkin, Ganesh Iyer, Serge Egelman, and David Wagner. A Usability Evaluation of Tor Launcher. *Proceedings on Privacy Enhancing Technologies*, (3):90–109, 2017.

[40] Naresh K. Malhotra, Sung S. Kim, and James Agarwal. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, 15(4):336–355, 2004.

[41] Naresh K. Malhotra, Sung S. Kim, and Ashutosh Patil. Common Method Variance in IS Research: A Comparison of Alternative Approaches and a Reanalysis of Past Research. *Management Science*, 52(12):1865–1883, 2006.

[42] Akshaya Mani, T. Wilson-Brown, Rob Jansen, Aaron Johnson, and Micah Sherr. Understanding Tor Usage with Privacy-Preserving Measurement. In *2018 Internet Measurement Conference (IMC'18)*, pages 1–13, 2018.

[43] Antonio Montieri, Domenico Ciuonzo, Giuseppe Aceto, and Antonio Pescapé. Anonymity services tor, i2p, jondonym: Classifying in the dark. In *Teletraffic Congress (ITC 29), 2017 29th International*, volume 1, pages 81–89. IEEE, 2017.

[44] Paul A. Pavlou. Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model. *International Journal of Electronic Commerce*, 7(3):101–134, 2003.

[45] paysafecard.com Deutschland. Website paysafecard. https://www.paysafecard.com/de-de/, 2018.

[46] Andreas Pfitzmann and Marit Hansen. A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management. 2010.

[47] Philip M Podsakoff, Scott B MacKenzie, J. Y. Lee, and Nathan P Podsakoff. Common method biases in behavioral research: a critical review of the literature and recommended remedies. *Journal of Applied Psychology*, 88(5):879–903, 2003.

[48] Christian M. Ringle, S. Wende, and Jan Michael Becker. SmartPLS 3. www.smartpls.com, 2015.

[49] L.D. Rosen, K. Whaling, L.M. Carrier, N.A. Cheever, and J. Rokkum. The Media and Technology Usage and Attitudes Scale: An empirical investigation. *Comput Human Behav.*, 29(6):2501–2511, 2013.

[50] Saad Saleh, Junaid Qadir, and Muhammad U. Ilyas. Shedding light on the dark corners of the internet: A survey of tor research. *Journal of Network and Computer Applications*, 114:1 – 28, 2018.

[51] Carsten Schmitz. LimeSurvey Project Team. http://www.limesurvey.org, 2015.

[52] Blair H. Sheppard, Jon Hartwick, and Paul R. Warshaw. 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, 1988.

[53] Rachee Singh, Rishab Nithyanand, Sadia Afroz, Paul Pearce, Michael Carl Tschantz, Phillipa Gill, and Vern Paxson. Characterizing the nature and dynamics of tor exit blocking. In *26th USENIX Security Symposium (USENIX Security). USENIX Association, Vancouver, BC*, pages 325–341, 2017.

[54] Matthias Söllner, Izak Benbasat, David Gefen, Jan Marco Leimeister, and Paul A. Pavlou. Trust : An MIS Quarterly Research Curation Focus of the Research Curation. *Management Information Systems Quarterly*, (October):1–9, 2016.

[55] Sarah Spiekermann. The Desire for Privacy: Insights into the Views and Nature of the Early Adopters of Privacy Services. *International Journal of Technology and Human Interaction*, 1(1):74–83, 2005.

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

[57] Twitter Discussion. Twitter Tweet by Edward Snowden on Tails and Tor. https://twitter.com/Snowden/status/1165297667490103302, 2019.

[58] G.W. van Blarkom, John J. Borking, and J.G.E. Olk. *"PET"*. *Handbook of Privacy and Privacy-Enhancing Technologies*.

2003.

[59] V. Venkatesh and F. D. Davis. A theoretical extension of the technology acceptance model: Four longitudinal Studies. *Management Science*, 46(2):186–205, 2000.

[60] Viswanath Venkatesh, James Thong, and Xin Xu. Consumer Acceptance and User of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology. *MIS Quarterly*, 36(1):157–178, 2012.

All websites have been accessed last on August 25th, 2019.

Distribution Channels of the Tor Online Survey

1. Mailinglists:
   (a) tor-talk[1]
   (b) liberationtech[2]
   (c) IFIP TC 11[3]
   (d) FOSAD[4]
   (e) GI PET[5]
   (f) GI FBSEC[6]
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[7], Off Topic
   (b) The Hub[8], Beginners
   (c) Onion Land[9], Off Topic
   (d) 8chan[10], /tech/
   (e) IntelExchange[11], Unverified Users
   (f) Code Green[12], Discussions
   (g) Changolia[13], overchan.random
   (h) Atlayo[14], Posting
5. Personal Announcements at Workshops

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