Why Do People Pay for Privacy-Enhancing Technologies? The Case of Tor and JonDonym

David Harborth, Xinyuan Cai, Sebastian Pape

Why Do People Pay for Privacy-Enhancing Technologies? The Case of Tor and JonDonym

David Harborth [0000−0001−9554−7567], Xinyuan Cai and Sebastian Pape [0000−0002−0893−7856]

Chair of Mobile Business and Multilateral Security, Goethe University Frankfurt, Frankfurt am Main, Germany

Abstract. Today's environment of data-driven business models relies heavily on collecting as much personal data as possible. One way to prevent this extensive collection, is to use privacy-enhancing technologies (PETs). However, until now, PETs did not succeed in larger consumer markets. In addition, there is a lot of research determining the technical properties of PETs, i.e. for Tor, but the use behavior of the users and, especially, their attitude towards spending money for such services is rarely considered. Yet, determining factors which lead to an increased willingness to pay (WTP) for privacy is an important step to establish economically sustainable PETs. We argue that the lack of WTP for privacy is one of the most important reasons for the non-existence of large players engaging in the offering of a PET. The relative success of services like Tor corroborates this claim since this is a service without any monetary costs attached. Thus, we empirically investigate the drivers of active users' WTP of a commercial PET - JonDonym - and compare them with the respective results for a donation-based service - Tor. Furthermore, we provide recommendations for the design of tariff schemes for commercial PETs.

Keywords: Privacy, Privacy-Enhancing Technologies, Pricing, Willingness to Pay, Tor, JonDonym.

1 Introduction

Perry Barlow 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" [1]. One of the reasons for surveilling users is a rising economic interest in the internet [2]. 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 [3]. Examples of PETs include services which allow anonymous communication, such as Tor [4] or JonDonym [5]. There has been lots of research on Tor and JonDonym [6, 7], but the large majority of it is of technical nature and does not consider the user. However, the number of users if 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 cause an action [8], thus a larger anonymity set may make it more difficult for an attacker to identify the sender or receiver of a message.

In the end, the sustainability of a service not only depends on the number of active users but also on a company or organization with the intention of running the service. One intention certainly is a well working business model. As a consequence, it is crucial to not only learn about the users' intention to use a PET, but also to understand the users' willingness to pay (WTP) for a service. Determining factors to understand the users' WTP along with a suitable tariff structure is the key step to establish economically sustainable services for privacy. The current market for PET providers is rather small, some say the market even fails [9]. We argue that the lack of WTP for privacy is one of the most important reasons for the non-existence of large players engaging in the offering of a PET. Earlier research on WTP often works with hypothetical scenarios (e.g. with conjoint-analyses) and concludes that users are not willing to pay for their privacy [10, 11]. We tackle the issue based on actual user experiences and behaviors and enhance the past research by analyzing two existing PETs with active users, with some of them already paying or donating for the service. Tor and JonDonym are comparable with respect to their functionality and partially with respect to the users' perceptions about them. However, they differ in their business model and organizational structure. Therefore, we investigate the two research questions:

RQ1: Which factors influence the willingness to pay for PETs?
RQ2: What are preferred tariff options of active users of a commercial PET?

The remainder of the paper is structured as follows: Section II briefly introduces the anonymization services Tor and JonDonym and lists related work on PETs and users' willingness to pay. In Section III, we present the research hypotheses and describe the questionnaire and the data collection process. We present the results of our empirical research in Section IV and discuss the results and conclude the paper in Section V.

2 Theoretical 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" [12]. In the following sections, we describe Tor and JonDonym as well as related work with respect to WTP for privacy.

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 / receiver's internet protocol (ip)

address) from passive network observers. Low latency anonymity services can be used for interactive services such as messengers. Due to network overheads this still leads to increased latency which was evaluated by Fabian et al. [13] 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 chosen traffic routes should be difficult for an adversary to observe, which means that 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, 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 [14] and decide to restrict users from the same origin. Restrictions range from outright rejection to limiting the users' access to a subset of the services functionality or imposing hurdles such as CAPTCHA-solving [15]. 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 technically different, 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 active users [4]. 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.

From a research perspective, there are some papers about JonDonym, e.g. a user study on user characteristics of privacy services [16]. Yet, the majority of work is about Tor. Most of the work is technical [6], e.g. on improvements such as relieved network congestion, improved router selection, enhanced scalability or reduced communication/computational cost of circuit construction [17]. There is also lots of work about the security respectively anonymity properties [18, 19] and traffic correlation [20].

2.2 Related Work

Previous non-technical work on PETs mainly considers usability studies and does not primarily focus on WTP. For example, Lee et al. [21] assess the usability of the Tor

Launcher and propose recommendations to overcome the found usability issues. Further research suggests zero-effort privacy [22, 23] by improving the usability of the service. In quantitative studies, we already investigated privacy concerns and trust on JonDonym [24] and Tor [25, 26] based on Internet users' information privacy concerns (IUIPC) [27] and could extent the causal model by "trust in the service" which plays a crucial role for the two PETs. Some experiments suggest that users are not willing to pay for their privacy [10, 11]. In contrast to these experiments, we surveyed actual users – some of them already paying or donating for the service. Grossklags find contradicting behavior of users when it comes to WTP to protect information and "willingness to accept" compensation for revealing information [28]. Further work covers selling personal data [29, 30] e.g. on data markets [31] or experiments on the value of privacy [32]. Some work tries to explain the privacy paradox with economic models [33] or discusses the right of the users to know the value of their data [34]. However, all of these are focused on the value of certain data or privacy and not on the users' WTP for privacy. Cranor et al. investigate how actual users use their privacy preferences tool [35]. Spiekermann investigate the traits and views of actual users of the predecessor of JonDonym, AN.ON/JAP, a free anonymity service [16]. However, since the tools were free, none of them investigated the users' WTP. Following a more high-level view, some research addresses the markets for PETs. Federrath claims that there is a market for PETs but they have to consider law enforcement functionality [36]. Rossnagel analyzes PET markets based on diffusion of innovations theory about anonymity services [9] and concludes a market failure. Schomakers et al. do a cluster analysis of users and find three groups with different attitudes towards privacy and argue that each of the groups need distinct tools [37]. In the same line, further research concludes that one should focus on specific subgroups for the adoption of Tor [38]. Following a market perspective, Boehme et al. analyze the condition under which it is profitable for sellers in e-commerce environments to support PETs, assuming that without PETs they could increase their profit with price discrimination [39].

3 Methodology

In this section we present the research hypotheses, 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 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.

The statistical analysis of the research data is conducted with the open-source software R. First of all, we focus solely on JonDonym and compare the differences of average preferences for alternative tariff schemes. Thereby, we differentiate between participants stating to use JonDonym in the free of charge option those stating to use it with one of the available premium tariffs. Due to non-normality of the data, we use the non-parametric test Wilcoxon rank sum test to determine whether preferences for newly

designed tariffs differ from each other among different types of users. We designed these new tariffs in collaboration with the chief executive of the JonDos GmbH in order to provide realistic pricing schemes which are economically viable and sustainable for the company. We used the paired Wilcoxon test to determine whether users' preferences for one tariff are statistically significantly different from the other tariffs. The Wilcoxon rank sum test is also called Mann-Whitney-U-Test. It is a nonparametric test of the null hypothesis that the mean of one sample will be different from the mean from a second sample. The paired Wilcoxon test is also called the Wilcoxon signed-rank test which is a similar nonparametric test used for dependent samples [40, 41]. In order to illustrate the difference in preferences among two types of users, i.e. free users and premium users, we use boxplots to visualize the descriptive statistics of the two samples [42]. A boxplot is a method for graphically depicting groups of numerical data through their quartiles. Boxplots are non-parametric. They display variation in samples of a statistical population without making any assumptions of the underlying statistical distribution. The upper line of the box is the first quartile, the band inside the box is the second quartile (the median) and the bottom line of the box is the third quartile.

3.1 Research Model and Hypotheses for the Logistic Regression Model

As a last step, we conduct a logistic regression to find out which factors influence users' willingness to pay for privacy (in our case willingness to pay for JonDonym and willingness to donate to Tor). We used the logistics regression to build the model because our dependent variable is a binary variable. A linear regression is not an appropriate model here due to the violation of the assumption that the dependent variable (WTP) is continuous, with errors which are normally distributed [43]. The probit regression is also not suitable because it assumes that our dependent variable is not normally distributed. Willingness to pay for JonDonym is defined as the binary classification of JonDonym users' actual behavior.

$$willingness\ to\ pay = \begin{cases} 0, if\ the\ respondent\ uses\ a\ free\ tariff \\ 1, if\ the\ respondent\ uses\ a\ premium\ tariff \end{cases} (1)$$

Accordingly, willingness to donate is defined as the binary classification of Tor users' actual behavior.

$$willingness\ to\ donate = \begin{cases} 0, if\ the\ respondent\ has\ never\ donated \\ 1, if\ the\ respondent \text{ has donated} \end{cases} (2)$$

The independent variables are risk propensity (RP), frequency of improper invasion of privacy (VIC), trusting beliefs in online companies (TRUST), trusting beliefs in JonDonym ($TRUST_{PET}$) and knowing of Tor / JonDonym (TOR / JD) or not. Thus, our research model is as follows:

$$WTP/WTD_i = \beta_0 + \beta_1 RP_i + \beta_2 VIC_i + \beta_3 TRUST_i + \beta_4 TRUST_{PET,i} + \beta_5 TOR/JD_i + \varepsilon_i \quad (3)$$

Risk propensity measures the risk aversion of the individual, i.e. the higher the measure, the more risk-averse the individual [44]. Literature finds that a risk aversion can act as a driver to protect an individual's privacy [45]. Thus, we hypothesize:

H1: Risk propensity (RP) has a positive effect on the likelihood of paying or donating for PETs.

Privacy victim (VIC) measures how often individuals experienced a perceived improper invasion in their privacy [27]. Results of past research dealing with perceived bad experiences with privacy indicate that such experiences can cause individuals to protect their privacy to a larger extent [46]. Thus, we hypothesize:

H2: The more frequent users felt that they were a victim of an improper breach of their privacy, the more likely they are to pay or donate for PETs.

The construct *trust in online companies* assesses individuals trust in online companies with respect to handling their personal data [27]. Results in the literature suggest that a higher trust in online companies has a positive effect on the willingness to disclose personal information. Following this finding, we argue that users who have a higher level of trust in online companies, are less likely to spend money for protecting their privacy. Therefore, we hypothesize:

H3: The more users trust online companies with handling their personal data, the less likely they are to pay or donate for PETs.

Trust in JonDonym / Tor is adapted from Pavlou [47]. Trust can refer to the technology (in our case PETs (Tor and JonDonym)) itself as well as to the service provider. Since the non-profit organization of Tor evolved around the service itself [4], 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 [24–26, 47]. In line with these results, we argue that a higher level of trust in the PET increases the likelihood to spend money for it. Thus, we hypothesize:

H4: The more users trust the PET, the more likely they are to pay or donate for it.

Lastly, we included a question about whether users of Tor /JonDonym know JonDonym / Tor. We included this question due to previous findings about a substituting effect of Tor with regard to the WTP for JonDonym [48]. Users of JonDonym partially stated that they would only spend money for a premium tariff, if Tor was not existent. Thus, we wanted to include this factor as a control variable in our analysis and hypothesize:

H5: The likelihood of JonDonym users to pay for a premium tariff decreases, if they are aware of Tor (we do not expect a similar effect for Tor users).

3.2 Data Collection

We conducted the studies with German and English-speaking users of Tor and JonDonym. For each service, we administered two questionnaires. Partially, items for the German questionnaire had to be translated since some constructs are adapted from

the 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 [49]. The items for all analyses can be found in the appendix.
We installed the surveys on a university server and managed it with the survey software LimeSurvey (version 2.72.6) [50]. For Tor, we distributed the links to the English and German version over multiple channels on the internet. An overview of every distribution channel can be found in an earlier paper based on the same dataset [26]. In sum, 314 participants started the questionnaire (245 English version, 40 English version posted in hidden service forums, 29 German version). Of those 314 approached participants, 135 (105 English version, 13 English version posted in hidden service forums, 17 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. 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. In sum, 416 participants started the questionnaire (173 English version, 243 German version). Of those 416 approached participants, 141 (53 English version, 88 German version) remained after deleting unfinished sets and all participants who answered a test question incorrectly.

4 Results

We present the results of our empirical analyses in this section. In the first part, we discuss the analysis of the current tariff structures (JonDonym) and donation statistics (Tor). Furthermore, we assess preferences of JonDonym users regarding new alternative tariff schemes. In the second part, we show the results of the logistic regression model with the factors influencing the willingness to pay (JonDonym) / to donate (Tor).

4.1 Tariff Analysis for JonDonym

Among the 141 JonDonym users in of our survey, 85 users use a free tariff. 56 users are using JonDonym with a paid tariff. Among the 124 Tor users of our survey, 93 of them have never donated to Tor. Among donating users, the amounts of donation are arbitrary. The payment structure of JonDonym and descriptive statistics for the donations to Tor are shown in Table 1. It can be seen that roughly 1/3 of the participants spend money for JonDonym (25%) and Tor (39.72%). To analyze potential tariff optimizations for JonDonym, we asked about users' preferences for three general tariff structures, namely a high-data-volume tariff (TP1), a low-price tariff (TP2) and a low-anonymity tariff (TP3). In addition, we designed five new tariffs. TRN4 is the tariff

with the lowest data volume per month and TRN5 is the tariff with highest data volume per month. The specific wording of the tariff options can be found in the appendix.

Table 1. Tariff and donation statistics of JonDonym and Tor users

JonDonym		Tor	
Tariff option	N=141	Tariff option	N=124
Free of charge option	85	No donation	93
Volume-M (1500 MB / 12 months 10€)	28	Donation	31
Volume-L (5000 MB / 24 months 30€)	19	Min. donation	0.00
Flat-M (monthly 2GB / 6 months / 50€)	5	Median donation	100.00
Flat-L (monthly 5GB / 6 months / 100€)	4	Mean donation	301.40
Volume-S (650 MB / 6 months 5€)	0	Max. donation	4500.00

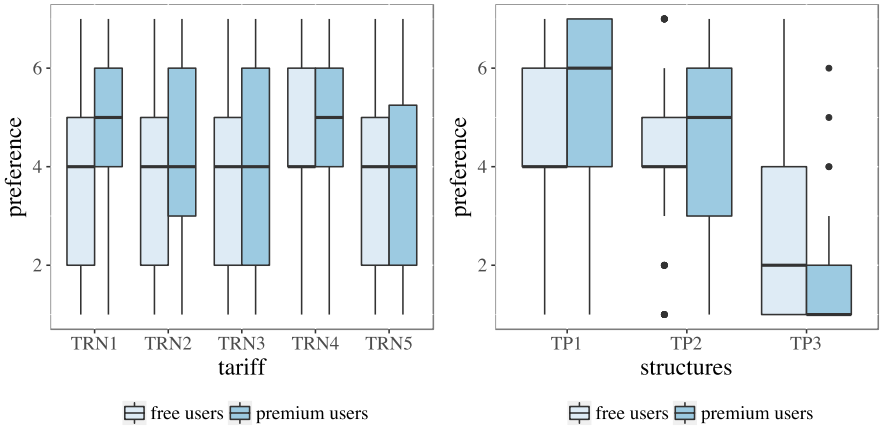

Figure 1. Users' preference for alternative tariff structures (left side) and users' preferences for tariff structures (right side), free users=85, premium users=56

Figure 1 shows the boxplots for the preferences for the five new tariff options (TRN) differentiated between free and premium users as well as three alternative tariff structures (TP). The median preferences of free users for the five tariffs are neutral (preference = 4). However, the mean preference of free users for TRN4 is slightly higher compared to the other options. In comparison, premium users have a higher preference for TRN1 and TRN4. In a next step, we analyze whether the differences illustrated with the boxplots between options for the different groups (full sample, premium users, free users) are statistically significant (Table 2). Our results indicate that the whole sample of users shows the highest preference for TRN4 and the second highest preference for TRN1. The remaining tariffs, i.e. TRN2, TRN3 and TRN5 are favored least of all. However, this contradicts with the conclusion that the total users show the highest preference for TP1. Thus, it makes sense to split the sample and look at free and premium users. Premium users show the highest preference for TRN1 and TRN4, the second highest preference for TRN2 and TRN3, and the least preference for TRN5. Thus, they show a higher preference for 100 GB tariffs. This is in line with the

conclusion that premium users have the highest preference for TP1. Free users show a neutral preference for all five tariffs except for TRN4 (slightly higher).

Table 2. Paired Wilcoxon tests for the five new tariffs and three tariff structures

New tariffs / structures		$reject\ H_0$:X=Y	$reject\ H_0$:X=Y	$reject\ H_0$: X = Y
X	Y	N=141 Total users	N=56 Premium users	N=85 Free users
TRN1	TRN2	Yes*	Yes**	No
TRN1	TRN3	Yes**	Yes*	No
TRN1	TRN4	Yes*	No	Yes***
TRN1	TRN5	Yes*	Yes**	No
TRN2	TRN3	No	No	No
TRN2	TRN4	Yes***	No	No
TRN2	TRN5	No	No	No
TRN3	TRN4	Yes***	Yes*	Yes**
TRN3	TRN5	No	No	No
TP1	TP2	Yes*	Yes ***	No
TP1	TP3	Yes ***	Yes ***	Yes ***
TP2	TP3	Yes ***	Yes ***	Yes ***

**significance level of paired Wilcoxon test:* * p < 0.05, ** p < 0.01, *** p < 0.001

Table 2 also presents the results for the differences in preferences for the tariff structures (TP). The results indicate that the 141 users have a higher preference for a high-data-volume tariff compared to a low-price tariff (TP1 vs. TP2). The results are similar for the sub-group of premium users. They have the same preference order as the whole sample of users. However, free users have the same preference for TP1 and TP2.

4.2 Factors Influencing Willingness to Pay for Privacy

Before analyzing the results in detail, we have to assess whether the independent variables correlate with each other (multicollinearity), since this would negatively impact the validity of our model. We test for multicollinearity by calculating the variance inflation factor (VIF) for all independent variables. None of the variables has a VIF larger than 1.7, indicating that multicollinearity is not an issue for our sample.
The results of the logistic regression model can be seen in Table 4. We highlighted statistically significant results in bold face. For JonDonym, RP and $TRUST_{PET}$ are the only statistically significant independent variables in the model. Surprisingly, RP has a negative coefficient, indicating that more risk-averse users are less likely to choose a premium tariff for JonDonym. This empirical result is in contrast to hypothesis 1, thus we cannot confirm this hypothesis derived from results of the literature and the associated rationale. Reasons for this contradictory result can be manifold. For example, there might be unobservable variables not included in the model which impact the relationship between RP and WTP. Hypotheses 2, 3 and 5 cannot be confirmed as well due to insignificant coefficients. In contrast to this, hypothesis 4 can be confirmed. Given the average marginal effect (avg. marg. effect), our result indicates that a one unit increase in trust in JonDonym increases the likelihood of choosing a premium tariff

by 12.17%. This result is statistically significant at the 0.1% level. Hypothesis 4 can also be confirmed for the logistic regression model for Tor users with a slightly larger average marginal effect size of 12.45%. The variable VIC is statistically significant at the 1% level with a marginal effect of 5.33%. This indicates that bad experiences with privacy breaches lead to a higher probability of donating money to Tor, and thereby, supporting the Tor project financially. No other hypotheses can be confirmed for Tor.

Table 3. Results of the Logistic Regression Model

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

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

5 Discussion and Conclusion

With respect to research question 1, our results show that PET providers should focus on building a strong reputation since trust in the PET is the strongest factor influencing the probability of spending money for privacy for both, JonDonym and Tor. In addition, we can observe that Tor users are more likely to donate for the service if they were a victim of a privacy breach or violation in their past.

Our second research question is about an optimized design of tariff options for users of commercial PETs based on the case of JonDonym. Here, we can see that the results differ when looking at different groups of users, which is in line with former research [37]. Users who use JonDonym with the free option, are indifferent with respect to the newly introduced tariffs as well as the general tariff structures (high volume vs. low price vs. low anonymity). However, some of them tend to prefer the tariff option with the lowest price with an included high-speed volume of 40 GB the most. Thus, free users would prefer the cheapest tariff, if they were to decide for paying at all. Practically, this implies that commercial PET providers should try to offer options with a relatively low monetary barrier to convert as many free users as possible into paying ones. The already paying users prefer high-volume tariffs over the other options.

Limitations of this study are the following. First, our sample only includes a relatively small number of active users of both PETs. This sample size is sufficient for the sake of our statistical analyses. However, the results about the current payment and donation numbers provide only a rough idea about the actual distribution. 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 issue by gathering the data fully

anonymized. 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 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. Lastly, 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). However, we must acknowledge that demographic variables might be relevant confounders in the regression model explaining the WTP of PET users.

Future work should aim to determine the relation between paying users and the groups Schomakers et al. [37] identified. In addition, researchers can build on our results by implementing such tariff options for commercial PET services in practice and investigate whether users are more prone to spend money for their privacy protection. Furthermore, it is relevant for commercial PET providers to differentiate themselves against free competitors as Tor in our example. This can be done by providing a higher level of usability in terms of ease of use, performance and compatibility with other applications [25, 48]. If commercial PET providers cannot create a unique selling point (USP) compared to free services, it is very unlikely that they establish a successful monetarization strategy in the market. Therefore, it is necessary to investigate how a USP for a commercial PET provider can look like and assess it in the field with active users of existing PETs as well as non-users.

References

1. Ball, J.: Hacktivists in the frontline battle for the internet, https://www.theguardian.com/technology/2012/apr/20/hacktivists-battle-internet.
2. Bédard, M.: The underestimated economic benefits of the internet. In: Regulation series, The Montreal Economic Institute (2016).
3. van Blarkom, G.W., Borking, J.J., Olk, J.G.E.: "PET". Handbook of Privacy and Privacy-Enhancing Technologies. (2003).
4. The Tor Project: Tor, https://www.torproject.org.
5. JonDos Gmbh: Official Homepage of JonDonym, https://www.anonym-surfen.de.
6. Saleh, S., Qadir, J., Ilyas, M.U.: Shedding light on the dark corners of the internet: A survey of tor research. J. Netw. Comput. Appl. 114, 1–28 (2018).
7. Montieri, A., Ciuonzo, D., Aceto, G., Pescapé, A.: Anonymity services Tor, I2P, JonDonym: Classifying in the dark. In: Int. Teletraffic Congress. pp. 81–89 (2017).
8. Pfitzmann, A., Hansen, M.: A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management. Tech. Univ. Dresden. 1–98 (2010).
9. Rossnagel, H.: The market failure of anonymity services. Lect. Notes Comput. Sci. (incl. Subser. Lect. Notes AI Lect. Notes Bioinformatics). 6033 LNCS, 340–354 (2010).
10. Grossklags, J., Acquisti, A.: When 25 Cents is Too Much: An Experiment on

Willingness-To-Sell and Willingness-To-Protect Personal Information. In: WEIS (2007).
11. Beresford, A.R., Kübler, D., Preibusch, S.: Unwillingness to pay for privacy: A field experiment. Econ. Lett. 117, 25–27 (2012).
12. Borking, J.J., Raab, C.: Laws, PETs and Other Technologies for Privacy Protection. J. Information, Law Technol. 1, 1–14 (2001).
13. Fabian, B., Goertz, F., Kunz, S., Müller, S., Nitzsche, M.: Privately Waiting – A Usability Analysis of the Tor Anonymity Network. In: AMCIS Proceedings (2010).
14. Singh, R., Nithyanand, R., Afroz, S., Pearce, P., Tschantz, M.C., Gill, P., Paxson, V.: Characterizing the nature and dynamics of Tor exit blocking. In: 26th USENIX Security Symposium (USENIX Security). Vancouver, BC. pp. 325–341 (2017).
15. Chirgwin, R.: CloudFlare shows Tor users the way out of CAPTCHA hell, https://www.theregister.co.uk/2016/10/05/cloudflare_tor/.
16. Spiekermann, S.: The Desire for Privacy: Insights into the Views and Nature of the Early Adopters of Privacy Services. Int. J. Technol. Hum. Interact. 1, 74–83 (2005).
17. Alsabah, M., Goldberg, I.: Performance and security improvements for tor: A survey. ACM Comput. Surv. 49, (2016).
18. Koch, R., Golling, M., Rodosek, G.D.: How anonymous is the tor network? A long-term black-box investigation. Computer (Long. Beach. Calif). 49, 42–49 (2016).
19. Juarez, M., Elahi, T., Jansen, R., Diaz, C., Galvez, R., Wright, M.: Poster: Fingerprinting hidden service circuits from a tor middle relay. In: Proceedings of IEEE S&P (2017).
20. Johnson, A., Wacek, C., Jansen, R., Sherr, M., Syverson, P.: Users get routed: Traffic correlation on tor by realistic adversaries. In: ACM CCS. pp. 337–348 (2013).
21. Lee, L., Fifield, D., Malkin, N., Iyer, G., Egelman, S., Wagner, D.: A Usability Evaluation of Tor Launcher. Proc. Priv. Enhancing Technol. 90–109 (2017).
22. Herrmann, D., Lindemann, J., Zimmer, E., Federrath, H.: Anonymity Online for Everyone: What is missing for zero-effort privacy on the Internet? In: International Workshop on Open Problems in Network Security. pp. 82–94 (2015).
23. Harborth, D., Herrmann, D., Köpsell, S., Pape, S., Roth, C., Federrath, H., Kesdogan, D., Rannenberg, K.: Integrating Privacy-Enhancing Technologies into the Internet Infrastructure. arXiv Prepr. arXiv1711.07220. (2017).
24. Harborth, D., Pape, S.: JonDonym Users' Information Privacy Concerns. In: Janczewski, L. and Kutyłowski, M. (eds.) ICT Systems Security and Privacy Protection. IFIP SEC 2018. pp. 1–14. Springer, Cham, Poznan, Poland (2018).
25. Harborth, D., Pape, S.: Examining Technology Use Factors of Privacy-Enhancing Technologies: The Role of Perceived Anonymity and Trust. In: Twenty-fourth Americas Conference on Information Systems. New Orleans, USA (2018).
26. Harborth, D., Pape, S.: 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 Proceedings. Hawaii, US (2019).
27. Malhotra, N.K., Kim, S.S., Agarwal, J.: Internet users' information privacy concerns: The construct, the scale, and a causal model. Inf. Syst. Res. 15, 336–355 (2004).
28. Grossklags, J.: Experimental Economics and Experimental Computer Science: A Survey. In: Workshop on Experimental Computer Science - ExpCS '07 (2007).
29. Acquisti, A.: The economics of personal data and the economics of privacy. Texte La

Conférence Donnée En Décembre. 1–24 (2010).
30. Benndorf, V., Normann, H.T.: The Willingness to Sell Personal Data. Scand. J. Econ. 120, 1260–1278 (2018).
31. Li, C., Li, D.Y., Miklau, G., Suciu, D.A.N.: A Theory of Pricing Private Data. ACM Trans. Database Syst. 39, 34:1-34:27 (2014).
32. Preibusch, S.: The value of privacy in web search. In: WEIS (2013).
33. Cofone, I.N.: The Value of Privacy: Keeping the Money Where the Mouth is. 14th Annu. Work. Econ. Inf. Secur. 1–31 (2015).
34. Malgieri, G., Custers, B.: Pricing privacy - the right to know the value of your personal data. Comput. Law Secur. Rev. (2017).
35. Cranor, L.F., Arjula, M., Guduru, P.: Use of a P3P user agent by early adopters. Proceeding ACM Work. Priv. Electron. Soc. - WPES '02. 1–10 (2002).
36. Federrath, H.: Privacy Enhanced Technologies: Methods – Markets – Misuse. In: International Conference on Trust, Privacy and Security in Digital Business (2005).
37. Schomakers, E.M., Lidynia, C., Vervier, L., Ziefle, M.: Of Guardians, Cynics, and Pragmatists - A Typology of Privacy Concerns and Behavior. In: IoTBDS. pp. 153–163 (2018).
38. Roßnagel, H., Zibuschka, J., Pimenides, L., Deselaers, T.: Facilitating the adoption of Tor by focusing on a promising target group. In: NordSec. pp. 15–27 (2009).
39. Böhme, R., Koble, S.: On the Viability of Privacy-Enhancing Technologies in a Self-Regulated Business-to-Consumer Market : Will Privacy Remain a Luxury Good? Dresden (2007).
40. Wilcoxon, F.: Individual comparisons by ranking methods. Biometrics Bull. 1, 80–83 (1945).
41. Mann, H.B., Whitney, D.R.: On a Test of Whether one of Two Random Variables is Stochastically Larger than the Other. Ann. Math. Stat. 18, 50 (1947).
42. Benjamini, Y.: Opening the Box of a Boxplot. Am. Stat. 42, 257–262 (1988).
43. McKelvey, D., Zavorina, W.: A Statistical Model for the Analysis of Ordinal Level Dependent Variables. J. Math. Sociol. 4, 103–120 (1975).
44. Donthu, N., Gilliland, D.: Observations: The infomercial shopper. J. Advert. Res. 36, 69–76 (1996).
45. Frik, A., Gaudeul, A.: The Relation between Privacy Protection and Risk Attitudes, with a New Experimental Method to Elicit the Implicit Monetary Value of Privacy. CEGE Discuss. Pap. Number 296, SSRN https//papers.ssrn.com/abstract=2874202. (2016).
46. Christofides, E., Muise, A., Desmarais, S.: Risky Disclosures on Facebook: The Effect of Having a Bad Experience on Online Behavior. J. Adolesc. Res. 27, 714–731 (2012).
47. Pavlou, P.A.: Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model. Int. J. Elect. Commer. 7, 101–134 (2003).
48. Harborth, D., Pape, S.: Explaining Technology Use Behaviors of Privacy-Enhancing Technologies: The Case of Tor and JonDonym. In: Submitted to: IEEE European Symposium on Security and Privacy (EuroS&P 2019) (2019).
49. Harborth, D., Pape, S.: German Translation of the Concerns for Information Privacy (CFIP) Construct. Available at SSRN: https://ssrn.com/abstract=3112207 (2018).
50. Schmitz, C.: LimeSurvey Project Team, http://www.limesurvey.org.

All websites were last accessed December 13, 2018.

Appendix - Questionnaire

A. Constructs and Questions for both PETs

Risk Propensity (RP)	**Trust in the PET (JonDonym / Tor) (TRUST$_{PET}$)**
1. I would rather be safe than sorry.	1. JonDonym / Tor is trustworthy.
2. I am cautious in trying new/ different products.	2. JonDonym / Tor keeps promises and commitments.
3. I avoid risky things.	3. I trust JonDonym / Tor because they keep my best interests in mind.

Trust in Online Companies (TRUST)

1. Online companies are trustworthy in handling information.
2. Online companies tell the truth and fulfill promises related to information provided by me.
3. I trust that online companies would keep my best interests in mind when dealing with information.
4. Online companies are in general predictable and consistent regarding the usage of information.
5. Online companies are always honest with customers when it comes to using the provided information.

Privacy Victim (VIC)

How frequently have you personally been the victim of what you felt was an improper invasion of privacy? (7-point frequency scale from "Never" to "Very frequently")

Knowledge about Tor (TOR) / JonDonym (JD)

Do you know the anonymization service Tor / JonDonym? (Yes / No)

B. Specific Questions for JonDonym

Current Tariff - Please choose your current tariff of JonDonym.

1. Free of charge option	4. Volume-S (650 MB / 6 months 5€)
2. Flat-M (monthly 2GB / 6 months / 50€)	5. Volume-M (1500 MB / 12 months 10€)
3. Flat-L (monthly 5GB / 6 months / 100€)	6. Volume-L (5000 MB / 24 months 30€)

Tariff Preference (TP)

1. I would use JD regularly with a data volume ten times higher than before (at the same price).
2. If the price decreased by half, I would use JonDonym regularly.
3. I would perceive a service with a lower anonymization level for half the price more attractive than JonDonym.

Tariff New (TRN)

1. Monthly 100 GB with a duration of 12 months for 100€ (total price)
2. Monthly 100 GB with a duration of 3 months for 30€ (total price)
3. Monthly 100 GB with a duration of 12 months for 10€ per month
4. Monthly 40 GB with a duration of 3 months for 5€ per month
5. Monthly 200 GB with a duration of 12 months for 15€ per month

C. Specific Questions for Tor

Donation to Tor

Did you ever donate money to the Tor project? (Yes / No)

Donation Amount

How much money did you donate to the Tor project? (open field with number only)

If not stated otherwise, constructs are measured based on a 7-point Likert scale ranging from strongly disagree to strongly agree.