

Association for Information Systems AIS Electronic Library (AISeL)

ECIS 2011 Proceedings

European Conference on Information Systems
(ECIS)

Summer 10-6-2011

ARE YOU WILLING TO WAIT LONGER FOR INTERNET PRIVACY?

Franziska Brecht

Benjamin Fabian

Steffen Kunz

Sebastian Mueller

Follow this and additional works at: <http://aisel.aisnet.org/ecis2011>

Recommended Citation

Brecht, Franziska; Fabian, Benjamin; Kunz, Steffen; and Mueller, Sebastian, "ARE YOU WILLING TO WAIT LONGER FOR INTERNET PRIVACY?" (2011). *ECIS 2011 Proceedings*. 236.
<http://aisel.aisnet.org/ecis2011/236>

This material is brought to you by the European Conference on Information Systems (ECIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in ECIS 2011 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

ARE YOU WILLING TO WAIT LONGER FOR INTERNET PRIVACY?

Brecht, Franziska, Humboldt-Universität zu Berlin, Spandauer Str.1, 10178 Berlin, Germany, franziska.brecht@wiwi.hu-berlin.de

Fabian, Benjamin, Humboldt-Universität zu Berlin, Spandauer Str.1, 10178 Berlin, Germany, bfabian@wiwi.hu-berlin.de

Kunz, Steffen, Humboldt-Universität zu Berlin, Spandauer Str.1, 10178 Berlin, Germany, steffen.kunz@wiwi.hu-berlin.de

Mueller, Sebastian, Humboldt-Universität zu Berlin, Spandauer Str.1, 10178 Berlin, Germany, sebastian.mueller.4@hu-berlin.de

Abstract

It becomes increasingly common for governments, service providers and specialized data aggregators to systematically collect traces of personal communication on the Internet without the user's knowledge or approval. An analysis of these personal traces by data mining algorithms can reveal sensitive personal information, such as location data, behavioral patterns, or personal profiles including preferences and dislikes. Recent studies show that this information can be used for various purposes, for example by insurance companies or banks to identify potentially risky customers, by governments to observe their citizens, and also by repressive regimes to monitor political opponents. Online anonymity software, such as Tor, can help users to protect their privacy, but often comes at the prize of low usability, e.g., by causing increased latency during surfing. In this exploratory study, we determine factors that influence the usage of Internet anonymity software. In particular, we show that Internet literacy, Internet privacy awareness and Internet privacy concerns are important antecedents for determining an Internet user's intention to use anonymity software, and that Internet patience has a positive moderating effect on the intention to use anonymity software, as well as on its perceived usefulness.

Keywords: Internet Privacy and Anonymity, Internet Latency, Tolerated Waiting Time, Technology Acceptance Model, Usability of Anonymity Software, Tor, Onion Routing

1 Introduction

Internet service providers and information aggregators such as Google, Microsoft, Facebook, or Amazon, automatically collect, aggregate, and analyze personal traces of millions of Internet users for their business purposes (Krishnamurthy et al., 2007). Users often unsuspectingly reveal large amounts of personal information and interests when surfing the Web. This information can secretly be used against a user's interest to create valuable personalized profiles for advertising and direct marketing purposes, or by insurance companies and banks to avoid potentially risky customers. Similarly, personalized communication and surfing profiles can be used for governmental surveillance, especially with regard to repressive regimes to identify and prosecute their political opponents. Such abuse can restrict the freedom of speech and, in particular, restrict the access to information on the Internet (Amnesty International, 2006).

An important solution for an Internet user to mitigate threats against her privacy is to use anonymity software such as 'the onion routing' (Tor) network (Tor Project, 2010). When using Tor during surfing, application messages are not normally routed between client and server, but are forwarded through additional ephemeral paths of an overlay network, using encryption and routes that are hard to analyze for an adversary (Dingledine et al., 2004). However, the main disadvantage for the user when using anonymity software is increased latency while surfing the Web (Dingledine and Murdoch, 2009; Fabian et al., 2010). This additional latency reduces the usability and therefore possibly the usage rate of anonymity software (Dingledine and Murdoch, 2009). Since, in general, anonymity provided by Tor increases with the number of participating users, this lack of usability may cause a considerable negative impact on the overall anonymity in the Tor network.

In a previous study, we analyzed the additional technical latency caused by Tor in detail and mapped the technical latency to the tolerated waiting time (TWT) of users (Fabian et al., 2010). There, we especially focused on the work of Nah (2004) who investigated the willingness of users to wait as they are searching for information – in contrast to other studies, which focus on transactions in e-commerce. Comparing the average latency between Tor-based and direct requests, we showed that the higher latency of Tor compared to unprotected surfing can be expected to increase the cancelation rate by 74% (based on Nah's TWT measures). However, we noticed that the technical latency cannot fully explain a user's TWT. Furthermore, it remained an open question why or why not Internet users use anonymity software.

Though TWT as well as the privacy of users in the Internet are subject to a variety of studies, most of them focus on e-commerce (e.g., Dinev and Hart, 2004a; 2006), but not on information search. While the user may willingly and actively disclose personal information during commercial transactions, it is much more difficult to assess and control the disclosure of personal information in the context of information search, i.e., when surfing the Web. We therefore decided to conduct an explorative study on influence factors for the acceptance of Internet anonymity software. The research questions we address are: (i) Which factors influence a person's intention to use anonymity software? (ii) How can the diffusion of anonymity software among Internet users be increased? (iii) How long are users willing to wait when surfing the Internet with and without anonymity software? Through our findings, we intend to provide hints how to increase the dissemination of Internet anonymity software.

2 Research Model and Literature

Relevant literature for our research model on acceptance of online anonymity software originates from three different areas: (i) latency and tolerated waiting time (TWT), which was already discussed in the introduction. Further IS research literature on (ii) privacy and (iii) technology acceptance will be discussed subsequently. Table 1 gives an overview of the constructs we used in our model, including their description and a list of related constructs in literature.

Construct	Definitions	Original Construct(s)
<i>Internet Literacy</i> (IL)	... measures the extent to which an Internet user feels confident when manipulating the security and privacy configurations of Web browsers.	<i>Internet (Technical) Literacy</i> (Dinev and Hart, 2004b)
<i>Internet Privacy Awareness</i> (PA)	... measures the awareness of Internet users regarding Internet privacy.	<i>Privacy Awareness</i> (Xu et al., 2008); <i>Social Awareness</i> (Dinev and Hart, 2004b); <i>Awareness of Privacy Practices</i> (Malhotra et al., 2004)
<i>Internet Privacy Concerns</i> (PC)	... measures the perceived risk that data about the surfing behavior of users is being transmitted and abused.	<i>Perceived Privacy Concerns</i> (Dinev and Hart, 2004a) <i>Internet Privacy Concerns</i> (Dinev and Hart, 2004b, 2006); <i>Internet User's Information Privacy Concerns</i> (Malhotra et al., 2004); <i>Concerns for Information Privacy</i> (Stewart and Segars, 2002)
<i>Perceived Usefulness of Anonymity Software</i> (PU)	... measures the degree of perceived usefulness of anonymity software.	<i>Perceived Usefulness of the System</i> (Davis et al., 1989)
<i>Intention to Use Anonymity Software</i> (ItU)	... measures the behavioral intention to use anonymity software in the future.	<i>Behavioral Intention to Use</i> (Davis et al., 1989)
<i>Internet Patience</i> (IP)	... measures the importance of a fast Internet connection to a user and her overall patience when surfing the Internet.	Developed by authors

Table 1. Definitions and Origins of Constructs.

2.1 Antecedents

Internet Literacy (IL) measures the extent to which an Internet user feels confident manipulating the security and privacy configurations of Internet clients such as Web browsers. According to Dinev and Hart (2004b), IL is closely related to *computer literacy*, i.e., it is influenced by the user's computer skills, attitudes and beliefs. However, IL can be regarded as a subset of *computer literacy* focusing on Internet transactions, searching the Internet and websites, etc. Users with a high IL are aware of potential attacks such as spyware, viruses and communication tracing. Therefore, we assume (H1a) a positive relationship between IL and *Internet Privacy Awareness* (PA), i.e., if a user has good Internet knowledge, she is aware of the associated risks. Dinev and Hart (2004b) assumed a negative relationship between IL and *Internet Privacy Concerns* (PC) implying that the more a user knows about the Internet, the lower will be her concerns. We included this as hypothesis (H1b) in our model. Furthermore, we assume a positive relationship between (H1c) IL and *Perceived Usefulness of Anonymity Software* (PU) as well as (H1d) between IL and *Intention to Use Anonymity Software* (ItU). We suppose that a user with higher IL considers the usefulness of anonymity software higher and therefore has a higher intention to use it.

H1a: IL will have a positive influence on PA.

H1b: IL will have a negative influence on PC.

H1c: IL will have a positive influence on PU.

H1d: IL will have a positive influence on ItU.

Internet Privacy Awareness (PA) measures how well a user is informed about privacy practices and policies in the Internet (Xu et al., 2008). According to Xu et al. (2008) the construct *social awareness*, which was developed by Dinev and Hart (2004b), can be regarded as a predictor of PA, since it is one of the key components of *consciousness rising*. Dinev and Hart (2004b) show a positive correlation between *social awareness* and *privacy concerns*. Transferred to our focus of research, we assume (H2a) a positive relationship between PA and *Internet Privacy Concerns* (PC). In addition, we suppose a positive relationship between (H2b) PA and the *Perceived Usefulness* (PU), and (H2c) PA and *Intention to Use Anonymity Software* (ItU), because if users are more aware of the risks when using the Internet, their PU is higher and their ItU increases.

H2a: PA will have a positive influence on PC.

H2b: PA will have a positive influence on PU.

H2c: PA will have a positive influence on ItU.

The construct *Internet Privacy Concerns* (PC) measures an Internet user's concerns that data about her surfing behavior is collected and abused. Dinev and Hart (2004b) first introduced PC in order to measure the privacy concerns of individuals who use the Internet. In another study Dinev and Hart (2004a) use *perceived vulnerability* and *perceived ability to control information* as antecedents for describing *perceived privacy concerns*. The results of the exploratory factor analysis supported the authors' hypothesis that *perceived vulnerability* has a strong impact on *privacy concerns*, while their hypothesis, according to which there exists a negative relationship between *perceived ability to control information* and *privacy concerns*, was only moderately supported. This implies that the latter relationship is more complex than expected. In a later study, Dinev and Hart (2006) used the construct PC in their extended privacy calculus model, showing that PC have a negative influence on the user's *willingness to provide personal information to transact on the Internet*. In our model, we assume (H3a) a positive correlation between PC and *Intention to Use Anonymity Software* (ItU) because the higher a user's PC, the higher we expect her motivation to use anonymity software. Similar reasoning applies for the relationship between PC and *Perceived Usefulness* (PU), i.e., we assume (H3b) that PC positively influences PU.

H3a: PC will have a positive influence on ItU.

H3b: PC will have a positive influence on PU.

2.2 Technology Acceptance Model (TAM)

The construct *Perceived Usefulness of Anonymity Software* (PU) originates from the Technology Acceptance Model (TAM; Davis et al. 1989) and measures the usefulness of anonymity software in our study. According to Davis et al. (1989), *Perceived Usefulness* is defined as the potential user's subjective belief that the usage of the software will increase her performance. Other studies adapt the TAM to investigate user behavior towards so-called protective technologies (e.g. Dinev and Hu, 2006). In our case, protective technologies correspond to anonymity software and the "performance" increase would translate to the increase of anonymity and therefore privacy when surfing the Web. In accordance to the TAM (Davis et al., 1989), we assume (H4) a positive relationship between PU and *Intention to use Anonymity Software* (ItU). We applied TAM because anonymity software is currently not widely applied by Internet users and many users do not have hands-on experience with this technology. In our survey, we explained the functionality of Internet anonymity software and asked users for their perceived usefulness of this software.

H4: PU will have a positive influence on ItU.

The final dependant construct of our model is the behavioral *Intention to Use Anonymity Software* (ItU) in the future. Similar to the PU construct, this construct originates from the TAM (Davis et al., 1989). Due to the fact that we focus on a rather unknown technology, many users of our survey have no or little experience with anonymity software. Therefore, we did not include the TAM construct *actual system use*. Furthermore, according to Venkatesh (2000) *perceived ease of use* may have been overestimated in IS research. According to him, "at all stages of user experience with a system, general, system-independent constructs play a stronger role than constructs that result of the user-system interaction" (Venkatesh, 2000). Therefore, and due to the fact that only few people have actual system use experience, we did not include *perceived ease of use* in our model. We rather focused on user-dependent constructs, such as IL and PA, for determining ItU. In addition, Szajna (1994) shows in her study the predictive validity of the ItU TAM construct.

2.3 Moderators

Using anonymity tools comes at a cost – an additional download latency. In order to account for this cost, we included a moderator: the stated and actual *Internet Patience* (IP) of a user.

Existing literature only contains constructs concerning the user's perception of waiting periods, such as *Perceived Waiting Duration* (Hui and Tse, 1996). The *Perceived Waiting Duration* depends not

only on user-external conditions such as providing a feedback bar in a browser window (cf. Nah, 2004), but also on user-internal conditions such as personality (cf. Hornik, 1984). However, there do not exist any constructs measuring this psychological aspect of the perception of time and especially in an information search context on the Internet. Therefore, we developed the multi-item IP construct (see Table 1) in order to measure the stated patience of an Internet user.

The actual IP was measured by an experimental part within the questionnaire (see Figure 1). Participants were asked to cancel the loading process of a website as soon as they would reach their maximum acceptable waiting time (TWT1). The same experiment was repeated later on in the questionnaire, though the participants were then told that they were surfing anonymously (TWT2). In order to measure the TWTs, we chose a within-subject design.

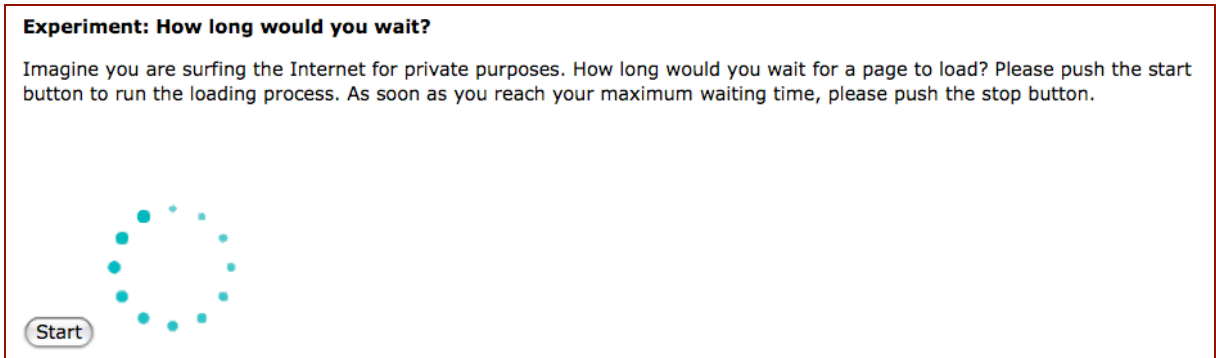


Figure 1. Screenshot of the Experimental Part for Measuring TWT1.

Most Internet users probably do have concerns about their privacy; but whether they find anonymity software useful or whether they would even use it, also depends on their IP. Therefore, we assume that IP moderates the relationship between the most relevant antecedent PC and one or both of the two target constructs PU and ItU. IP can be measured as a multi-item construct (stated behavior) and as TWT1 and TWT2 (actual behavior), which leads us to the following hypotheses:

H5a/b/c: IP (multi-item/TWT1/TWT2) will positively influence the relationship between PU and ItU.

H6a/b/c: IP (multi-item/TWT1/TWT2) will positively influence the relationship between PC and ItU.

H7a/b/c: IP (multi-item/TWT1/TWT2) will positively influence the relationship between PC and PU.

The conceptual model is depicted below (Figure 2).

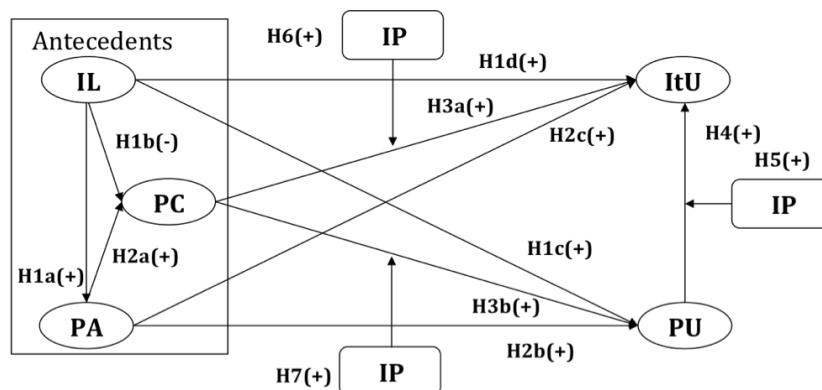


Figure 2. Conceptual Model.

3 Survey Development

Most of the constructs of our model, except IP, are based on constructs found in the literature (cf. Table 1). However, since those were mostly developed for an Internet transaction context, we had to adapt them to the context of information search. Furthermore, we newly developed the IP construct. Therefore, we tested the reliability of the constructs by *Category Shuffling* (Nahm et al., 2002). We asked six experts to assign the items to the constructs, which led to an Overall Hit Ratio (OHR) – the ratio of correctly placed items and total number of items (Landis and Koch, 1977) – of 72.22% (Table 2). Accordingly, we refined our items.

	IU	IL	IP	PU	PA	PC	none
IU	46			10	5	2	2
IL		69	2		3		4
IP		3	56			1	5
PU	8	4	1	37	1	6	8
PA		3			58	2	2
PC		1		1	17	61	11
Placed items: 429		Correctly placed items: 327			OHR: 72.22% $K_{free} = 0.592$		

Table 2. Results from Category Shuffling.

4 Data Analysis

To analyze the hypothesized model, we used Partial Least Squares (PLS) modeling, which is a variance-based approach to Structural Equation Modeling (SEM; Henseler et al., 2009). We used PLS-SEM because it is especially recommended during an early stage of theory development in order to test and validate exploratory models (ibid.). Furthermore, PLS-SEM has less stringent requirements concerning the distributional assumptions (ibid.). Therefore, models containing TAM constructs, such as our model (PU and IU), are usually analyzed with PLS (see e.g. Venkatesh, 2000; Venkatesh et al., 2003) as they tend to be skewed.

We send a link with an invitation to our online survey via university mailing lists. Out of 1345 respondents, 234 abandoned the questionnaire at some point and were therefore excluded from analysis, resulting in a total sample size of 1111 subjects. We adopted SmartPLS 2 (Ringle et al., 2005) to analyze the model.

PLS-SEM assessment typically follows a two-step assessment consisting of the evaluation of the measurement model and the structural model (Hair et al., 2011). Since the proposed model contains only reflective constructs, only reflective measurement evaluations are applied.

4.1 Demographics

The sample contained 59.5% females and 40.5% males; 80.4% of the participants were between 18 and 29 years old. The majority of the participants were not familiar with anonymity software: 74% did not know Tor, 21% had heard of it, and only 4% of the participants had used it before. We also asked if they knew other anonymity software (I2P or JAP), which approximately 85% of the participants denied.

4.2 Measurement Model

The measurement model determines the relationship between latent variables (constructs) and manifest variables (indicators). It can be evaluated by determining the reliability and the validity (see Table 4):

- (i) Indicator reliability can be readily assumed for all indicator loadings above 0.7 as recommended by Chin (1998). Only indicators that exhibit very low loadings (> 0.4) should be eliminated from reflective scales (Hair et al., 2011). In our model, only four indicator loadings (PC3, PU3, IP3, IP4) are below 0.7, but still above 4.0. Therefore, no indicator of the model is deleted.
- (ii) The values for construct validity in our model, determined by the composite reliability, are all above 0.8, which is satisfactory even for more advanced stages of research (Nunally and Bernstein, 1994).
- (iii) The convergent validity can be assessed by means of the Average Variance Extracted (AVE). The model fulfills the criterion of $AVE > 0.5$ (Chin, 1998). The discriminant validity can be assessed by means of the Fornell-Larcker criterion (Fornell and Larcker, 1981, p. 46) and is also satisfied in this model (see Table 3). It postulates that a latent construct shares more variance with its assigned indicators than with another latent variable in the structural model (ibid.).

Construct	IL	PA	PC	PU	ItU
Internet Literacy (IL)	0.982				
Privacy Awareness (PA)	0.403	0.914			
Privacy Concerns (PC)	-0.026	0.231	0.741		
Perceived Usefulness of Anonymity Software (PU)	-0.113	0.141	0.353	0.792	
Intention to Use Anonymity Software (ItU)	-0.017	0.241	0.297	0.614	0.946

Table 3. Square Root of AVE (diagonal elements) and Correlation between Latent Variables.

Construct Indicators (measured on a 7-point Likert scale)	AVE	Composite Reliability	Factor Loadings
Internet Literacy (IL)	0.778	0.913	
IL1. I am able to manage my browser's privacy and security options without difficulties.			0.904
IL2. I am able to clear my Internet browser cache, cookies, browsing and search history, and stored passwords without difficulties.			0.862
IL3. I feel competent cleaning spyware and adware installations from my computer.			0.880
Internet Privacy Awareness (PA)	0.663	0.887	
PA1. I follow the news and developments about Internet privacy issues and privacy violations.			0.839
PA2. I am interested in political discussions about privacy on the Internet.			0.827
PA3. I keep myself updated about Internet privacy issues and possible solutions that companies and the government employ to ensure our privacy.			0.875
PA4. I enjoy discussing Internet privacy issues with others.			0.708
Internet Privacy Concerns (PC)	0.549	0.829	
PC1. When I am online, I have the feeling of being watched			0.769
PC2. When I am online, I have the feeling that all my clicks and actions are being tracked.			0.803
PC3. Through the use of the Internet, information about Internet users can be disclosed unknowingly.			0.653
PC4. Internet websites are unsafe environments in which to exchange information with others.			0.731
Perceived Usefulness of Anonymity Software (PU)	0.627	0.870	
PU1. Overall, using anonymity software would be advantageous for me.			0.841
PU2. I would feel more secure on the Internet when using anonymity software.			0.859
PU3. Even when using anonymity software, I could complete tasks in the Internet efficiently.			0.672
PU4. The advantages of anonymity software would outweigh the delay when surfing the Internet.			0.783
Intention to Use Anonymity Software (ItU)	0.716	0.910	
ItU1. I am going to try out anonymity software for surfing the Internet.			0.825
ItU2. I intend to regularly use anonymity software in the future when surfing the Internet.			0.869
ItU3. I would inform others about anonymity software.			0.814
ItU4. I would recommend to others to routinely use anonymity software in the future.			0.876
Internet Patience (IP) as moderator	0.482	0.786	
IP1. It is very important for me to surf the Internet with a fast Internet connection.			0.783
IP2. If I think that a website takes too long to load, I cancel the loading process.			0.740
IP3. I am quickly frustrated if the Internet connection is slow.			0.646
IP4. I am used to quickly navigating the Internet due to a rapid Internet connection.			0.610

Table 4. Psychometric Properties of the Measurement Model.

The values for IP (multi-item) as a moderator are presented for the relationship between PC and PU in the table above because this relationship is the only one where the moderator (IP as a multi-item) has a significant influence (see Table 6). The composite reliability as well as the AVE value for IP lie just

beneath the recommended values, which we consider acceptable for the purposes of the model, since IP is not one of its central constructs.

4.3 Structural Model

The structural model determines the relationships between the constructs and each relationship corresponds to one hypothesis in our model (see Figure 3). Important criteria to evaluate the structural model are R^2 , the level and the significance of the path coefficients (Hair et al., 2011). The value of R^2 of the target construct should be high, since the goal of the prediction-oriented PLS-SEM approach is to explain the variance of the endogenous latent variables (ibid.). However, the concrete ranges for R^2 are depending on the stage of research and on the discipline. Our target construct ItU yields a value for R^2 of 40.4% (for PU: $R^2 = 14.9\%$), which seems good, as we are in an exploratory phase of research with the aim to predict behavioral intentions. PA yields a R^2 of 7% and PC of 16,1%.

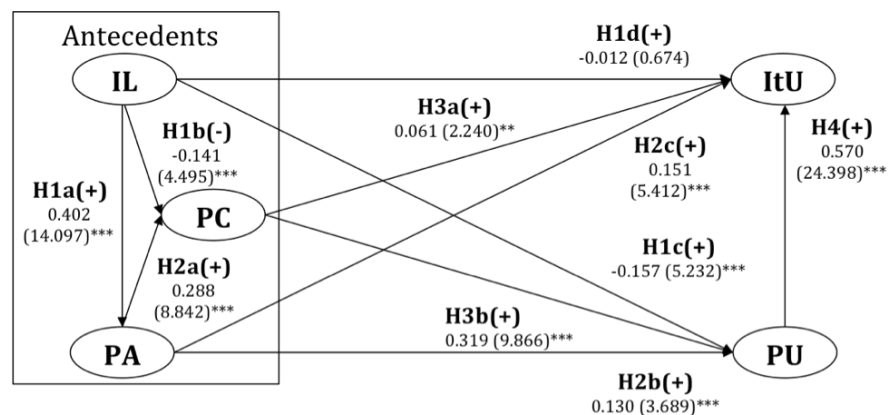


Figure 3. Structural Model (** $p < 0.001$; ** $p < 0.05$; * $p < 0.1$; Two-tailed Test).

The path coefficient between PU and ItU is the highest of all coefficients in the model. This is not surprising, as this relationship has already been validated in other TAM-based models. To test the significance of the path coefficients, we used the bootstrapping procedure with 1500 samples, 1111 cases, individual sign changes, and a case-wise replacement for missing values. The t-values from the bootstrapping procedures are presented in the figure above in parentheses. All path coefficients are significant at a minimum of at least 5% significance, except H1d. All hypotheses are supported except H1c (significant, but negative instead of positive) and H1d (not significant).

4.4 Moderators

After validating the basic model (H1-H4), we tested the hypothesis concerning the moderator (see Table 5). As described above, we introduced a moderator in this model in order to show that the relationships between the antecedents and our target constructs PU and ItU can be influenced by the IP of a user, affecting his willingness to wait for anonymity. This moderator (IP) was measured in three different ways: as a multi-item construct (stated behavior), and as measured tolerated waiting time (actual behavior) when surfing 'normally' (TWT1), and the tolerated waiting time when surfing anonymously (TWT2). We then tested the different moderators on different relationships (see Table 6).

SmartPLS (Ringle et al., 2005) allows to graphically model moderators and then to calculate the path coefficients and factor loadings. The results from the moderators were interpreted the same way as were the remaining constructs. We found three significant positive moderators (IP as multi-item, TWT1, and TWT2) for the relationship PC to PU.

n = 1111	IP (multi-item)				TWT1 (sec)	TWT2 (sec)
	IP1	IP2	IP3	IP4		
Mean	1.64	2.91	2.73	2.03	27.29	35.98
Std. Dev.	0.93	1.57	1.46	1.26	37.02	64.31
Median	1.00	3.00	2.00	2.00	18.66	21.10
Min / Max	1 / 7	1 / 7	1 / 7	1 / 7	0.71 / 545.17	0.72 / 1125.35

Table 5. Descriptive Statistics of IP Measured as Multi-Item, TWT1 and TWT2.

Hypothesis	Path estimate for moderator IP measured as ...		
	...multi-item (a)	... TWT1 (b)	...TWT2 (c)
H5: PU → ItU	-0.016 (0.584)	0.023 (0.688)	-0.035 (1.634)
H6: PC → ItU	0.037 (1.250)	0.036 (1.017)	-0.024 (1.043)
H7: PC → PU	0.168 (4.511)***	0.09 (2.673)***	0.044 (1.857)*

Table 6. Results of Hypotheses Testing Concerning Different Moderators (rejected hypotheses are highlighted in grey).

5 Results

As far as the first (i) research question is concerned, based on our results shown in Table 7, we can state that a user's IL negatively influences her PC (H1b), which confirms the findings of Dinev and Hart (2004b). Furthermore, the positive relation between IL and PA implies that a higher IL leads to a higher PA of the Internet users (H1A). PA is positively correlated with PC (H2A), which confirms our assumption that Internet users with higher privacy awareness have higher privacy concerns. We hypothesized that the three antecedents (IL, PC, and PA) positively influence the target constructs, PU and ItU. This positive correlation was confirmed for H2b, H2c, H3a, and H3b. A positive correlation between IL and ItU (H1d) could not be confirmed. Interestingly, we found a negative significant correlation between IL and PU (H1c), which was actually assumed to be positive. The reason for this could be that users with high IL assume that they can better evaluate where privacy threats occur and mitigate them by not using the respective website or technology, which leads to a lower PU of anonymity software for them. The positive correlation between PU and ItU (H4) has already been confirmed in earlier studies (e.g., by Venkatesh, 2000; Venkatesh et al., 2003). Accordingly, it is therefore not surprising that this relationship is significant and displays a very high t-value from the bootstrapping procedure. PU (H1c, H2b, and H3b) significantly mediates the relationships between the antecedents to the target construct ItU, all three hypothesized were confirmed. As assumed, (H3a) PC and PA (H2c) are positively correlated with ItU.

Concerning the moderators (Table 8), we can state that IP (measured as multi-item, TWT1, and TWT2) has a significant positive moderating effect on the relationship between PC and PU.

H1a (+): IL→PA	H2b (+): PA→PU
H1b (-): IL→PC	H2c (+): PA→ItU
H1c (+): IL→PU	H3a (+): PC→ItU
H1d (+): IL→ItU	H3b (+): PC→PU
H2a (+): PA→PC	H4 (+): PU→ItU

Table 7. Synopsis of Hypotheses.

Moderator IP measured as		
(a)multi-item	(b) TWT1	(c) TWT2
H5a (+): PU→ItU	H5b (+): PU→ItU	H5c (+): PU→ItU
H6a (+): PC→It	H6b (+): PC→ItU	H6c (+): PC→ItU
H7a (+): PC→PU	H7b (+): PC→PU	H7c (+): PC→PU

Table 8. Synopsis of Hypotheses concerning Moderators.

Our model explains 40.4% of the variance of the target construct ItU, which can be regarded as a good result, since our research is in an exploratory phase. That means that our goal is to explain behavior in the future (intention to use), and most of our subjects (74%) did not know about anonymity software before participating in our study. However, most of them can be expected to be above-average Internet savvy as they are mostly university graduates or students.

With respect to our second (ii) research question, we identified three antecedents that have a significant influence on our final dependant construct ItU, partially mediated by PU. These findings show that the important factors, which influence ItU are PA and PC. Accordingly, to broaden the use of anonymity software, it seems advisable to increase privacy awareness (PA) and accordingly the concerns (PC) of users, since the study revealed that users with higher PA have higher PC, too. The third antecedent IL also plays an important role, since it negatively influences PC and PU, but positively influences PA. This implies that users with a higher IL have lower PC, since they probably assume to know the technologies and the associated problems well. The negative correlation between IL and PU further suggests that it is more difficult to motivate more literate Internet users to use anonymity software than 'Internet illiterates'. This result might be caused by an overestimation of the participant's own IL skills, since we could not measure the real IL of the participant. Accordingly, we assume another effect, which we cannot explain with our model, but which we plan to investigate in future work: An overestimated IL (stated vs. actual IL) leads to a negative effect on PU. The significant positive moderating effect of IP on the relationship between PC and PU suggests that the IP of users has a positive effect on the PU. The fact that the relationship between PU to ItU and PC to ItU was not significant shows the importance of our mediator PU and implies that IP is important for ItU.

The variables TWT1 and TWT2 were already used as moderators. To answer the last and main (iii) research question, we reused these variables outside the SEM and compared TWT1 and TWT2 by means of a paired-sampled t-test. Our data reveals that the user's waiting time when surfing anonymously (TWT2) is significantly higher than the 'normal' waiting time (TWT1), i.e., users are willing to wait longer for Internet privacy (significant at 1%). The t-test was chosen due to the within-subject design: the TWT1 is not independent of TWT2, since every subject conducted both waiting time tests. Moreover, the median of TWT1 is of 18.6 seconds, whereas the median of TWT2 is 21.1 seconds. However, the absolute values are only given as an indication, but should not be considered to, e.g., predict acceptance rates of anonymity tools, as they could be biased by different searching behaviors and our within-subject design.

6 Limitations and Future Research

As mentioned, our study is subject to several limitations: The sample is quite homogeneous regarding nationality, age, and educational background, as the link to the survey was sent through the university's mailing list. Therefore, the degree of transferability to other user groups (other countries, participants who are not students) is difficult to evaluate. In future work, our study could be refined and extended to a less homogeneous group for identifying socio-cultural influence factors, such as age, education, or country of origin. Further, TAM was originally conceived for systems already in use, while in our study, we analyze the perceived usefulness of a system which most participants never used before. Third, participants often mispredict their own future behavior (cf. Loewenstein and Schkade, 1999) and therefore might have over- or underestimated their ItU and PU of anonymity software. Fourth, our experimental data (TWT1 and TWT2) might be influenced by the fact that we conducted the experiment with a within-subject design, i.e., each user had to measure her patience twice, once for the 'normal' waiting time (TWT1) and once for the 'anonymous' waiting time (TWT2), possibly adding some noise to our results. In addition, the experiment was conducted online and therefore, we could not control tab browsing, i.e., participants switching to other browser tabs during the waiting time. But since this would reflect the normal surfing behavior of those particular users, their TWT can still be compared to those of others. Another limitation of our study is that we recognized that the construct IL only offers a high level view on a user's personal skills. A more fine-grained view by adding additional determinants of IL, e.g. actual vs. perceived IL, would provide a better evaluation of a users real IL. Furthermore, it would be interesting to investigate which type of personal information users are willing to use anonymity software for when disclosing this information.

7 Conclusion

In our study we investigated the acceptance of Internet anonymity software among Internet users. We addressed the following questions in particular: (i) which factors influence Internet users' intention to use anonymity software? (ii) How can the diffusion of anonymity software among Internet users be increased? (iii) And how long are users willing to wait when surfing the Internet with and without anonymity software?

The results of our survey imply that the acceptance of anonymity software is influenced by three main factors – the Internet literacy of users, their privacy concerns and their Internet privacy awareness, which all are mediated by the degree of how useful the user perceives the anonymity software. We conclude that an increase of Internet privacy awareness and therefore Internet privacy concerns would increase the usage of anonymity software. Interestingly, a user's self-estimated Internet literacy had a negative effect on the perceived usefulness of anonymity software in our study. Further, Internet users with higher patience when surfing the Internet consider anonymity software more useful than those with lower patience in the Internet, which indicates that designers of Internet anonymity software should focus on reducing latency if they would like to extend the user community. We also can answer our initial questions whether users are willing to wait longer for Internet privacy in the affirmative: the accepted waiting time when surfing anonymously is significantly higher than the accepted waiting time when surfing 'normally'.

Acknowledgements

We would like to thank Marko Sarstedt and Christian Theel for their statistical support, and Annika Baumann. This research was funded by the German Federal Ministry of Education and Research under grant number 01IA08001E as part of the Aletheia project (<http://www.aletheiaprojekt.de/>). The responsibility for this publication lies with the authors.

References

- Amnesty International (2006). Undermining Freedom of Expression in China – The Role of Yahoo!, Microsoft and Google, <http://irrepressible.info/static/pdf/FOE-in-china-2006-lores.pdf>. Accessed 11-28-2010.
- Chin, W.W. (1998). The Partial Least Squares Approach to Structural Equation Modeling. In *Proceedings of Modern Methods for Business Research* (Marcoulides, G. A. Ed.), Lawrence Erlbaum Associates, Mahwah, NJ, 295-336.
- Davis, F.D., Bagozzi, R.P. and Warshaw P.R. (1989). User Acceptance of Computer Technology: a comparison of two theoretical models. *MIS Quarterly*, 35 (8), 982-1003.
- Dinev, T. and Hart, P. (2004a). Internet Privacy Concerns and Their Antecedents –Measurement validity and a regression model. *Behaviour & Information Technology*, 23 (6), 413-422.
- Dinev, T. and Hart, P. (2004b). Internet Privacy, Social Awareness, and Internet Technical Literacy – An Exploratory Investigation. In *Proceedings of the 17th Bled eCommerce Conference*.
- Dinev, T. and Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research*, 17 (1), 61–80.
- Dinev, T. and Hu, Q. (2006). The Centrality of Awareness in the Formation of User Behavioural Intention toward Protective Information Technologies. *Journal of the Association for Information Systems*, 8 (7), 386-408.
- Dingledine, R., Mathewson, N. and Syverson, P. (2004). Tor: The Second-Generation Onion Router. *Proceedings of the 13th USENIX Security Symposium*, 303-320.
- Dingledine, R. and Murdoch, S. J. (2009). Performance Improvements on Tor – or, why Tor is Slow and What we're Going to do about it, Online: <http://www.torproject.org/press/presskit/2009-03-11-performance.pdf>. Accessed 11-28-2010.

- Fabian, B., Goertz, F., Kunz, S., Müller, S. and Nitzsche, M. (2010) Privately Waiting – A Usability Analysis of the Tor Anonymity Network. In Proceedings 16th Americas Conference on Information Systems (AMCIS 2010), Selected Papers, Springer LNBI, Vol. 58.
- Fornell, C.G. and Larcker, D.F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research*, 18 (1), 39-50.
- Hair, J. F., Ringle, C. M. and Sarstedt, M. (2011). PLS-SEM – Indeed a Silver Bullet. *Journal of Marketing Theory & Practice*, 19 (2), 139-152.
- Henseler, J., Ringle, C. and Sinkovics, R. (2009). The Use of Partial Least Squares Modeling in International Marketing. *Advances in International Marketing*, 20, 277-319.
- Hui, M. K. and Tse, D. (1996). What to Tell Consumers in Waits of Different Lengths: An integrative Model of Service Evaluation. *Journal of Marketing*, 60 (2), 81-90.
- Hornik, Jacob (1984). Subjective vs. Objective Time Measures: A Note on the Perception of Time in Consumer Behavior. *Journal of Consumer Research*, 11, 615-18.
- Krishnamurthy B., Malandrino D. and Wills, C.E. (2007). Measuring Privacy Loss and the Impact of Privacy Protection in Web Browsing. In Proceedings of the Symposium on Usable Privacy and Security.
- Landis, J.R., and Koch, G.G. (1977). The Measurement of Observer Agreement for Categorical Data. *Biometrics*, 33 (1), 159-174.
- Loewenstein, G. and Schkade, D. (1999). Wouldn't it be Nice? Predicting future feelings. In Daniel Kahneman (Diener, E. and Schwarz, N. Eds.) *Well-being: the foundations of hedonic psychology*, Sage, NY, 85-105.
- Malhotra, N.K., Kim, S.S. and Agarwal, J. (2004). Internet Users' Information Privacy Concerns: The Construct, the Scale, and a Causal Model. *Information Systems Research*, 15 (4), 336–355.
- Nah, F. F.-H. (2004). A Study on Tolerable Waiting Time: How long are Web users willing to wait? *Behaviour & Information Technology*, 23 (3), 153-163.
- Nahm, A.Y., Solís-Galván, L.E., Rao, S.S. and Ragun-Nathau, T.S. (2002). The Q-Sort Method: Assessing Reliability and Construct Validity of Questionnaire Items at a Pre-Testing Stage. *Journal of Applied Statistics*, 1(1), 114 - 125.
- Nunnally, J.C. and Bernstein, I. 1994. *Psychometric Theory*. New York: McGraw Hill.
- Randolph, J.J. (2005). Free-Marginal Multirater Kappa: An alternative to Fleiss' fixed-marginal multirater kappa. *Joensuu University Learning and Instruction Symposium*.
- Ringle, C.M., Wende, S. and Will, S. (2005) *SmartPLS 2.0 (M3) Beta*, Hamburg, <http://www.smartpls.de>. Accessed 11-28-2010.
- Stewart, K.A. and Segars, A. H. (2002). An Empirical Examination of the Concern for Information Privacy Instrument. *Information Systems Research*, 13 (1), 36-49.
- Szajna, B. (1994). Software Evaluation and Choice: Predictive Validation of the Technology Acceptance Instrument. *MIS Quarterly*, 18 (3), 319-324.
- Tor Project: <http://www.torproject.org/>. Accessed 11-28-2010.
- Venkatesh, V. (2000). Determinants of Perceived Ease of Use: Integrating Control, Intrinsic Motivation, and Emotion into the Technology Acceptance Model. *Information Systems Research*, 11 (4), 342-365.
- Venkatesh, V., Morris, M.G., Davis, G.B. and Davis, F. D. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly*, 27 (3), 425-478.
- Xu, H., Dinev, T., Smith, H.J. and Hart, P. (2008). Examining the Formation of Individual's Privacy Concerns: Toward an Integrative View. *Proceedings of the International Conference on Information Systems (ICIS 2008)*.