Association for Information Systems
AIS Electronic Library (AISeL)

COMMUNICATION ANONYMIZERS: PERSONALITY, INTERNET PRIVACY LITERACY AND THEIR INFLUENCE ON TECHNOLOGY ACCEPTANCE

Franziska Brecht
Institute of Information Systems

Benjamin Fabian
School of Business and Economics

Steffen Kunz
School of Business and Economics

Sebastian Müller
Freie Universität Berlin

Follow this and additional works at: http://aisel.aisnet.org/ecis2012

COMMUNICATION ANONYMIZERS: PERSONALITY, INTERNET PRIVACY LITERACY AND THEIR INFLUENCE ON TECHNOLOGY ACCEPTANCE

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

Müller, Sebastian, Freie Universität Berlin, Takustr.9, 14195 Berlin, Germany, sebastian.mueller@fu-berlin.de

Abstract

Despite the fact that many individuals are concerned about privacy issues on the Internet and know about the existence of communication anonymizers, very few individuals actually use them. This discrepancy can only partially be explained by evident factors such as a small degree of knowledge about Internet privacy issues, or the latency of the Internet connection caused by communication anonymizers. In this study, we determine factors that influence the acceptance of communication anonymizers: the role of personality traits of individuals, the actual knowledge about privacy issues on the Internet and how much individuals really know about them, as well as the time an individual is willing to wait when using a communication anonymizer. Our study shows that the personality traits

'Agreeableness,' 'Extroversion' and 'Conscientiousness' do not influence an individual's acceptance of communication anonymizers. Further, we can show that individuals with a strong personality trait of neuroticism are more likely to have strong privacy concerns and that individuals that can be characterized as 'open' are more likely to use communication anonymizers. With regard to the knowledge about privacy issues on the Internet, we find that individuals generally possess a low knowledge. Surprisingly, we find a negative correlation between an individual's 'stated' and his/her 'actual' knowledge of privacy issues. Last, we find that individuals are willing to wait slightly longer (3.5 seconds) when using communication anonymizers.

Keywords: Communication Anonymizer, Technology Acceptance, Personality, Big Five, Tolerated Waiting Time, Structural Equation Modelling

1   Introduction

Communication anonymizers such as Tor (Tor Project, 2011) or Freenet (Freenet Project, 2011) are privacy-enhancing technologies that can help individuals to protect their privacy on the Internet. Privacy is the claim of individuals to determine when, how, and to what extent information about them is communicated to others (Westin, 1967). Communication anonymizers impede the identification of an individual in a larger set of individuals communicating at the same time (Pfitzmann and Hansen, 2010). Despite their apparent benefits for increasing privacy, very few individuals use communication anonymizers. Tor – to name one – had only 400.000 users worldwide in November 2011 (Tor Project, 2011). This phenomenon cannot solely be explained by a low usability of communication anonymizers. For example, the installation and configuration procedures, the usability of which has been criticized in the past (Clark et al., 2007), has been improved during recent years by the provision of pre-configured browser packages and live distributions of the software (Tor Project, 2011). One usability problem that has not been solved yet is the increased latency during surfing (Wendolski et al., 2007; Freenet Project, 2011; Tor Project, 2011). Reasons for the latency are the indirect flow of messages and cryptography necessary in order to provide anonymity (Dingledine et al., 2004), and several unsolved performance issues (Dingledine et al., 2009). But is high latency the crucial factor explaining the general reluctance to anonymize an individual's communications on the Internet?

In information systems (IS) research, the technology acceptance model (TAM; Davis et al., 1989) aims at specifying factors that lead individuals to accept or to reject a technology. More specifically, TAM states that the behavioral intention to use a technology is determined by an individual's attitude towards that behavior. However, external variables such as individual differences and personality traits may equally impact that behavior (Davis et al., 1989). The influence of personality on technology acceptance decisions is not well investigated, even though psychological research has identified personality traits as highly relevant predictors of human behavior (Junglas and Spitzmüller, 2006).

Therefore, our research questions are: (i) How does personality influence the intention to use communication anonymizers? (ii) How does the knowledge about Internet privacy influence the intention to use communication anonymizers? (iii) How long is the tolerated waiting time individuals are willing to wait when using communication anonymizers?

To answer these research questions, we developed and empirically validated a model based on IS and psychology literature, which incorporates a widely accepted personality test (Barrick et al., 2001) called the Big Five (McCrae et al., 1986). Furthermore, we included different tests in order to measure knowledge about Internet privacy, as such knowledge is an important antecedent to explain privacy perceptions and behavioral intentions to use communication anonymizers (Brecht et al., 2010).

2   Model Development and Hypothesis

Our hypothesized model takes over the constructs and their relationships as described by Brecht et al. (2011). Our model therefore includes the following constructs: 'Internet Privacy Literacy', 'Privacy Awareness', 'Privacy Concerns', 'Perceived Usefulness' and 'Intention to Use'. 'Privacy Awareness' measures the awareness of Internet users regarding a general existence and possibility of Internet privacy issues, without focusing on technical details or on a particular user. 'Privacy Concerns' measures the perceived risk that data about the individual personal surfing behavior of a user is being collected, transmitted and abused. '(Stated) Internet Privacy Literacy' assesses the extent to which an Internet user states to understand the technical background of Internet privacy problems and feels confident, e.g., when manipulating the privacy configurations of Web browsers. 'Perceived

Usefulness' describes the degree of perceived usefulness of anonymity software, and 'Intention to Use' the behavioral intention to use anonymity software in the future. According to Brecht et al. (2011) the relationships could be validated as follows:

H1/2: 'Privacy Awareness' will have a positive influence on 'Privacy Concerns' / 'Perceived Usefulness'.

H3/4: 'Privacy Concerns will have a positive influence on 'Intention to Use' / 'Perceived Usefulness'.

H5: 'Perceived Usefulness' will have a positive influence on 'Intention to Use'.

H6/7: 'Internet Privacy Literacy' will have a positive influence on 'Privacy Awareness' / 'Privacy Concerns'.

Additionally, our model extends the model of Brecht et al. (2011) by two factors that are explained in the following sections: personality traits and the actual 'Internet Privacy Literacy' of an individual.

2.1 'Internet Privacy Literacy': stated vs. actual

The construct 'Internet Privacy Literacy' (PL) is an important antecedent of our model, as individuals who are not aware that e.g. surveillance of their individual surfing behavior is technically easy to conduct, will probably not be concerned about privacy problems and will most certainly feel no need to use communication anonymizers. According to Dinev and Hart (2004), PL is a subset of computer literacy, i.e., it is influenced by the individual's computer skills, attitudes and beliefs. Since Internet privacy and anonymity requires knowledge of complex technical topics, an individual's self-assessment may not reflect the actual degree of her/his knowledge. Therefore, we measured PL in two ways: stated PL (PL-S) and actual PL (PL-A).

The PL-S measures the extent to which an individual feels confident to be able to manipulate the security and privacy configurations of Internet clients such as Web browsers (Brecht et al., 2010). PL-S was measured with items such as 'I know much about anonymity and privacy on the Internet' or 'I know which web pages store my surfing behavior'. Brecht et al. (2010) found a negative relationship between PL-S and 'Perceived Usefulness', i.e., individuals who stated that they have good knowledge of Internet privacy are less likely to find communication anonymizers useful. This seems contradictory. One possible explanation could be that individuals with a higher knowledge about Internet privacy assume that they could better evaluate where privacy threats occur and mitigate them, e.g. by not using the respective web page or technology (Brecht et al., 2010). However, as this assumption has not been proven empirically, we also measured PL-A.

PL-A was measured with a single-item construct: We developed six questions that were pre-tested several times (Table 1). The six answers (0-incorrect answer, 1-correct answer) were then mapped to a 7-point Likert scale, where '1' indicates that a participant did not answer any of the questions correctly and '7' that all questions were answered correctly.

Questions and answers	Solution
1. How can a Web site distinguish its users from another? (Multiple answers could be correct.) a) Login Name; b) IP Address; c) Cookie; d) Browser Version and Configuration; e) I don't know.	a,b,c,d
2. Which of the following statements are true? (Multiple answers could be correct.) a) When you are surfing the Web without encryption, your Internet provider can observe the content of the Web site you are surfing to. b) When you are surfing the Web using encryption, your Internet provider can observe the content of the Web site you are surfing to. c) When you are surfing the Web using encryption, the Web server can observe the content of the Web site you are surfing to. d) When you are surfing the Web without encryption, any router on the way to the server can observe the content of the Web site you are surfing to. e) I don't know.	a,c,d
3. Which of the following protocols can provide confidentiality for e-mail transmission? (Only one answer is correct.) a) Sec4Mail; b) POPSEC; c) SSL; d) SIMAP; e) I don't know.	c
4. Which of the following protocols are used during Web Surfing? (Multiple answers could be correct.) a) HTTP; b) IMAP; c) TCP; d) IP; e) I don't know.	a,c,d

5. Which of the following actions may enhance your privacy while surfing the Web? (Multiple answers could be correct.) a) Use of a Web proxy; b) Always accepting cookies; c) Deleting the browser history; d) Not revealing your personal data; e) I don't know.	a,c,d
6. What are Web proxies useful for? (Multiple answers could be correct.) a) To hide the IP address of a computer. b) To speed up access to web sites (using caching). c) To block undesired web sites. d) To hide the location of a computer. e) I don't know.	a,b,c,d

Table 1.   Questions and answers for the construct 'Internet Privacy Literacy - Actual'.

2.2   The influence of personality on technology acceptance

Personality traits have been recognized to explain behavioral intention in IS research to a certain degree. Personality traits are generally conceptualized as individual characteristics that influence human behavior in a consistent manner across a variety of situations (Junglas and Spitzmüller, 2006). We will employ the constructs 'Agreeableness', 'Neuroticism', 'Extroversion', 'Conscientiousness' and 'Openness' (the so called Big Five, cf. McCrae and John, 1992), which have been meta-analytically found to subsume all other personality traits (McCrae, 1992; McCrae et al., 1986). Though this personality test has been validated and used to predict behavior across various studies, there exists little research on the impact of personality traits with regard to technology issues, such as privacy concerns, computer anxiety and behavioral intentions (e.g. Korukonda, 2007; Korzaan and Boswell, 2008).

Based on this background, we deduct our hypothesis as follows: Agreeable individuals are trusting, sympathetic, straightforward and selfless (McCrae and Costa, 1986). Korzaan and Boswell (2008) argue that agreeable individuals are especially worried about others and they are more likely to be concerned about privacy issues. Junglas and Spitzmüller (2006) state that agreeable individuals trust in others and are therefore not expecting negative consequences when revealing data. We formulate our hypothesis accordingly, i.e., that individuals scoring high on agreeableness will have less 'Privacy Concerns':

H8: 'Agreeableness' will have a negative influence on 'Privacy Concerns'.

Individuals scoring high on 'Neuroticism' tend to be insecure and highly concerned about potential failures or risks; they have a tendency to experience more threats and anxiety than do emotionally stable individuals (Goldberg, 1990). Due to their worrisome nature and their tendency to focus on negative events and possible losses, we expect highly neurotic or emotionally unstable individuals to be worried and concerned about privacy:

H9: 'Neuroticism' will have a positive influence on 'Privacy Concerns'.

'Extroversion' measures an individual's approach to dealing with his environment. McCrae and Costa (1986) use terms such as assured, dominant, gregarious and warm to describe this construct. Korzaan and Boswell (2008) argue that leadership characteristics fall under this trait; therefore the individual exhibiting this personality trait is more inclined to take responsibility and guide others. Therefore, they hypothesize that individuals showing high levels of 'Extroversion' would be more concerned with information privacy, because such individuals wish to protect those around her/him.

Since the construct 'Privacy Concerns' only measures one's own concerns, we agree with Junglas and Spitzmüller (2006) who argue that extroverted individuals are more likely to make efforts to be actively involved and are more interested in opportunities to provide and obtain information. As a result, we hypothesize that extroverted individuals should be less likely to be concerned about privacy, and thus be more likely to reveal personal information:

H10: 'Extroversion' will have a negative influence on 'Privacy Concerns'.

The next character trait, 'Conscientiousness', assesses the extent to which an individual behaves rational, ordered or informed (McCrae et al., 1986). Conscientiousness can also be interpreted as

ambiguity intolerance. Persons showing this character trait are likely to gather more information during risk processing (Conchar et al., 2004). Also, they consider ambiguous situations as more risky, and are less willing to take risks (Conchar et al., 2004). Conscientious individuals gather whatever information is needed to make informed decisions and act cautiously. As there is ample information on privacy issues publicly available, a conscientious individual is likely to investigate and be concerned about privacy aspects (Junglas and Spitzmüller, 2006), and finally act accordingly to reduce the risks. As a result, we hypothesize that conscientious individuals will be concerned about privacy issues and will show a behavioral intention to use communication anonymizers:

H11/12: 'Conscientiousness' will have a positive influence on 'Privacy Concerns'/ 'Intention to Use'.

Individuals with a high score concerning 'Openness' are said to be curious, intellectual, and to enjoy experiencing new situations (McCrae et al., 1986). Therefore, we hypothesize that highly open individuals are more inclined to try out communication anonymizers than individuals scoring low on that character trait:

H13: 'Openness' will have a positive influence on 'Intention to Use'.

3   Data Collection

Our data was generated by means of a lab experiment. We sent an invitation to participate in the lab experiment via several university mailing lists. The experiment consisted of an experimental part and a questionnaire. The experiment took place in a computer lab with up to 24 participants per session. The computer lab provided access to the experimental web page and to the questionnaire for each participant via Internet access.

The participants were mainly students with different fields of studies from two large universities. Each session lasted for about 60 minutes and included an introductory briefing about the functionality of communication anonymizers. Then, participants completed the experimental part and the questionnaire. Participants were remunerated with 10€ in cash. In order to avoid interaction between the participants, we separated them visually by means of operable walls and provided them with earplugs.

3.1   Experimental Part

The goal of the experimental part was to measure if and how long participants would be willing to wait longer when surfing anonymously with communication anonymizers, such as Tor. Therefore, we realized a between-subject design with a total sample size of n=151. The treatment group (n=85) was told that they were surfing anonymously by means of Tor, although they used a standard Internet connection, as did the control group (n=66).

The experimental design was adapted from Nah (2004). Our participants were confronted with a list of questions and were required to access specific web pages to obtain the answers. All participants used the same experimental software, specifically designed for the experiment, through the same kind of browser. Furthermore, the first question was collectively solved as an example question by the entire group. The experimental software provided hyperlinks to the other web pages that contained the information needed to obtain the answers to complete the assignment. The participants were asked to type in the answer and then to proceed to the next question (see Figure 1).

Most often the questions concerned specific facts. However, some questions were about personal matters to sensitize participants with regard to a possible revelation of personal information. Participants were confronted with the following questions:

	Question	URL
1.	How many goals did Ballack shoot for FC Chelsea?	http://de.wikipedia.org/wiki/Michael_Ballack
2	Please indicate the surface of the world in km^2.	http://www.pdwb.de/nd16-1.htm
3	Please indicate the number of inhabitants of the city in which you were born.	http://de.wikipedia.org/
4	Which of the diseases you suffered from until now have the longest incubation period?	'broken' hyperlink
5	How many victims did the sinking of the Titanic claim?	http://www.augenblicke-zwischen-leben-und-tod.de/t708f59-Katastrophen-der-Seefahrt.html
6	For which movie did Tom Hanks win an Oscar?	http://de.wikipedia.org/wiki/Tom_Hanks
7	What would be your most probable reason for an occupational disability?	http://www.berufsunfaehigkeitsversicherung-vergleich-01.de/ursachen.php
8	Please indicate the international airport which is the nearest to the city you grew up in.	'broken' hyperlink
9	How deep (in meters) is the "Great Blue Hole" in Belize?	http://sevennaturalwonders.org/north-america
10	Please indicate the twin city of the city you were born in.	http://de.wikipedia.org/
11	Please indicate the surface (km^2) of the city were you graduated from high school.	http://de.wikipedia.org/
12	Please indicate the date of death of J. F. Kennedy.	http://www.presidents.com/
13	What does the abbreviation Tor represent?	https://www.torproject.org/
14	What is the capital of the Central African Republic?	http://www.state.gov/r/pa/ei/bgn/4007.htm
15	Find the birth date of A. Einstein.	http://www.einsteingalerie.de/bio/bio.html

Table 2.   Questions asked during the experimental part and their URLs.

Figure 1.   Screenshot of the experimental software.

Out of the 15 hyperlinks to web pages that we provided to all participants for answering the questions, two hyperlinks were intentionally disrupted or 'broken', namely for question 3 and 7. Upon clicking on the 'broken' hyperlink, a feedback bar appeared to indicate that the system was carrying out their request, but the browser never showed any web page. The feedback bar did not provide information about the waiting duration. For the two 'broken' hyperlinks, the participants would have to click the 'next question' button to terminate the wait. Upon clicking on any of the hyperlinks that did work, a web page would appear within a negligible download time.

Tolerated Waiting Time (TWT) is defined as the time elapsed between the moment the link was clicked upon (i.e., download request was made) and the moment the 'next question' button was clicked (i.e., download request was terminated).

3.2   Personality Traits

Our questionnaire was based the original items of the Big Five (Costa and McCrae, 1992), which include approximately ten items per construct. Some of the original items are reversed to avoid response biases, i.e. acquiescence or agreement response tendency, as recommended by psychometricians (e.g. Nunally and Bernstein, 1994). For the data analysis, we first re-reversed those items and then performed a principal component analysis in SPSS (version 19) with Varimax Rotation.

Our data confirms all personality constructs. However, many items did not load onto the corresponding construct. Therefore, we refined the personality constructs by only choosing items which explained the corresponding construct well, leaving us with approximately 4 items per construct. The selected personality items are depicted in the table below.

Construct	I see myself as someone who …
Agreeableness	*tends to find fault with others; starts quarrels with others; is sometimes rude to others.*
Extroversion	is talkative; generates a lot of enthusiasm; *tends to be quiet*; is outgoing, sociable.
Openness	is original, comes up with new ideas; has an active imagination; likes to reflect, play with ideas.
Conscientiousness	is a reliable worker; perseveres until the task is finished; does things efficiently; makes plans and follows through with them.
Neuroticism	is depressed, blue; worries a lot; *is emotionally stable*, *not easily upset*; gets nervous easily.

Table 3.   Items of personality constructs (italic items are reversed).

4   Data Analysis

With regard to the demographics, we find that 86% of the 151 participants were between 18-29 years old, 12% were between 30-45 years old. 46% were female and 54% male. 74% were students or university graduates (23%).

Further, we asked our participants whether they knew and used certain communication anonymizers (Figure 2). Sixty-eight percent of our participants knew at least one of the communication anonymizers we asked for, and 10% of the participants stated to use at least one of them. If participants knew certain communication anonymizers but did not use them, we asked them why not (free text field). In their answers, the reason stated most was that participants did not find it necessary to use communication anonymizers (15%) or that they complained about the increased latency when surfing the Internet (11%).

With regard to the TWT, we find that participants from our treatment group (anonymous surfers) were willing to wait significantly longer for the web page to load for the question with the first 'broken' hyperlink than participants from the control group (non-anonymous surfers). Furthermore, we could not find any significant differences regarding the TWT for the second 'broken' hyperlink (see Table 4).
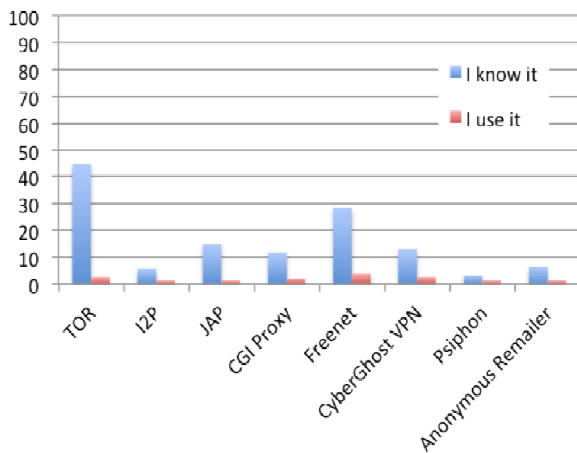

Tolerated Waiting Time (TWT, in seconds)		'broken' hyperlink	
		1st	2nd
Control Group (Non-anonymous surfers) n = 66	Mean	33.6	32.2
	Median	26.0	17.0
	St. Dev.	24.9	40.8
	Min/Max	3.8/119.6	1.9/167.4
Treatment Group (Anonymous surfers) n = 85	Mean	37.1	31.7
	Median	31.0	23.0
	St. Dev.	22.6	33.3
	Min/Max	5.0/111.0	1.3/140.1
p-value (Mann-Whitney-U test)		**0.10***	0.49

Figure 2. Awareness and usage of communication anonymizers (in %).

Table 4. TWTs for the 'broken' hyperlinks

4.1　　Internet Privacy Literacy

As concerns the actual Internet Privacy Literacy (PL-A), most participants did not answer the questions correctly (see Table 1 for questions). More specifically, the question asking for measures to enhance one's privacy while browsing the web was only answered correctly by 25% of the participants, and this was the best result for all relevant questions. The question about web proxy usage and encryption was only solved by 3% of the participants, which represents the worst result.

In order to see whether there is a correlation between PL-A and the mean of all items of PL-S, we conducted a non-parametric related samples test (Kendall's tau). The result is a significantly negative correlation (correlation coefficient of 0.283, significant at 1%). This means that the higher individuals estimate their knowledge about Internet privacy issues, the lower it could be in reality.

To analyze the hypothesized model, we used partial least squares (PLS) modeling because it has less strict requirements concerning the distributional assumptions (Henseler et al., 2009). Therefore, models containing TAM constructs, such as our model (cf. 'Perceived Usefulness' and 'Intention to Use'), are usually analyzed with PLS (see e.g. Venkatesh, 2000) as they tend to be skewed. 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).

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: Indicator reliability can be assumed because most indicator loadings are above 0.7, a threshold recommended by Chin (1998). Construct validity can also be assumed as most constructs show a composite reliability of above 0.8 (Table 5), a threshold which is even satisfactory for more advanced stages of research (Nunally and Bernstein, 1994). Further, the convergent validity can also be assumed as all constructs have an average variance extracted (AVE) of above 0.5, a threshold recommended by (Cohen, 1988). Furthermore, the discriminant validity, which can be assessed by means of the Fornell-Larcker criterion (Fornell and Larcker, 1981, p. 46), is also satisfied in this model. The criterion postulates that a latent construct shares more variance with its assigned indicators than with another latent variable in the structural model (Fornell and Larcker, 1981).

The structural model determines the relationships between the constructs and is evaluated by R2, and the level and the significance of the path coefficients (Hair et al., 2011). Our target construct 'Intention to Use' yields a value for R2 of 48%, while it is 34% for 'Perceived Usefulness', 72% for 'Privacy Awareness' and 51% for 'Privacy Concerns' (Figure 3). To test the significance of the path coefficients, we used the bootstrapping procedure with 1500 samples, 154 cases, individual sign changes, and a case-wise replacement for missing values. Our structural model and its path coefficients are depicted in Figure 3, which also shows that all path coefficients could be proven to be significant, except for the path coefficients 'Agreeableness'-> 'Privacy Concerns' (H8), 'Extroversion'->'Privacy Concerns' (H10) and 'Conscientiousness'->'Privacy Concerns' (H11) and 'Conscientiousness'->'Intention to Use' (H12).

We compare the influence of PL-A and PL-S on the 'Privacy Concerns' and the 'Privacy Awareness' both qualitatively by means of the path coefficients, and quantitatively by means of the R2 and the effect sizes (Table 6). First, we compare the path coefficients: whereas PL-S has a negative influence on 'Privacy Concerns', PL-A has a positive one. Further, whereas PL-S has a positive influence on 'Privacy Awareness', the opposite is the case with PL-A. Second, we compare the R2: PL-S has a higher influence on the construct 'Privacy Awareness' than PL-A. This indicates that the variance of 'Privacy Awareness' can be predominantly explained by the PL-S of our participants. The values for R2 for 'Privacy Concerns' do not differ much, regardless of whether this construct is influenced by PL-A or PL-S. Finally, an analysis of the effect sizes enables us to determine to what extent the PL of our participants' influences their 'Privacy Concerns'. According to Cohen (1988), effect sizes of 0.02, 0.15, and 0.35 are termed small, medium, and large. Whereas PL-A has a small effect on the 'Privacy

Concerns', PL-S has a medium effect on the 'Privacy Concerns'. The effect size might also be influenced by the fact the PL-S is a multi-item construct, whereas PL-A is a single-item construct. Therefore, PL-S might explain more variance of the endogenous constructs than PL-A.
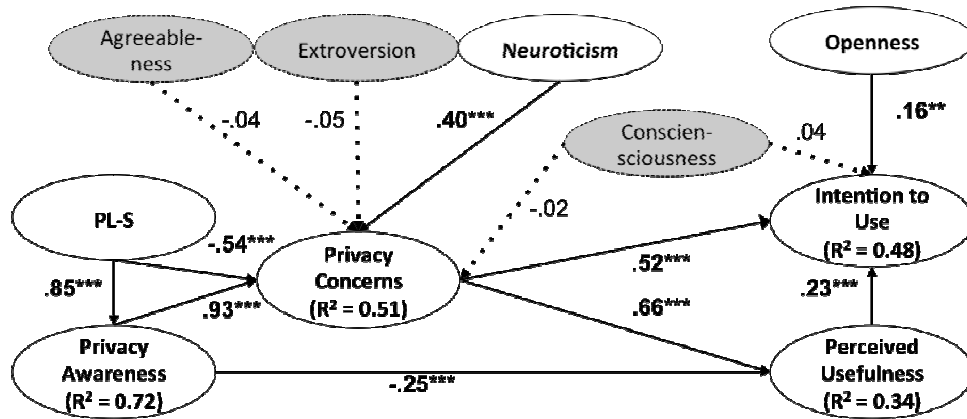

Figure 3.   *Structural model (*p<0.10; **p<0.05; ***p<0.01) and explained variance (R²).*

Construct	AVE	C.R.
Internet Privacy Literacy (IP-S)	.56	.84
Privacy Awareness	.83	.90
Privacy Concerns	.59	.85
Perceived Usefulness	.65	.88
Intention to Use	.74	.92
Agreeableness	.59	.80
Extroversion	.53	.55
Conscientiousness	.99	.99
Neuroticism	.50	.74
Openness	.57	.80

Table 5. Average variance extracted and composite reliability (C.R.).

	PL-S	PL-A
PL -> 'Privacy Awareness'	0.85***	-0.36***
PL -> 'Privacy Concerns'	-0.54***	0.16**
R^2 (Privacy Awareness)	71.7%	12.8%
R^2 (Privacy Concerns)	50.7%	45.1%
f^2 (Privacy Concerns)	15.8%	4.0%

Table 6. Path coefficients, R^2 and effect size (f^2) of PL-S and PL-A.

5   Discussion

The results of our survey enable us to answer our three research questions, which were directed at (i) the influence of personality traits; (ii) the knowledge about Internet privacy issues on the behavioral intention to use communication anonymizers; and (iii) the TWT individuals are willing to wait when using communication anonymizer.

With regard to the first research question, we find that individuals that can be characterized as neurotic are more likely than other individuals to have high privacy concerns. Our findings therefore can be said to confirm those of Korzaan and Boswell (2008), who showed that neuroticism has an influence on computer anxiety. According to our data, all other personality factors explored (namely 'Agreeableness', 'Extroversion' and 'Conscientiousness') do not influence the degree to which an individual has privacy concerns. In contrast to our results, Korzaan and Boswell (2008) concluded that agreeable individuals tend to have higher privacy concerns. They also did not find that extroverted or conscientious individuals are particularly concerned about their privacy. Furthermore, as we hypothesized, our study confirms that the character trait of openness are more likely to use communication anonymizers.

With regard to our second research question, we find that the path coefficients from both stated and actual Internet Privacy Literacy to 'Privacy Awareness' and 'Privacy Concerns' are significant (see Table 6). However, it seems worth to emphasize that the signs of the coefficients are inversed, which came as a surprise to us: The PL-S positively influences 'Privacy Awareness', whereas PL-A negatively influences 'Privacy Awareness'. This means that individuals who think that they possess a high knowledge about Internet privacy have a higher stated awareness of Internet privacy than individuals with lower PL-S. Individuals who actually dispose of that knowledge stated to be less aware of privacy problems than individuals with a lower PL-A.

We assume that this contradiction can be explained by a social desirability bias. A social desirability bias is the tendency of participants to answer questions in a manner that will be viewed favourably by others, which poses problems when relying on self-reports such as questionnaires (Crowne and Marlowe, 1960). Individuals who think that they know much about Internet privacy issues might also state that they are aware of those issues, as it can be assumed that 'Privacy Awareness' is a socially desirable attribute. Furthermore, individuals with a higher actual understanding of privacy issues might be more cautious in assessing their 'Privacy Awareness'. Further, the PL-S negatively influences the 'Privacy Concerns', as confirmed by Brecht et al. (2010), whereas the PL-A positively influences the 'Privacy Concerns'.

This means that individuals with a high degree of stated privacy literacy in fact turn out to be less concerned about privacy. However, individuals with a high degree of actual literacy are more concerned about privacy. We assume that individuals with high actual literacy can better assess privacy risks and might therefore be more concerned about them. In addition, we assume that individuals scoring high on PL-S might underestimate privacy risks, as they might think they can better evaluate and mitigate them (Brecht et al., 2010).

With regard to our third research question, we find that individuals are willing to wait slightly longer when using communication anonymizers. In our study, the medians of the TWT are higher for both 'broken' hyperlinks in the treatment group compared to the control group. Whereas the median of the TWT for the first 'broken' hyperlink for the 'anonymous surfer' group was 31 seconds, the 'non- anonymous surfer' group was willing to wait for 26 seconds. With regard to the second broken hyperlink, the 'anonymous surfer' group was willing to wait for 23 seconds, while the 'non- anonymous surfer' group had a median of 17 seconds. This indicates that there is a willingness to wait for anonymity among our participants. However, our sample size is quite small and the TWTs are not distributed normally.

6   Managerial Implications

There is a large percentage of individuals who know communication anonymizers but do not use them. While this is often believed to depend on the latency, we find that this is not the case. Although many participants complained about the latency, we still found that the Tor group was willing to wait significantly longer than the control group. Thus it can be stated that individuals are generally willing to accept latency.

A factor that can explain the discrepancy between knowledge about and usage of anonymizers, and that has not been described before, can be derived directly from our results: Participants who stated to know much about Internet privacy issues stated to have a high degree of privacy awareness but low privacy concerns. Inversely, participants who revealed a high degree of actual knowledge about Internet privacy issues often stated to have low privacy awareness but high privacy concerns. Therefore, many individuals do not seem to use communication anonymizers because they underestimate privacy threats and overestimate their capacity to mitigate them. Thus, in order to increase the general use of communication anonymizers, it seems advisable to inform individuals about privacy threats on the Internet in the first place. This seems more promising to increase user numbers than reducing latency.

7   Conclusion

Concerning our first research question about the influence of personality on the acceptance of communication anonymizers, we could show that only the character trait of neuroticism leads to higher privacy concerns. According to our results, the character trait of openness makes it more likely that an individual uses such anonymizers. Furthermore, the character traits of agreeableness, extroversion and conscientiousness did not show any influence privacy concerns, nor on the intention to use communication anonymizers.

As to our second research question on privacy knowledge, we found out that individuals with high values for stated 'Internet Privacy Literacy' will most likely score high on 'Privacy Awareness' but low on 'Privacy Concerns'. It can be concluded that the more an individual thinks to know about Internet privacy, the more she/he is aware of privacy issues and the less she/he is concerned about privacy risks.

However, the opposite turned out to be the case with individuals who score high on actual 'Internet Privacy Literacy', as they score low on 'Privacy Awareness' and high on 'Privacy Concerns' on average. This can be interpreted as follows: the more individuals really know about Internet privacy, the less they state to be comprehensively aware of privacy issues and the more they are concerned about privacy risks.

Concerning our last research question, we could show that many individuals are willing to wait for an increase of Internet privacy. Although the difference of the TWTs between both control groups was only significant for the first 'broken' hyperlink, the medians of the TWTs for both 'broken' hyperlinks were larger among the participants of the treatment group (i.e., the anonymous surfers).

References

Barrick, M.R., Mount, M.K. and Judge, T. (2001). Personality and Performance at the Beginning of the New Millennium: What Do We Know and Where Do We Go Next? International Journal of Selection and Assessment (9), 9-30.

Brecht, F., Fabian, B., Müller, S. and Kunz, S. (2011). Are you willing to wait longer for Internet privacy? In Proceedings of the European Conference on Information Systems.

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.

Clark, J., van Oorschot, P.C. and Adams, C. (2007). Usability of Anonymous Web Browsing: An Examination of Tor Interfaces and Deployability. Symposium On Usable Privacy and Security (SOUPS).

Cohen, J. (1988). Statistical Power Analysis for the Behavioral Sciences . Lawrence Erlbaum Associates, 2nd edition, NJ: Hillsdale.

Conchar, M.P., Zinkhan, G.M., Peters, C. and Olavarrieta, S. (2004). An Integrated Framework for the Conceptualization of Consumers' Perceived-Risk Processing. Journal of the Academy of Marketing Science, (32) 4, 418-436.

Crowne, D.P. and Marlowe, D. (1960). A new scale of social desirability independent of psychopathology. Journal of Consulting Psychology, (24), 349-354.

Davis, F.D., Bagozzi, R.P. and Warshaw P.R. (1989). Individual Acceptance of Computer Technology: a comparison of two theoretical models. MIS Quarterly, (35) 8, 982-1003.

Dinev, T. and Hart, P. (2004). Internet Privacy, Social Awareness, and Internet Technical Literacy – An Exploratory Investigation. In Proceedings of the 17th Bled eCommerce Conference.

Dingledine, R., Mathewson, N., and Syverson, P. (2004). Tor: The second-generation onion router. Proceedings of the 13th USENIX Security Symposium.

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. https://blog.torproject.org/blog/why-tor-is-slow/. Accessed 12-02-2011.

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. Freenet Project: http://freenetproject.org/. Accessed 12-02-2011.

Goldberg, L. R. (1990). An Alternative 'Description of Personality': The Big-Five Factor Structure, Journal of Personality and Social Psychology, (59), 1216-1229.

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.

Junglas, I and Spitzmüller, C. (2006). Personality Traits and Privacy Perceptions: An Empirical Study in the Context of Location-Based Services. In Proceedings of the International Conference on Mobile Business.

Korukonda, A.R. (2007). Differences that do matter: A dialectic analysis of individual characteristics and personality dimensions contributing to computer anxiety. Computers in Human Behavior, (23) 4, 1921-1942.

Korzaan M. and Boswell K.T. (2008). The influence of personality traits and information privacy concerns on behavioral intentions. Journal of Computer Information Systems, (48) 4, 15-24.

McCrae, R.R. (Ed.) (1992). The five-factor model: Issues and applications. Journal of Personality, (60)2.

McCrae, R.R., Costa, P.T. and Busch, C.M. (1986). Evaluating Comprehensiveness in Personality Systems: The California Q-Set and the Five-Factor Model. Journal of Personality, (54) 2, 430-446.

McCrae, R. and John, O. (1992). An introduction to the Five-Factor Model and its applications. Journal of Personality, (2), 174–214.

Nah, F.H. (2004). A Study on Tolerable Waiting Time: How long are Web individuals willing to wait? Behaviour & Information Technology, (23) 3, 153-163.

Nunally, J.C. and Bernstein, I. Psychometric Theory (1994). New York: McGraw Hill.

Pfitzmann, A. and Hansen, M.A. (2010). Terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management. Version 0.34, August 2010, http://dud.inf.tu-dresden.de/Anon_Terminology.shtml. Accessed 12-02-2011.

Ringle, C.M., Wende, S. and Will, S. (2005). SmartPLS 2.0 (M3) Beta, Hamburg, http://www.smartpls.de/. Accessed 12-02-2011.

Tor Project (2011). http://www.torproject.org/. Accessed 12-02-2011.

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.

Wendolsky, R., Herrmann, D. and Federrath, H. (2007). Performance Comparison of low-latency Anonymisation Services from a User Perspective. Proceedings of Privacy Enhancing Technologies, LNCS Volume 4776, 233-253.

Westin, A. (1967). Privacy and Freedom. Atheneum Publishers, New York.