Examining Technology Use Factors of Privacy-Enhancing Technologies: The Role of Perceived Anonymity and Trust

Completed Research

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

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

Abstract

Today's environment of data-driven business models relies heavily on collecting as much personal data as possible. This is one of the main causes for the importance of privacy-enhancing technologies (PETs) to protect internet users' privacy. Still, PETs are rather a niche product used by relatively few users on the internet. We undertake a first step towards understanding the use behavior of such technologies. For that purpose, we conducted an online survey with 141 users of the anonymity service "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. Our model explains almost half of the variance of the behavioral intention to use JonDonym and the actual use behavior. In addition, the results indicate that both added variables are highly relevant factors in the path model.

Keywords

Privacy-enhancing technologies (PETs), technology use, technology acceptance, perceived anonymity, trust, privacy, structural equation model.

Introduction

Perry Barlow (Ball 2012) 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 (Bédard 2016). 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 (van Blarkom et al. 2003). PETs have a property that is not characteristic for many other technology types. They usually serve not only the primary goals of the users, but also their secondary goals (Cranor and Garfinkel 2008). 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 (Benenson et al. 2015)). In contrast to PETs integrated in services, standalone PETs (e.g. overlay networks like Tor (The Tor Project 2018)) are not integrated into a specific service and can be used for several purposes.

In this paper, we investigate how the users’ main goal (privacy respectively anonymity) and their trust in the service influence the intention to use the PET. In order to focus on the PET itself and not to interfere with possible other goals, we choose a standalone PET as object for investigation. This allows us to focus on the usefulness of the PET with regard to privacy protection and avoids confounders due to other goals of the user. Therefore, we conducted a survey of the users of the anonymity service JonDonym. JonDonym is a proxy client and will forward the traffic of the users’ internet applications encrypted to the mix cascades to hide their IP addresses (JonDos Gmbh 2018).

To determine the use factors of this PET, we focused on perceived anonymity and trust: 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 influences the behavioral intention to use it?

We further refine the two research questions and in particular the connection between perceived anonymity, perceived usefulness and trust in the service (JonDonym) in section 3. This allows us to integrate them into a technology acceptance model (TAM) which we then use to answer the research questions.

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

Background and Related Work

Privacy-Enhancing Technologies (PETs) is an umbrella term for different privacy protecting technologies. Borking and Raab define PETs as a "coherent system of ICT measures that protects privacy [...] by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data; all without losing the functionality of the data system" (Borking and Raab 2001, p. 1).

In this paper, we investigate the role of perceived anonymity and trust in the context of a technology acceptance model for the case of the anonymity service JonDonym (JonDos Gmbh 2018). Comparable to Tor (The Tor Project 2018), JonDonym is an anonymity service and a PET. However, unlike Tor, it is a proxy system based on mix cascades. It is available for free with several limitations, like a restricted maximum download speed. In addition, there are different premium rates without these limitations that differ with regard to duration and included data volume. Thus, JonDonym offers several different tariffs and is not based on donations like Tor. The actual number of users is not predictable since the service does not keep track of this. JonDonym is also the focus of an earlier user study on user characteristics of privacy services (Spiekermann 2005). However, the focus of the study is rather descriptive and does not focus on users' beliefs and concerns.

Previous non-technical work on PETs considers mainly usability studies and does not primarily focus on privacy concerns and related trust and risk beliefs of PET users. For example, Lee et al. (2017) assess the usability of the Tor Launcher and propose recommendations to overcome the found usability issues. Comparable studies to ours are the ones by Benenson et al. (2014, 2015) and Krontiris et al. (2015), who investigate acceptance factors for an anonymous credentials service. However, in their case the anonymous credential service is integrated into an 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. (2014) 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. 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.

Methodology

We base our research on the well-known technology acceptance model (TAM) by Davis (1985, 1989). For analyzing the cause-effect relationships between the latent variables, we use structural equation modelling (SEM). There are two main approaches for SEM, namely covariance-based SEM (CB-SEM) and partial least squares SEM (PLS-SEM). Since our research goal is to predict the target construct actual use behavior of JonDonym, we use PLS-SEM for our analysis (Hair et al. 2011). In the following subsections, we discuss the research model and hypotheses based on the extended TAM, the questionnaire and the data collection process. The demographic questions were not mandatory to fill out. This was done on purpose since we assumed that most of the participants are highly sensitive with respect to their personal data. Therefore, we resign from a discussion of the demographics in our research context. This decision is backed up by Singh and Hill, who found no statistically significant differences across gender, income groups, educational levels, or political affiliation in the desire to protect one's privacy (Singh and Hill 2003).

Research Model and Hypotheses

PETs are structurally different than formerly investigated technologies in the job context or hedonic information systems. 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 hedonic technologies which provide an immediate feedback to the user during the interaction. However, this interaction and feedback structure is different with PETs. The main impact a user can achieve by using JonDonym is anonymity. 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 (Chirgwin 2016), the user may not be able to detect the PET at all. 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.

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 validated construct named "perceived anonymity" to the case of JonDonym (Benenson et al. 2015). 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 use of a PET. Thus, we hypothesize that the perceived anonymity has a positive effect on the perceived usefulness of the PET to protect the user's privacy (H1b).

> *H1a: Perceived anonymity achieved by using JonDonym has a positive effect on trust in JonDonym.*
>
> *H1b: Perceived anonymity achieved by using JonDonym has a positive effect on the perceived usefulness of JonDonym to protect the user's privacy.*

Trust is a diverse concept integrated in several models in the IS domain. It is shown that different trust relationships exist in the context of technology adoption of information systems (Söllner et al. 2016). Trust can refer to the technology (in our case JonDonym) itself as well as to the service provider (in our case JonDos). However, JonDonym is the company's main product. 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 service (JonDonym), assuming that the difference to ask for trust in the company is negligible. The items for measuring trust and the effects of trust on other variables of the technology acceptance model are adapted from Pavlou (2003). Thus, we hypothesize that trust influences behavioral intention, perceived usefulness and perceived ease of use positively.

> *H2a: Trust in JonDonym has a positive effect on the behavioral intention to use the technology.*
>
> *H2b: Trust in JonDonym has a positive effect on the perceived usefulness of JonDonym to protect the user's privacy.*

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

The theoretical underlying of hypotheses H3, H4a, H4b and H5 can be adapted from the original work on TAM by Davis (1985, 1989) since PETs are not different to other technologies with regard to 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. Thus, 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 JonDonym to protect the user's privacy.

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

Questionnaire Composition and Data Collection Procedure

The questionnaire constructs are adapted from different sources. The constructs Perceived ease of use (PEOU) and perceived usefulness are adapted from Venkatesh and Davis (2000), behavioral intention (BI) is adapted from Venkatesh et al. (2012), trust in the PET service is adapted from Pavlou (2003) and perceived anonymity is adapted from Benenson et al. (2015). The actual use behavior is measured with a ten-item frequency scale (Rosen et al. 2013). We conducted the study with German and English speaking JonDonym users. Thus, we administered two questionnaires. All items for the German questionnaire had to be translated into German since all of the constructs are adapted from English literature.

To ensure content validity of the translation, we followed a rigorous translation process. First, we translated the English questionnaire into German with the help of a certified translator (translators are standardized following the DIN EN 15038 norm). The German version was then given to a second independent certified translator who retranslated the questionnaire to English. This step was done to ensure the equivalence of the translation. Third, a group of five academic colleagues checked the two English versions with regard to this equivalence. All items were found to be equivalent. The items can be found in Table 1.

Since we investigate the drivers of the use behavior of JonDonym, we collected data from actual users of the PET. We installed the surveys on a university server and managed it with the survey software LimeSurvey (version 2.63.1) (Schmitz 2015). The links to the English and German version were distributed with the beta version of the JonDonym browser and published on the official JonDonym homepage. This made it possible to address the actual users of the PET in the most efficient manner. In sum, 416 participants started the questionnaire (173 for the English version and 243 for the German version). Of those 416 approached participants, 141 (53 for the English version and 88 for the German version) remained after deleting unfinished sets and all participants who answered a test question in the middle of the survey incorrectly.

Results

We tested the model using SmartPLS version 3.2.7 (Ringle et al. 2015). Before looking at the result of the structural model and discussing its implications, we discuss the measurement model, and check for the reliability and validity of our results. This is a precondition of being able to interpret the results of the structural model. Furthermore, it is recommended to report the computational settings. For the PLS algorithm, we choose the path weighting scheme with a maximum of 300 iterations and a stop criterion of 10^{-7}. For the bootstrapping procedure, we use 5000 bootstrap subsamples and no sign changes as the method for handling sign changes during the iterations of the bootstrapping procedure. In addition, it is relevant to mention that we met the suggested minimum sample size with 141 datasets considering the threshold of ten times the number of structural paths headed towards a latent construct in the model (Hair et al. 2011).

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 (Hair et al. 2011). 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 ∝ and the composite reliability. The values of both measures should be between 0.7 and 0.95 for research that builds upon accepted models. Values of Cronbach's α are seen as a lower bound and values of the composite reliability as an upper bound of the assessment (Hair et al. 2017). Table 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.

Constructs	BI	PEOU	PA	Trust	PU
BI1. I intend to continue using JonDonym in the future.	**0.913**	0.432	0.546	0.622	0.541
BI2. I will always try to use JonDonym in my daily life.	**0.806**	0.328	0.331	0.362	0.313
BI3. I plan to continue to use JonDonym frequently.	**0.941**	0.393	0.466	0.582	0.458
PEUO1. My interaction with JonDonym is clear and understandable.	0.369	**0.862**	0.224	0.372	0.327
PEUO2. Interacting with JonDonym does not require a lot of my mental effort.	0.349	**0.843**	0.130	0.224	0.227
PEUO3. I find JonDonym to be easy to use.	0.341	**0.920**	0.145	0.246	0.303
PEUO4. I find it easy to get JonDonym to do what I want it to do.	0.444	**0.893**	0.373	0.426	0.464
PA1. JonDonym is able to protect my anonymity in during my online activities.	0.398	0.151	**0.882**	0.482	0.584
PA2. With JonDonym I obtain a sense of anonymity in my online activities.	0.489	0.254	**0.874**	0.593	0.657
PA3. JonDonym can prevent threats to my anonymity when being online.	0.445	0.297	**0.869**	0.480	0.574
Trust1. JonDonym is trustworthy.	0.494	0.321	0.580	**0.909**	0.557
Trust2. JonDonym keeps promises and commitments.	0.568	0.365	0.531	**0.922**	0.505
Trust3. I trust JonDonym because they keep my best interests in mind.	0.576	0.350	0.526	**0.911**	0.491
PU1. Using JonDonym improves the performance of my privacy protection.	0.330	0.347	0.553	0.398	**0.885**
PU2. Using JonDonym increases my level of privacy.	0.468	0.334	0.669	0.578	**0.923**
PU3. Using JonDonym enhances the effectiveness of my privacy.	0.304	0.322	0.547	0.372	**0.855**
PU4. I find JonDonym to be useful in protecting my privacy.	0.592	0.377	0.653	0.590	**0.863**
Cronbach's ∝	0.865	0.904	0.847	0.902	0.906
Composite Reliability	0.918	0.932	0.907	0.939	0.933

Table 1. Loadings and Cross-Loadings of the Reflective Items and ICR measures

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) (Hair et al. 2017). 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 in bold 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 variance of the indicators. The first column of Table 2 presents the AVE of the constructs. All values are well 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. Comparable to the convergent validity assessment, two approaches are used for investigated discriminant validity. The first approach, assessing cross-loadings, is dealing with single indicators. All outer loadings of a certain construct should be larger than its cross-loadings with other constructs (Hair et al. 2017). Table 1 illustrates the cross-loadings as off-diagonal elements. All cross-loadings are smaller than the outer loadings, fulfilling the first assessment approach of discriminant validity. The second approach is on the construct level and compares the square root of the constructs' AVE with the correlations with other constructs. The square root of the AVE of a single construct should be larger than the correlation with other constructs (Fornell-Larcker criterion). Table 2 contains the square root of the AVE as on-diagonal values. All values are larger than the correlations with other constructs, indicating discriminant validity.

Constructs (AVE)	BI	PA	PEOU	PU	Trust
BI (0.790)	0.889				
PA (0.765)	0.510	0.875			
PEOU (0.774)	0.435	0.268	0.880		
PU (0.778)	0.500	0.695	0.393	0.882	
Trust (0.836)	0.597	0.597	0.378	0.566	0.914

Table 2. Discriminant Validity with AVEs and Construct Correlations

The last step of the measurement model assessment is the 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 (Malhotra et al. 2006). Since this is the case in our research design, the need to test for CMB arises. An unrotated principal component factor analysis is performed with the software package STATA 14.0 to conduct the Harman's single-factor test to address the issue of CMB (Podsakoff et al. 2003). The assumptions of the test are that CMB is not an issue if there is no single factor that results from the factor analysis or that the first factor does not account for the majority of the total variance. The test shows that four factors have eigenvalues larger than 1 which account for 75.48% of the total variance. The first factor explains 45.35% 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 in the data set.

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 (Hair et al. 2017). For our model, the highest VIF is 1.688. Thus, collinearity is apparently not an issue.

Figure 1 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 (Hair et al. 2011). Based on this classification, the R^2-values for behavioral intention and actual use are rather moderate in size. Thus, our model explains 42.9% of the variance in the behavioral intention to use the PET and 46.1% of the variance of the actual use behavior. This result is very good considering the parsimonious measurement model. In addition, the explained variance of perceived usefulness is 54.7%, indicating that the three variables, perceived anonymity, trust and perceived ease of use explain more than half 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. 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 strong and statistically significant effect on trust (H1a confirmed). Thus, users' trust in the PET is mainly driven by their perceptions that the service can create anonymity.

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. It has the strongest effect size (0.416) on behavioral intention. As discussed earlier, hypotheses H3 - H5 are adapted from the original work on TAM (Davis 1985, 1989) and can be confirmed for the case of PETs.

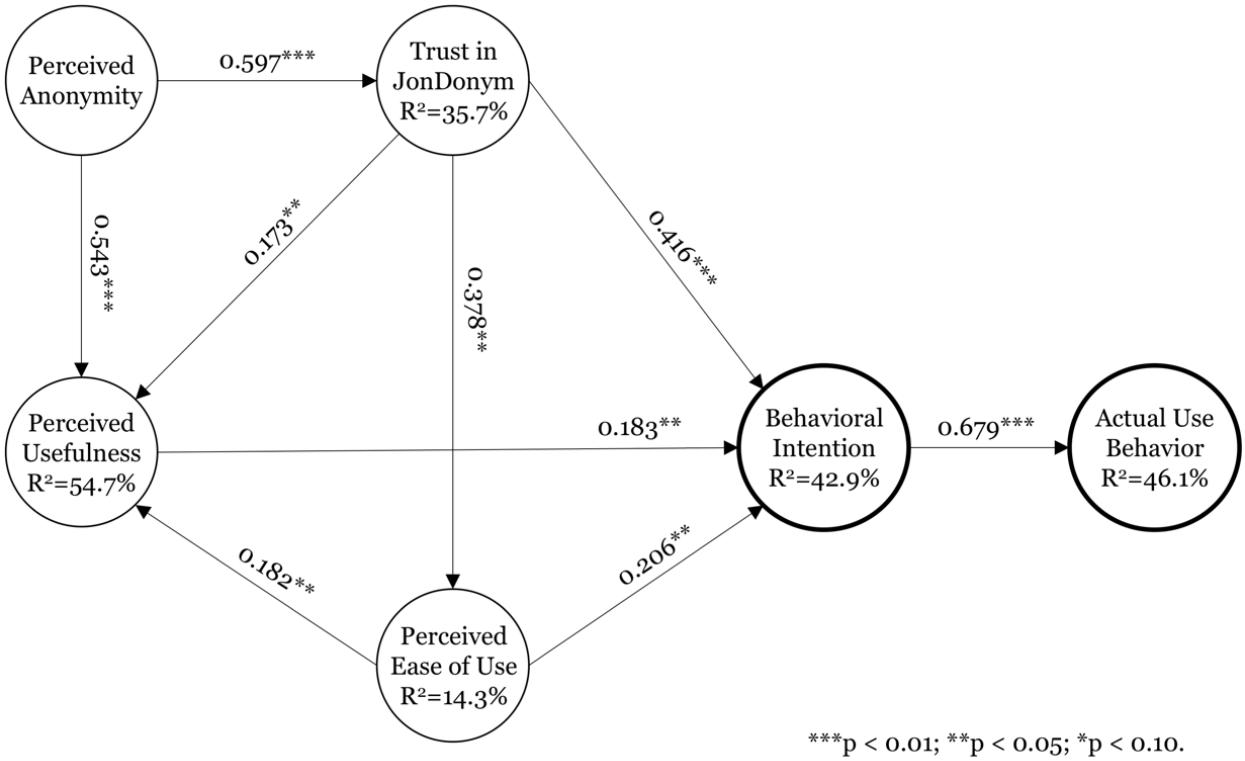

Figure 1. Path Estimates and Adjusted R^2-values of the Structural Model

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 3). It can be seen that all total effects are relatively large and highly statistically significant. Thus, perceived anonymity and trust strongly influence the target variables BI and USE.

Total effect	Effect size	P-value
PA → BI	0.431	0.000
PA → USE	0.289	0.000
Trust → BI	0.551	0.000
Trust → USE	0.370	0.000

Table 3. Total Effects for the Variables Perceived Anonymity and Trust

As a next, we assessed the predictive relevance of the two added variables for behavioral intention and actual use behavior. 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 31.9% (= eleven percentage points less). Thus, without the two new variables the explained variance for behavioral intention decreases by roughly a quarter (25.64%). 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 (Hair et al. 2017). 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 cannot be provided due to space limitations. For further information see Chin (1998). 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 0.304 to 0.223. R^2 as well as Q^2 did not change for actual use when deleting the new variables, since there is not direct relation from the constructs to the actual use construct and behavioral intention solely explains a large share of variance in use.

Discussion and Conclusion

Research on privacy-enhancing technologies mainly focused on the technical aspects of the technologies up to now. However, a successful implementation and adoption of PETs requires of profound understanding of the perceptions and behaviors of actual and possible users of the technologies. The IS domain has the proper methods and knowledge to tackle such questions. Thus, with this paper we investigated actual users of an existing PET as a first step to address this research problem. Our results indicate that the basic rationale of technology use models holds for privacy-enhancing technologies. However, the newly introduced variables perceived anonymity and trust strongly improved the explanatory of the structural model for the case of a PET and should be considered for comparable research problems in future work.

Although we checked for several reliability and validity issues, certain limitations might impact our results. First, the sample size of 141 participants 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. A second limitation concerns possible self-report biases (e.g. social desirability). We addressed this possible issue by gathering the data fully anonymized. Furthermore, demographic questions were not mandatory to fill out. Third, 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. Lastly, 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 JonDonym.

We found strong effects for the influence of the perceived anonymity on the behavioral intention to use a PET (RQ1). In contrast to the findings of Benenson et al. (2015), who found that trust in the PET has no

statistically significant impact on the intention to use the service, we also found a strong effect of trust in the PET on the behavioral intention to use it (RQ2). One reason for the difference might be that the trust in the service and the trust in the service provider were very likely equivalent in our use case. However, to adequately address the difference further research is needed. From a practical point of view, our results indicate that PET providers should aim to establish a trustworthy service with a high level of transparency in order to increase the perceived anonymity of users.

Future work can build on the proposed relationships and extensions of our model to investigate the acceptance and use of PETs in more detail. We could explain almost half of the variance in the target constructs behavioral intention and actual use behavior with a rather parsimonious model. Thus, the current model provides a good starting point to investigate other comparable PETs, like Tor or a VPN service. In addition, new privacy or technology-specific variables could be added to strengthen the understanding about usage of PETs. Based on our findings, future work could also investigate the found relationships with a qualitative research approach in more detail. In a next step, it would be interesting to investigate the perceptions of non-users about PETs and compare the findings to actual users. By that, it would be possible for developers and marketers to specifically address issue hindering a broader diffusion of PETs. This could be a real contribution for strengthening the personal right for privacy in times of ever-increasing personal data collection in the internet.

Acknowledgements

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

REFERENCES

Ball, J. 2012. "Hacktivists in the Frontline Battle for the Internet," *The Guardian*. (https://www.theguardian.com/technology/2012/apr/20/hacktivists-battle-internet, accessed February 26, 2018).

Bédard, M. 2016. "The Underestimated Economic Benefits of the Internet," in *Regulation Series, The Montreal Economic Institute*.

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

Benenson, Z., Girard, A., Krontiris, I., Liagkou, V., Rannenberg, K., and Stamatiou, Y. C. 2014. "User Acceptance of Privacy-ABCs: An Exploratory Study," in *Human–Computer Interaction*, pp. 375–386.

van Blarkom, G. W., Borking, J. J., and Olk, J. G. E. 2003. *"PET". Handbook of Privacy and Privacy-Enhancing Technologies*.

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

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

Chirgwin, R. 2016. "CloudFlare Shows Tor Users the Way out of CAPTCHA Hell," *The Register*. (https://www.theregister.co.uk/2016/10/05/cloudflare_tor/, accessed February 23, 2018).

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

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

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

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

Hair, J., Ringle, C. M., and Sarstedt, M. 2011. "PLS-SEM: Indeed a Silver Bullet," *The Journal of Marketing Theory and Practice* (19:2), pp. 139–152.

JonDos Gmbh. 2018. "Official Homepage of JonDonym." (https://www.anonym-surfen.de, accessed

January 16, 2018).
Krontiris, I., Benenson, Z., Girard, A., Sabouri, A., Rannenberg, K., and Schoo, P. 2015. "Privacy-ABCs as a Case for Studying the Adoption of PETs by Users and Service Providers," in *APF*, pp. 104–123.
Lee, L., Fifield, D., Malkin, N., Iyer, G., Egelman, S., and Wagner, D. 2017. "A Usability Evaluation of Tor Launcher," *Proceedings on Privacy Enhancing Technologies* (3), pp. 90–109.
Malhotra, N. K., Kim, S. S., and Patil, A. 2006. "Common Method Variance in IS Research: A Comparison of Alternative Approaches and a Reanalysis of Past Research," *Management Science* (52:12), pp. 1865–1883.
Pavlou, P. A. 2003. "Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model," *International Journal of Electronic Commerce* (7:3), pp. 101–134.
Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., and Podsakoff, N. P. 2003. "Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies.," *Journal of Applied Psychology* (88:5), pp. 879–903.
Ringle, C. M., Wende, S., and Becker, J. M. 2015. *SmartPLS 3*, Boenningstedt: SmartPLS GmbH, http://www.smartpls.com.
Rosen, L. D., Whaling, K., Carrier, L. M., Cheever, N. A., and Rokkum, J. 2013. "The Media and Technology Usage and Attitudes Scale: An Empirical Investigation," *Comput Human Behav*. (29:6), pp. 2501–2511.
Schmitz, C. 2015. *LimeSurvey Project Team*, LimeSurvey Project Hamburg, Germany, LimeSurvey: An Open Source survey tool.
Singh, T., and Hill, M. E. 2003. "Consumer Privacy and the Internet in Europe: A View from Germany," *Journal of Consumer Marketing* (20:7), pp. 634–651.
Söllner, M., Hoffmann, A., and Leimeister, J. M. 2016. "Why Different Trust Relationships Matter for Information Systems Users," *European Journal of Information Systems* (25:3), pp. 274–287.
Spiekermann, S. 2005. "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), pp. 74–83.
The Tor Project. 2018. "Tor." (https://www.torproject.org, accessed February 20, 2018).
Venkatesh, V., and Davis, F. D. 2000. "A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Studies," *Management Science* (46:2), pp. 186–205.
Venkatesh, V., Thong, J., and Xu, X. 2012. "Consumer Acceptance and User of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology," *MIS Quarterly* (36:1), pp. 157–178.