User Aspects of Privacy-Enhancing Technologies
Insights from the Project "AN.ON-Next"

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

GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung

mobile business

Agenda

1. Introduction

2. Study I: Technology Acceptance Factors of PETs
   Harborth, D., Pape, S., & Rannenberg, K. (2020). Explaining Technology Use Behaviors of Privacy-Enhancing Technologies: The Case of Tor and JonDonym. Proceedings on Privacy Enhancing Technologies (PoPETs), 2020(2), 111–128. https://doi.org/10.2478/popets-2020-0020

3. Study II: Willingness to Pay for PETs
   Harborth, D., Cai, X., Pape, S. (2019). "Why Do People Pay for Privacy- Enhancing Technologies? The Case of Tor and JonDonym", In: 34th IFIP TC-11 SEC 2019 International Conference on Information Security and Privacy Protection (IFIP SEC). Lisbon, Portugal, DOI: 10.1007/978-3-030-22312-0_18. (Nominated for best student paper award)

4. Discussion and Conclusion

1. Introduction
Initial Situation

- Perry Barlow: "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." (Ball 2012)

- Privacy protection by law (see for example European Union with the General Data Protection Regulation GDPR)
  AND / OR
  enabling individuals to make informed decisions and use appropriate tools

→ Privacy-enhancing technologies (PETs) as a means to accomplish individual protection

Source picture: Mark Pernice for NYTimes. URL: http://www.nytimes.com/2012/01/29/opinion/sunday/in-the-gps-case-issues-of-privacy-and-technology.html?_r=0, Date Accessed 25.01.2016

1. Introduction
Definition and Motivation (I)

- PETs are "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)
- Not only primary goals from a user point of view, but also secondary goals (Cranor and Garfinkel 2008)
- PETs integrated into existing services (e.g. Privacy ABCs) vs. "standalone" PETs like Tor or JonDonym with multiple use scenarios → focus on the latter
- PETs are not well accepted among individuals
- Results of general experiments on WTP for privacy indicate that users do not want to pay for privacy (e.g. Beresford et al. 2012, Grossklags and Acquisti 2007)

1. Introduction
Definition and Motivation (II)

- PETs have specific characteristics:

1. immediate results of use not visible (a "good" PET should not change user experience) → in contrast to other systems
2. technical functioning quite complex (layman users will / cannot evaluate the services and their reliability)

→Which aspects influence your use intention?

→Would you pay for it?

1. Introduction Goals

I. Technology Acceptance Factors (TAF):

- quantitative analysis with known acceptance factors for this kind of PET
- integration of new relevant constructs for PETs, perceived anonymity and trust
- augment quantitative insights with qualitative insights

II. Willingness to pay (WTP):

- analyze tariff preferences and donation behaviors of active users of PETs
- analyze possible factors which influence the willingness to pay (WTP) for PETs

2. Study I - TAF Research Questions

Research Question 1:
Does perceived anonymity influence the behavioral intention to use a PET?

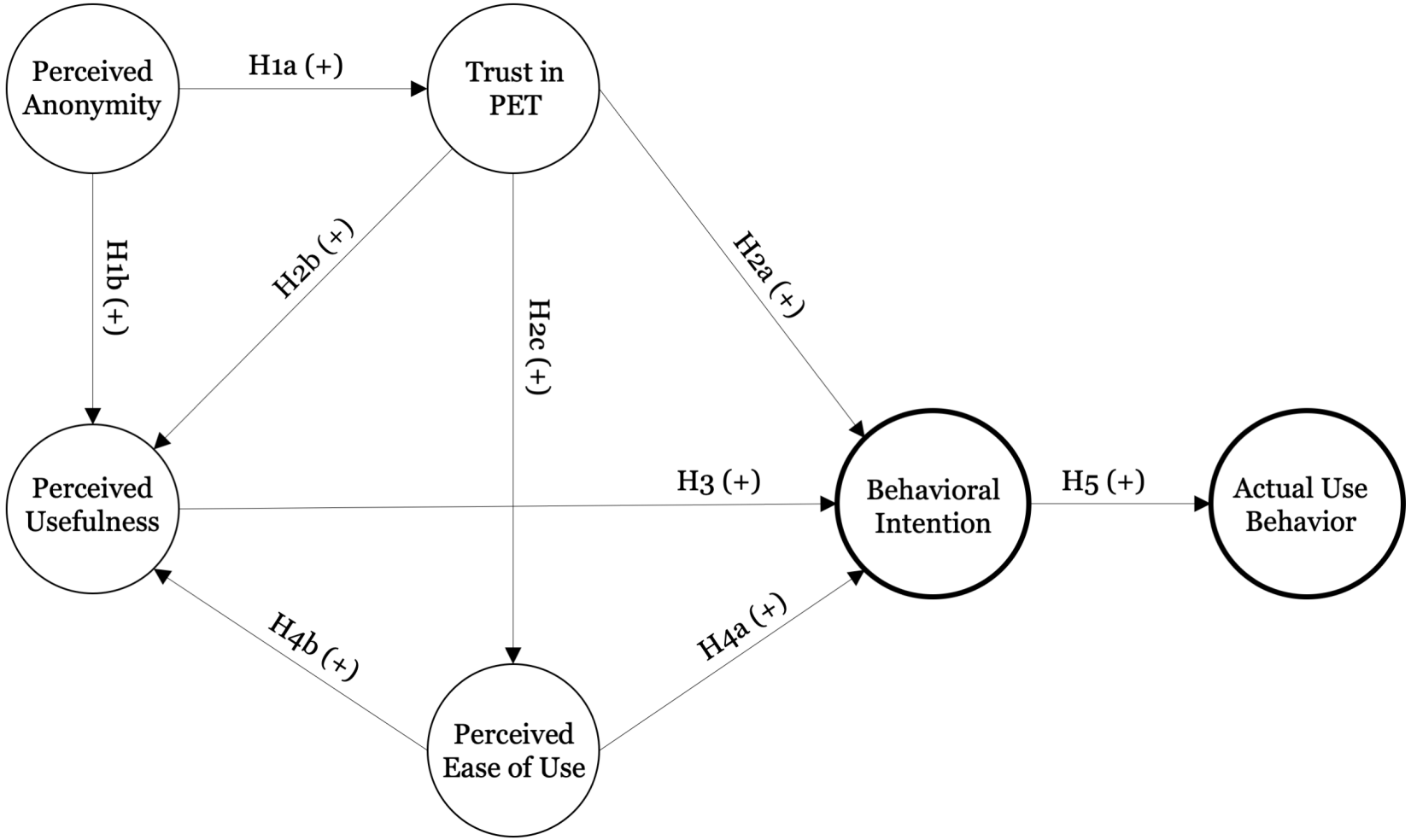
Research Question 2:
Does trust in the PET influences the behavioral intention to use it?

→Technology acceptance model as theoretical underlying (Davis 1985, 1989)

2. Study I - TAF Methodology

- Constructs adapted from existing literature: technology acceptance factors (Venkatesh and Davis 2000, Venkatesh et al. 2012), trust (Pavlou 2003) and perceived anonymity (Benenson et al. 2015)
- German and English-speaking users of JonDonym and Tor acquired via survey ad during the rollout of a new browser and on the official homepage and the Tor mailing list (+ diverse other channels to reach Tor users)
- Online survey installed on university server and managed with LimeSurvey (version 2.63.1) (Schmitz 2015)
- Constructs translated into German with two certified translators
- Active users (N=141 for JonDonym + 124 for Tor)
- Partial least squares structural equation modelling (PLS-SEM) with SmartPLS 3.2.7 (Ringle et al. 2015)

2. Study I - TAF Research Model



2. Study I - TAF
Rationale Research Hypotheses (I)

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

- Main impact of PETs (anonymity / privacy protection) is not immediately tangible for the user
  → The perception with regard to anonymity matters
- Perceived anonymity influences trust in the service, because of the natural importance of this concept for PETs
- Creating anonymity is the main purpose of the service
  → if this is perceived to be high, the perception w.r.t. to the usefulness should increase

2. Study I - TAF
Rationale Research Hypotheses (II)

	Hypothesis
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 PETs to protect the user's privacy.
H2c	Trust in PETs has a positive effect on the perceived ease of use of PETs.

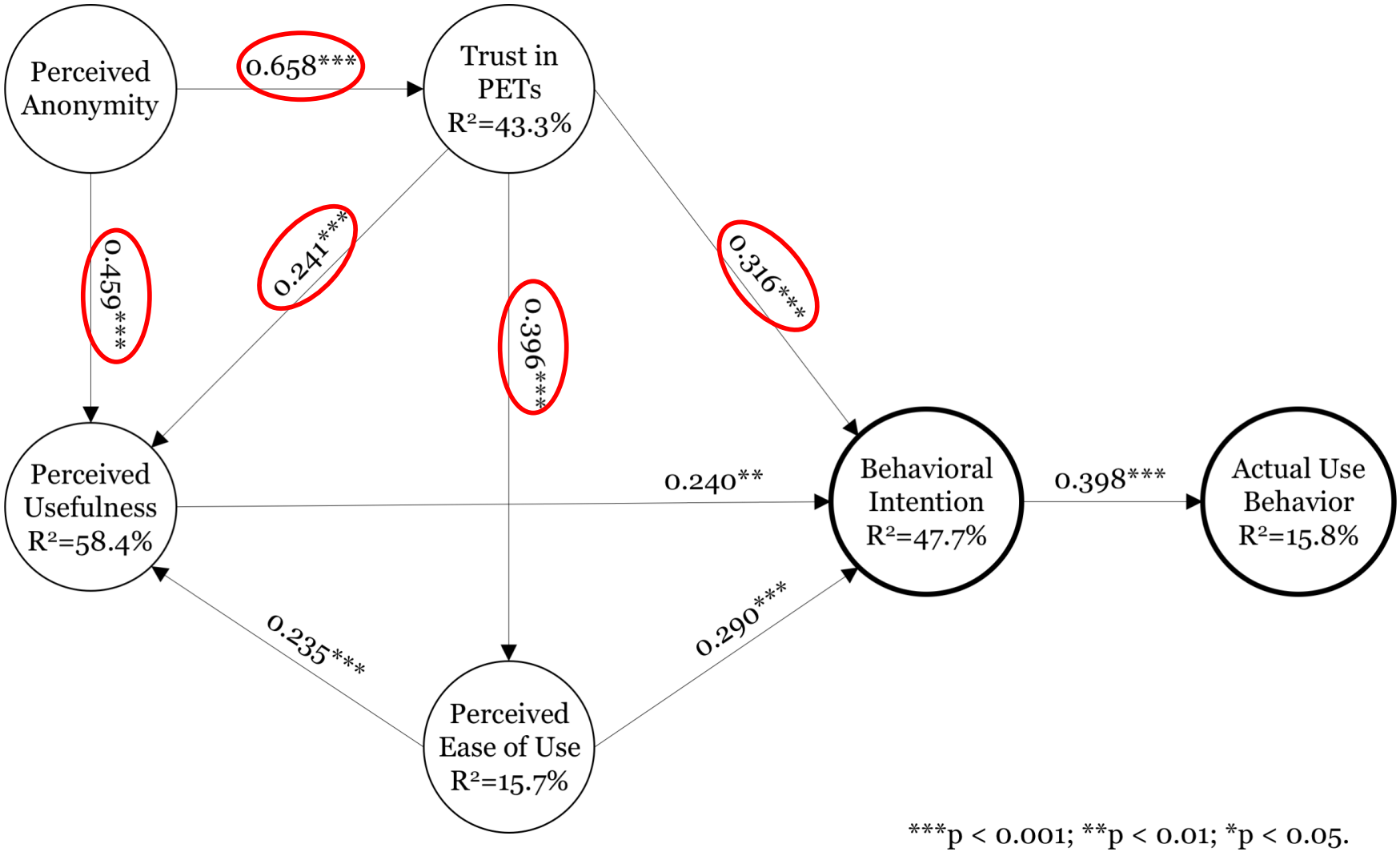
- Trust in the service enables positive attitudes and and therefore influences the intention to the PET
- User has to trust the service in order to perceive it as useful
  → if a user does not trust the PET in providing anonymity, the usefulness w.r.t. this primary goal will not be given
- Trust decreases the need to understand every detail of the technology (Chircu et al. 2000)
  → especially relevant for the case of PETs with their high level of complexity

2. Study I - TAF Measurement and Structural Model

Measurement Model Assessment	Structural Model Assessment
Internal consistency reliability ✓	Collinearity ✓
Convergent validity ✓	Significance and Relevance of Model Relationships (see next slide) ✓
Discriminant validity ✓	Predictive Relevance Q^2 ✓
Common Method Bias ✓	

- Assessments indicate valid and reliable results

2. Study I - TAF
Path Estimates and R^2-values



***p < 0.001; **p < 0.01; *p < 0.05.

2. Study I - TAF Qualitative Results

- Coding of participants' answers to open questions
  1. Do you have any concerns about using JonDonym / Tor?
  2. Under which circumstances would you choose one of the premium tariffs? (JonDonym)
  3. Which additional features would you like to have at your current tariff? (JonDonym)
     Which additional features would you like to have for Tor?
  4. Why would you recommend JonDonym / Tor?
  5. Why would you not recommend JonDonym / Tor?

2. Study I - TAF Qualitative Results

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**)

3. Study II - WTP Research Questions

Research Question 1:

What are preferred tariff options of active users of a commercial PET?

Research Question 2:

Which factors influence the willingness to pay for PETs?

3. Study II – WTP Methodology

- Constructs adapted from existing literature: Trust, privacy victim experience (Malhotra 2004), trust in the service (Pavlou 2003) and risk propensity (Donthu and Gilliland 1996)
- German and English-speaking users of Tor acquired via multiple sources (mailing lists, forums, Twitter, personal announcements at workshops)
- Constructs translated into German with two certified translators
- Online survey installed on university server and managed with LimeSurvey (version 2.63.1) (Schmitz 2015)
- Active users (Tor: N=124; JonDonym: N=141)
- Descriptive part with preferred tariffs of JonDonym users
- Logit regression model (binary dependent variable)

3. Study II - WTP Research Hypotheses

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

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.

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

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

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).

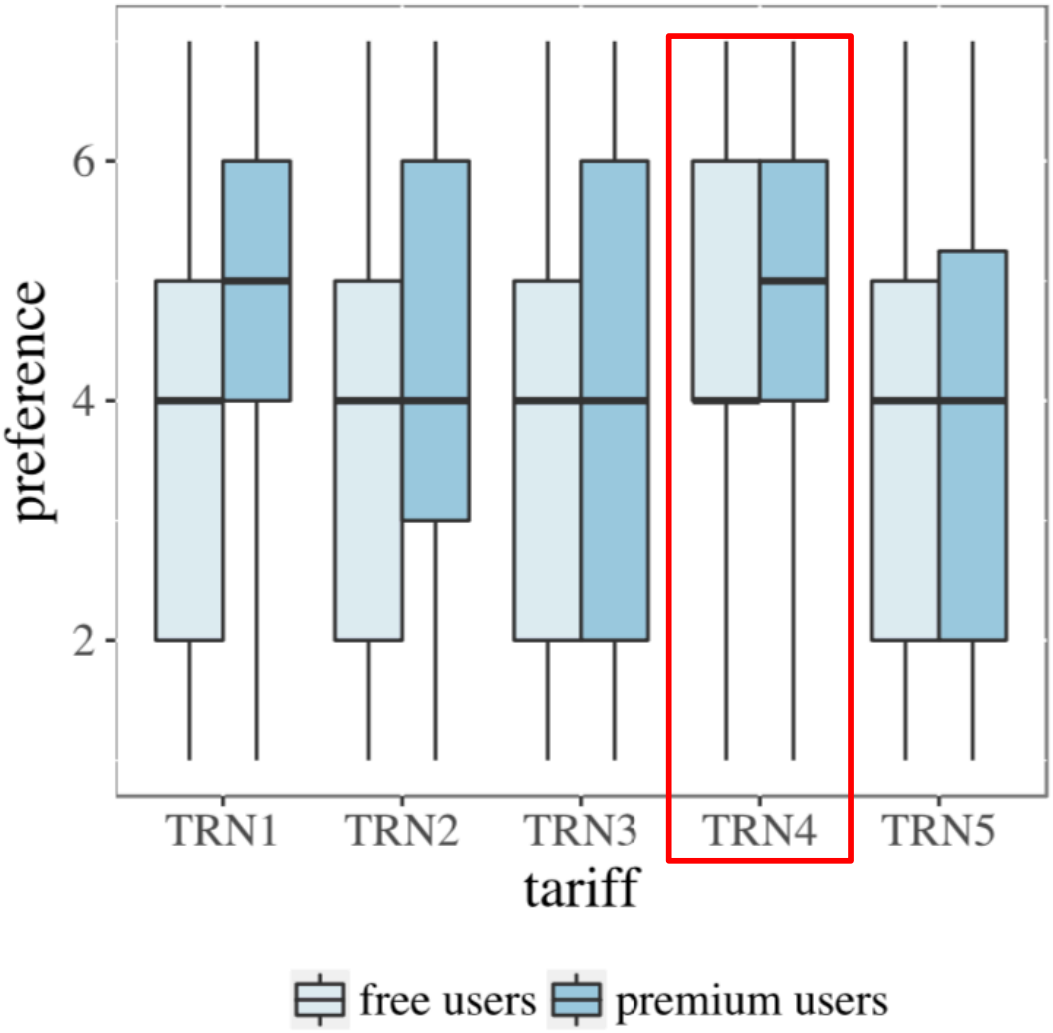
$$WTP/WTD_i = \beta_0 + \beta_1 RP_i + \beta_2 VIC_i + \beta_3 TRUST_i + \beta_4 TRUST_{PET,i} + \beta_5 TOR/JD_i + \varepsilon_i$$

3. Study II - WTP
Current Tariffs and Donations

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

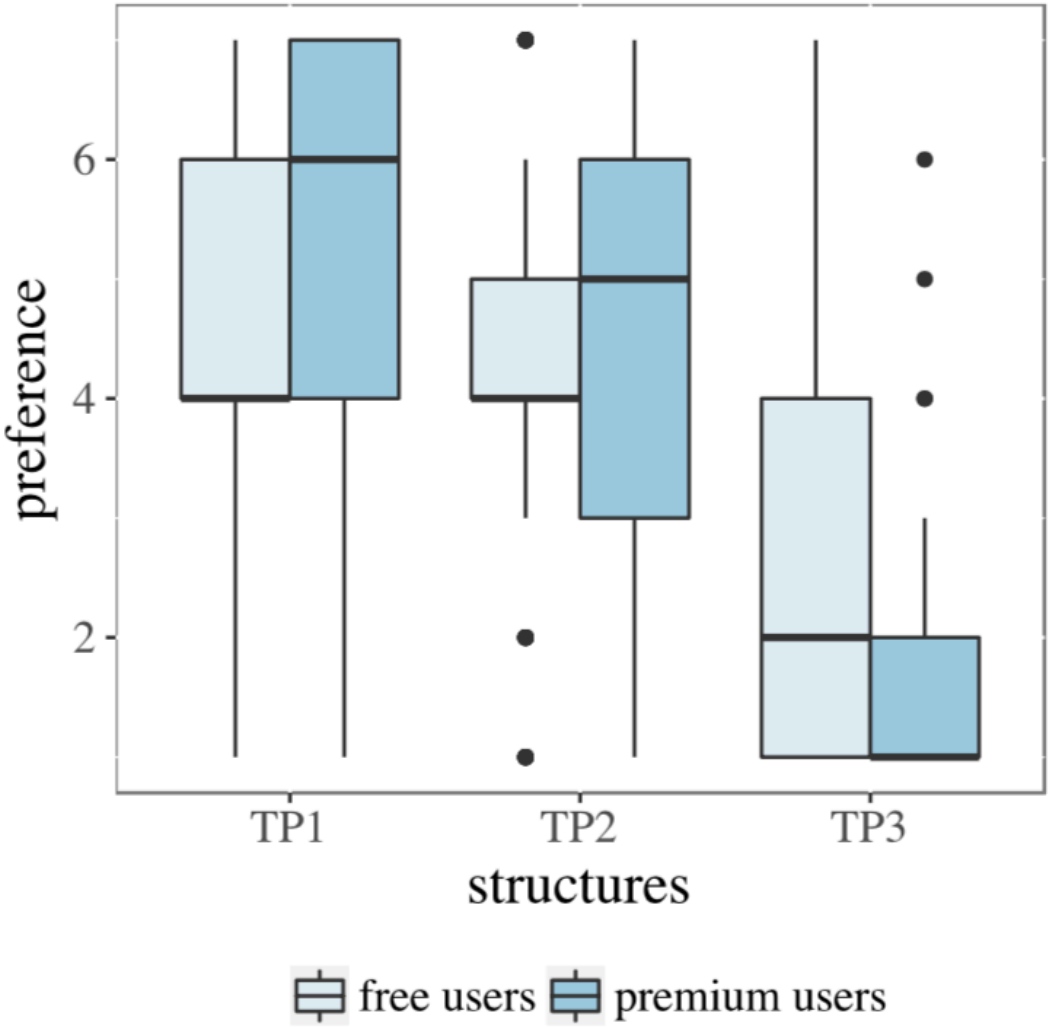
JonDonym		Tor	
Tariff option	N=141	Tariff option	N=124
Free of charge option	85	No donation	93
Volume-M (1500 MB / 12 months 10€)	28	Donation	31
Volume-L (5000 MB / 24 months 30€)	19	Min. donation	0.00
Flat-M (monthly 2GB / 6 months / 50€)	5	Median donation	100.00
Flat-L (monthly 5GB / 6 months / 100€)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

3. Study II - WTP Tariff Preferences (I)



- TRN1: 100 GB/month, 12 months, 100€ (total)
- TRN2: 100 GB/month, 3 months, 30€ (total)
- TRN3: 100 GB/month, 12 months, 10€ per month
- TRN4: 40 GB/month, 3 months, 5€ per month
- TRN5: 200 GB/month, 12 months, 15€ per month

3. Study II - WTP Tariff Preferences (II)



- TP1: Ten times higher data volume at the same price
- TP2: Price halved, same data volume
- TP3: Price halved, lower anonymity level

3. Study II - WTP Regression Results

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

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

- WTP for JonDonym influenced by $Trust_{JD}$ (+) and (surprisingly) by risk propensity (-)
- WTP for Tor influenced by prior privacy victim experiences (+) and $Trust_{Tor}$(+)

3. Study II - WTP Summary of the Results

Hypotheses	Confirm / Reject
H1: Risk Propensity positively influences the WTP	Not confirmed
H2: Prior privacy victim experiences positively influence the WTP	Confirmed for Tor (✓) Not confirmed for JD
H3: Trust Beliefs in online companies negatively influence the WTP	Not confirmed
H4: Trust in the PET positively influences the WTP	Confirmed ✓
H5: Awareness of JD users about Tor negatively influences their WTP for JD	Not confirmed

4. Discussion and Conclusion
Summary and Key Findings

- Past research on PETs mainly technical

→ successful implementation and adoption requires a profound understanding of the perceptions and behaviors of actual and non-users

1. Basic acceptance factors hold for PETs, too
2. Perceived anonymity and trust increase the explained variance in BI by approx. 11 percentage points

→ establishing PETs in the market requires a sustainable revenue model

1. Tariff preferences of JD users differ between users with the free tariff and the ones already paying for JD → convert free users with cheapest tariff
2. Trust in the PETs is the major driver for WTP
   → Reputation is key

4*. Addendum
A Few General Thoughts...

- Privacy Paradox & Privacy Calculus
- Two different paradigms/assumptions if you think about the importance people attribute to privacy and the resulting cognitive effort
- PP: low effort, people do not care
  PC: high effort, deliberate trade-off process that requires people to understand costs (privacy risks) as well as benefits (Dinev et al. 2015)

→ Researcher has to consider the assumption underlying the research

→ Causal relationships can only be seen in this *high-effort/deliberate thinking* paradigm if you do not control for biasing factors

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).
- Beresford, A.R., Kübler, D., Preibusch, S.: Unwillingness to pay for privacy: A field experiment. Econ. Lett. 117, 25–27 (2012).
- 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.
- Cranor, L. F., and Garfinkel, S. 2008. Security and Usability: Designing Secure Systems That People Can Use, Farnham: O'Reilly.
- Dinev, T., McConnell, A. R., & Smith, H. J. (2015). Research commentary—informing privacy research through information systems, psychology, and behavioral economics: thinking outside the "APCO" box. Information Systems Research, 26(4), 639-655.
- Donthu, N., and Gilliland, D. 1996. "Observations: The Infomercial Shopper," *Journal of Advertising Research* (36:April), pp. 69–76.
- 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).
- Malhotra, N. K., S. S. Kim and J. Agarwal. (2004). "Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model." Information Systems Research, 15(4), 336–355.
- 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.
- Schmitz, C. 2015. *LimeSurvey Project Team*, LimeSurvey Project Hamburg, Germany, LimeSurvey: An Open Source survey tool.

mobile business

Thank you for your attention!

Chair of Mobile Business & Multilateral Security

David Harborth
Goethe University Frankfurt
E-Mail: david.harborth@m-chair.de
WWW: www.m-chair.de