Transactions on
Replication Research

Conceptual Replication DOI: 10.17705/1atrr.00061 ISSN 2473-3458

Re-Evaluating Internet Users' Information Privacy Concerns: The Case in Japan

Sebastian Pape
Chair of Mobile Business & Multilateral Security, Goethe University Frankfurt, 60323 Frankfurt, Germany
sebastian.pape@m-chair.de

Ana Ivan
Chair of Mobile Business & Multilateral Security,
Goethe University Frankfurt, 60323 Frankfurt, Germany
ana.ivan@m-chair.de

David Harborth
Chair of Mobile Business & Multilateral Security,
Goethe University Frankfurt, 60323 Frankfurt, Germany
david.harborth@m-chair.de

Toru Nakamura
Information Security Laboratory, KDDI research, Inc.,
2-1-15 Ohara, Fujimino-shi, Saitama, 356-8502, Japan
tr-nakamura@kddi-research.jp

Shinsaku Kiyomoto
Information Security Laboratory, KDDI research, Inc.,
2-1-15 Ohara, Fujimino-shi, Saitama, 356-8502, Japan
kiyomoto@kddi-research.jp

Haruo Takasaki
Information Security Laboratory, KDDI research, Inc.,
2-1-15 Ohara, Fujimino-shi, Saitama, 356-8502, Japan
ha-takasaki@kddi-research.jp

Kai Rannenberg
Chair of Mobile Business & Multilateral Security,
Goethe University Frankfurt, 60323 Frankfurt, Germany
kai.rannenberg@m-chair.de

Abstract:

To expand the understanding of privacy concerns in the digital sphere, this paper makes use of the Internet Users' Information Privacy Concerns (IUIPC) model by Malhotra et al. (2004). The lack of empirical studies conducted in East-Asian societies makes it difficult, if not impossible, to shed light on multi-cultural differences in information privacy concerns of internet users. Therefore, we collected data of more than 9,000 Japanese respondents to conduct a conceptual replication of the IUIPC model. For our research goal, we re-assess the validity and reliability of the IUIPC model for Japan and compare the results with internet users' privacy concerns in the USA. Our results indicate that the second-order IUIPC construct, measured reflectively through the constructs awareness, collection, and control, is reliable and valid. Furthermore, three out of the five structural paths of the IUIPC model were confirmed for our Japanese sample. In contrast to the original study, the impact of IUIPC on trusting beliefs, as well as that of trusting beliefs on risk beliefs was negligible. Statistically significant differences in the IUIPC could only be found for the covariate gender.

Keywords: privacy concerns, IUIPC, Japan, partial least squares, IUIPC replication study

The manuscript was received 12/14/2017 and was with the authors 25 months for 3 revisions.

1 Introduction

With the information society in the digital age and personal data being referred to as the new oil, privacy and people's attitude about sharing personal data take an important role to retain self-determination with regard to one's personal information. Therefore, determining the factors influencing the privacy behavior of individuals has become a pivotal aspect in information-oriented societies. In particular, observing what influences individuals to disclose their personal data in spite of their concerns for privacy is a significant line of analysis.

One popular model in the privacy literature that tries to explain privacy concerns of online users is the one including the *Internet Users' Information Privacy Concerns (IUIPC)* construct by Malhotra et al. (2004), using data collected in the United States of America (USA). Their research targets involve a theoretical framework and an instrument for operationalizing privacy concerns (IUIPC) as well as a causal model for this construct. Their hypotheses, replicated fully in Section 2, involve the direct effect of IUIPC on trusting and risk beliefs, and the mediated effect on the intention of self-disclosure. The results of the analysis of Malhotra et al. (2004) suggest that the privacy concerns of users are reflected in a second-order construct with three main constructs: information collection, control, and awareness of privacy practices. In turn, the construct *Internet Users' Information Privacy Concerns (IUIPC)* has a statistically significant effect on the intention to self-disclose, which is mediated by the trust and risk beliefs of the users. These results are presented in

Figure 1.

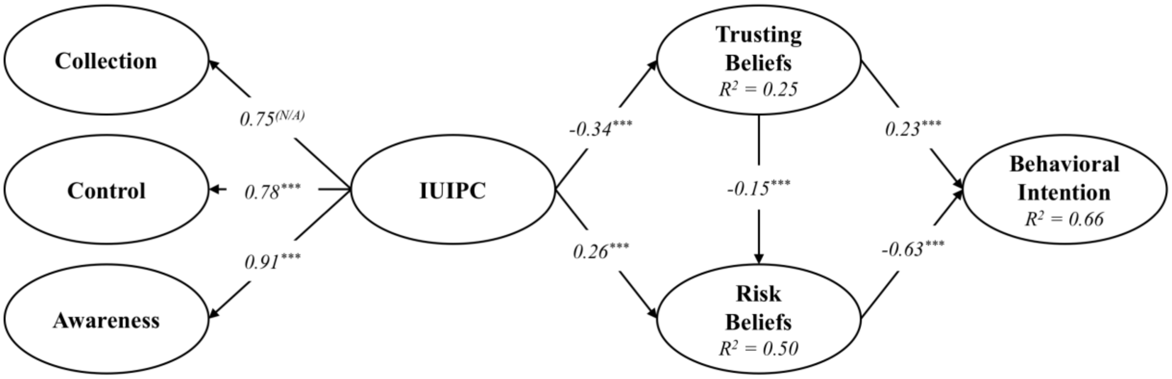

Figure 1. IUIPC Results of Malhotra et al. (2004).* p < 0.05, ** p < 0.01, *** p < 0.001

Several factors such as cultural differences (Wang, Norice, & Cranor, 2011) or different legislation between countries (Ishii and Komukai, 2016) are assumed to have decisive impact on individuals' privacy behavior. In this context, it is noteworthy that many papers do not consider this impact and just focus on Western societies (e.g. Europe or USA). Therefore, we chose Japan as a sample population for our research, as the existing literature shows significant cultural and societal differences to the views represented in the USA society. On the other hand, as the latest privacy incidents show, people in both countries are concerned about data leaks. Recent examples for such incidents in Japan are the Benesse case[1] in 2014, where a data leak affected more than 20 million people, and the leak of 1.25 million cases from Japan Pension Service staff computers[2] was discovered in 2015.

Due to the use prevalence of the IUIPC model and deviations which may occur across nations and across time, it is relevant to evaluate the validity of the IUIPC model in new contexts. This was already noticed by Malhotra et al. (2004, pg. 350): *"Thus it remains to be seen whether or not the results of this study retain their validity with different contextual variables."* and *"[…] the data collected for this study was specific to a given geographic location … care must be taken in any effort to generalize our findings beyond the boundary*

[1] https://www.japantoday.com/category/national/view/1789-file-y100-mil-damages-suit-against-benesse-over-data-leak

[2] https://www.databreaches.net/japans-pension-system-hacked-1-25-million-cases-of-personal-data-leaked/

of our sample." Thus, through a re-assessment of the same model in a country with different privacy views and at a later point in time, we aim to provide valuable insights on the general applicability of the model.

1.1 Background and Prior Replications

Privacy concern operationalizations and models have been integrated in various studies. Besides IUIPC, another instrument to measure information privacy concerns is the *concern for information privacy (CFIP)* by Smith et al. (1996) which was restructured by Stewart and Segars (2002). CFIP consists of four dimensions: *collection, unauthorized secondary use, improper access,* and *errors*. IUIPC is comprised of three dimensions: *collection, control,* and *awareness*. Since CFIP and IUIPC overlap in the *collection* dimension, combined they include six dimensions. According to Hong and Thong (2013), these six dimensions are the most popular dimensions in the existing literature.

Belanger and Crossler (2011) point out that even though Malhotra et al. (2004) showed that IUIPC explains more of the variance in a person's willingness to transact than CFIP, CFIP is still more widely used (cf. Osatuyi, 2015). Hong and Thong (2013) combined CFIP and IUIPC to develop the six-dimensional Internet Privacy Concerns (IPC) measure. Thus, with respect to the model of Malhotra et al. (2004), replication studies are scarce.

A closely related study investigating IUIPC is the one by Sipior et al. (2013) which confirms the constructs and most relationships within the model, but does not use structural equation modelling. The relationships which were not confirmed by Sipiro et al. are those between IUIPC and *risk beliefs*, and *trusting beliefs*, respectively. This finding can impact the quality of the IUIPC model, as *trusting and risk beliefs* are mediators of the relationship between IUIPC and the intention to share. However, the study of Sipior et al. (2013) only had a small sample size (63 respondents) and also was conducted in the USA. They conclude that IUIPC is not a valid scale for measuring privacy concerns.

We only found two applications of the IUIPC construct in Japan, the sample country of our analysis. Okazaki et al. (2009) aim to evaluate privacy concerns and their impact on preferences for regulatory control in mobile advertising. The authors adapt the initial IUIPC model by adding, for example, a construct for negative past experiences, which they hypothesize to influence the privacy concerns. In a second paper Okazaki et al. (2012) focus on consumers' acceptance of mobile advertising by considering the effects of perceived ubiquity. However, in addition to a smaller sample (510), Okazaki et al. focus on mobile advertising and therefore have a more limited scope than we have. Zukowski and Brown (2007) investigated the influence of demographic factors on IUIPC with 199 internet users from South Africa. However, they did not include *trust and risk beliefs* or any kind of *behavioral intention* construct. Yang and Miao (2008) studied the influence of IUIPC on users' intention to transact online in China. However, they only included *trust beliefs* and do not use *risk beliefs* in their research model. Nov and Wattal (2009) extended IUIPC with constructs for social norms and trust in community members and examined 192 Flickr users. Harborth and Pape investigated the influence of IUIPC on users' behavioral intentions to use privacy enhancing technologies (PET), namely JonDonym (Harborth and Pape, 2018) and Tor (Harborth and Pape, 2019). They also had a smaller sample size (141 and 124 users, respectively), a more limited focus on PET users and they extended the model of IUIPC by considering trust in the service provider of the PET.

Table 1 gives a brief overview about the identified studies. No current research was found to replicate the IUIPC model in a general context in Eastern societies. Furthermore, all of the studies deviate from the original model. Thus the need for a more recent replication is given.

Table 1. Overview of IUIPC Replications

Author	Year	Sample	Location	Comment	Replication
Zukowski and Brown	2007	199 internet users	South Africa	influence of demographic factors on IUIPC	Partially
Yang and Miao	2008	759 students	China	Did not use risk beliefs	Partially
Nov and Wattal	2009	192 Flickr users	Global	Focus on extensions for social norms and communities	Partially
Okazaki et al.	2009	510 mobile phone users	Japan	Focus on mobile advertising	Partially
Okazaki et al.	2012	510 mobile phone users	Japan	Focus on ad avoidance, no behavioral intention	Partially
Sipior et al.	2013	63 students	USA	No structural equation modelling used	Partially
Harborth and Pape	2018	141 JonDonym users	Global	Focus on Privacy Enhancing Technology	Partially
Harborth and Pape	2019	124 Tor users	Global	Focus on Privacy Enhancing Technology	Partially
Harborth and Pape	2020	124 Tor users	Global	Focus on Privacy Enhancing Technology	Partially

The remainder of this paper is organized as follows: in the next section, we discuss our research hypotheses. Section 3 outlines our methodology. Section 4 presents the results. A discussion and concluding remarks, along with some limitations and threats to validity are included in the final section.

2 Research Hypotheses

The research hypotheses of Malhotra et al. (2004) regard the coefficients of the causal (inner) model, which we present in this section. However, in order to replicate the inner model, the constructs need to be measured adequately, and fulfil reliability and validity criteria. Analyzing causal models for which IUIPC is used requires an analysis of how well IUIPC is measured. The replications we found mostly confirmed the IUIPC construct, expressed by data collection concerns, control over the user data, and awareness of privacy.

Existing literature indicates privacy differences between Western and Eastern societies (Mizutani, Dorsey, & Moor, 2004; Nakada and Tamura, 2005; Orito and Murata, 2005). For the understanding of privacy concerns in Japan it is helpful to have a look on the related legal framework. As emphasized by Tschersich et al. (2016) the legislation is centered around the "Act on the Protection of Personal Information", which was implemented in 2005. Recent work by Ishii and Komukai (2016) focuses on the liability and duties of data controllers regarding data leaks and compares the relevant legal schemes of Japan, the U.S., and the U.K. Other scientific contributions evaluate the evolution of privacy as a legal concept, and how the aforementioned act enforced it in various fields of the Japanese economy (Miyashita, 2011). In particular, Adams et al. (2009), discuss the Japanese sense of information privacy by distinguishing information privacy and physical privacy. They show evidence that social norms change from traditional values to limiting the sharing and use of personal information and developing legal responses for the breakdown of these norms. There is more work on the Japanese concept of privacy published in national venues, but unfortunately it is not published in English.

A primary contrast between Eastern and Western cultures is the relative focus on the good-of-the-group (collectivism) in the East versus the good-of-the-individual (individualism) in the West (Ralston, Holt, Terpstra, & Kai-cheng, 1997). Morris et al. (1994) claim that collectivism can be viewed as the subordination of personal goals under the goals of the group with an emphasis on sharing and harmony. Results by Cockcroft and Heales (2005) indicate that group collectivism has a considerable influence on the relationships within the IUIPC model, but they only had a sample size of 27. Chow et al. (1999) compare cultural factors for information sharing by interviewing managers in Taiwan and in Australia. Their results show a "sense of collective responsibility [...] to share information for the good of the company, even if doing so was potentially disadvantageous for the person concerned" for the Taiwanese respondents. Shin et al. (2007) show a positive relationship between collectivism and the attitude towards information sharing in China.

Further findings, e.g. from Orito and Murata (2005) underline that privacy is a “subjective and timeserving concept” (p. 1), resulting in a lesser expectation for privacy protection. They also invoke a linguistic argument, based on the fact that there is no Japanese word for privacy. As the word for that is an adapted English word, the authors expect it to conjure less meaning than it would to native speakers. As a consequence, a different perception of privacy between Japan and Western societies arises. In order to evaluate such differences, the model of Malhotra et al. (2004) can offer more explicit effects by investigating the mediators (*trusting and risk beliefs*). When forming our research hypotheses, we considered their results as well as the IUIPC re-testing results of Sipior et al. (2013). Although both studies were conducted in the USA, it was the best starting point to derive the hypotheses for our sample. The different results of these two papers are the relationships between IUIPC and *risk beliefs*, and between IUIPC and *trust beliefs*. Specifically, Malhotra et al. observe significant relationships, while Sipior et al. do not. However, since Sipior et al. do not use structural equation modelling and have a significant smaller sample, we adopt the hypotheses of Malhotra et al. (2004, pp. 341-342):

Hypothesis 1: IUIPC will have a negative effect on trusting beliefs.

Hypothesis 2: IUIPC will have a positive effect on risk beliefs.

Hypothesis 3: Trusting beliefs will have a negative effect on risk beliefs.

Hypothesis 4: Trusting beliefs will have a positive effect on the willingness to share.

Hypothesis 5: Risk beliefs will have a negative effect on the willingness to share.

Note that hypothesis 1, 2 and 3 remain unchanged, while hypothesis 4 and 5 reflect that we used “willingness to share” instead of “intention to give/release information” by Malhotra et al. for measuring the users’ intentions. The reason for this deviation from the original model is to ensure a more general applicability of our claims and to focus on the basic relationship between privacy concerns and the willingness to share. The original study is focused on individuals engaging in e-commerce transactions. However, there can be other reasons to share information, e.g. social networks or information which is valuable to the society, such as medical databases or information about the utilization of transport services which can be used to improve public transport or for traffic jam forecasts. Thus, our construct consists of three items asking if the user would share information in general, if there is a benefit for the user or if there is a benefit for the online company. As a consequence, we decided to not include the contextual variable “type of information” since we could not cover all kind of information types and develop corresponding scenarios for them.

3 Methodology

This section includes an assessment of whether our sample is representative for the Japanese population. Afterwards, we discuss the structural equation modelling approach for the analysis of the IUIPC model. In order to check for computation and implementation consistency, two software solutions were used: SmartPLS version 3 (Ringle, Wende, & Becker, 2015), as well as the package semPLS (Monecke and Leisch, 2012) in R (R Core Team, 2017).

3.1 Sampling Method and Sample Demographics

We conducted the online survey in 2015 with the help of the market research institute “Macromill Group”[3], which contained - amongst other items - the items used by Malhotra et al. (2004). The 9,287 respondents were selected with no bias towards location, marital status, or number of children. In contrast, Malhotra et al. (2004) “collected a total of 449 usable questionnaires from household respondents in one-on-one, face-to-face interviews”. Our decision for an online survey was motivated by the idea to get a larger sample along with the consideration that nowadays data sharing is mainly done online with computers or smartphones. One of the main drawbacks of online surveys is that one can only reach those who are online (cf. Hoogendorn and Daalmans, 2009). On the other hand, because of the interviewer’s presence respondents in face-to-face interviews are more susceptible to social desirability (Duffy et al., 2005). Given the sample demographics, studies from Duffy et al. (2005) suggest that online surveys attract a more knowledgeable, viewpoint-orientated sample and Szolnoki and Hoffmann (2013) and Hoogendorn and Daalmans (2009) find that online surveys attract respondents with better education and a higher income than face-to-face

[3] https://group.macromill.com

surveys. Summing up, our main goal was to achieve a large sample size. Since we could accept the discussed limitations, we decided to make use of an online survey.

The Japanese participants were balanced in terms of *gender*, with 50.53% males. With respect to the Japanese population, Statista identifies Japanese *internet users* to be 52.1% male (Ofcom, 2015). Due to the small difference, our sample can be considered as representative with respect to gender for the Japanese population. 54% of the respondents in the original study by Malhotra et al. (2004) were male.

Figure 2 shows an *age* comparison between our sample and the Statista numbers (Ofcom, 2015) of Japanese internet users, to allow a comparison of the representativeness of our sample. The only remarkable age differences are observed for users aged between 15 and 24, and between 45 and 54.

The median of the yearly *personal income* is between 2 and 4 million Yen (approximately between 16,500 and 33,000 Euro) in our survey, with an inter-quartile range of 2 to 3 million Yen. In an income study (Nensyu Labo, 2014), the median personal income in Japan was around 3 million Yen, while the interquartile range was also of about 3 million Yen. Thus, our sample exhibits no issues of representativeness with respect to income. Malhotra et al. (2004) observed "a median income of $60.000" in their sample. With respect to *education*, 49.5% of the Japanese people aged between 25 and 64 hold a Bachelor's degree (OECD, 2016), while in our sample 35.7% of the respondents in the same age group have the same education level. In total, 41.96% of our respondents hold at least a Bachelor's degree. 71% of the sample of Malhotra et al. (2004) held at least a bachelor's degree.

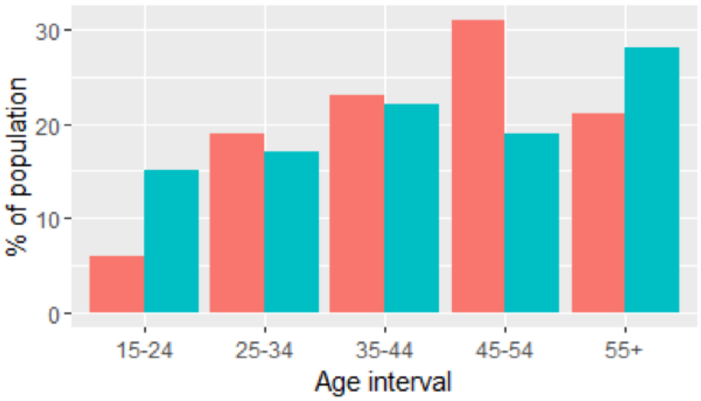

Figure 2. Age comparison between samples of Japanese internet users. Our sample is represented in red while the Statista sample is denoted in blue. Own figure generated in R with ggplot2 (Wickham, 2009).

3.2 Measurement Model

A required step in the analysis of any structural equation model is analyzing the measurement (outer) model. In this step, the constructs are evaluated for reliability and validity conditions. Since all the constructs are measured reflectively, the reliability must be assessed via internal consistency reliability and indicator reliability tests. Additionally, validity criteria are fulfilled if convergent validity and discriminant validity are exhibited (Hair, Ringle, & Sarstedt, 2011).

Malhotra et al. (2004, p. 341) assume a second-order structure for IUIPC. Therefore, we estimated this construct by using the repeated indicators approach (Wilson and Henseler, 2007). That means, the observable variables (i.e. questionnaire items) as indicators of the first order constructs are used as indicators of the second order construct IUIPC. One modification that we brought to the model of Malhotra et al. (2004) is that we used a self-developed construct, *willingness to share*, as a dependent variable. This construct was designed to measure the extent to which internet users are willing to share their personal information (as a behavioral intention). The specific items we used for our construct, *willingness to share*, as well as the items developed by Malhotra et al. (2004), which we used verbatim, are given in the Appendix.

3.3 Structural Model

The model following Malhotra et al. (2004) is used; the target is to examine whether there are any differences between the USA – represented in the original study by Malhotra et al. (2004) – and Japan with respect to the IUIPC construct and its relationship with the *willingness to share* construct (Hypotheses 1 to 5). As a conceptual replication, we did not include the contextual variable "type of information" (cf. Section 2.2). The results, reported in the section below, are obtained via structural equation modelling in SmartPLS 3.2.6 (Ringle et al., 2015). Non-parametric bootstrapping with 5,000 subsamples is used to test the significance of the obtained path coefficients. Additionally, we investigated demographic factors' influence on the IUIPC score. Specifically, we used a t-test for the gender effects, and Spearman rank-order correlation for the age, education, and income covariates. These tests were implemented using R (R Core Team, 2017).

4 Results

We found no computational differences for the results of the model between the two software platforms, SmartPLS and R. Therefore, we do not further distinguish between them in the following report.

4.1 Measurement Model

As a preliminary step before assessing the overall path models, reliability and validity are evaluated. Internal consistency reliability, or the property of a group of items measuring the same underlying concept, is analyzed via the composite reliability and Cronbach's Alpha. The values of both measures should be between 0.7 and 0.95 for research that builds upon accepted models. Values of Cronbach's α are seen as a lower bound and values of the composite reliability as an upper bound of the assessment. The values for both measures are within this range for all constructs, including the construct we developed, *willingness to share* (cf. Table 2). Analyzing the indicator reliability is related to understanding the extent to which a questionnaire item aids in predicting the variance of a certain construct. As we are undertaking a confirmatory study, we considered all items with a loading above 0.7 at a 95% significance level to be reliable. The only item with a loading below this threshold was Item 5 of the *risk beliefs* construct with a loading of -0.487. Hence, we decided to drop this item from the *risk beliefs* construct. The items we chose for our construct were acceptable with regard to their loadings and cross loadings (Table 3). One of the measures for validity that we check for is the average variance extracted (AVE), which measures convergent validity. This type of validity verifies whether the items chosen for one construct are, in fact, measuring the related construct. AVE values higher than 0.5 apply to all the constructs used, thus the constructs are valid, including the construct *willingness to share* (AVE equals to 0.752). The AVE values of the other constructs are shown in Table 2.

Discriminant validity ensures that there is no expression overlap between the constructs, and that they measure different phenomena. One tool for this measure is the cross-loading matrix, showing whether the used items are adequate for measuring only the construct they were assigned to. Specifically, this would ideally translate to high item loadings for the target construct, as well as low ones for the other constructs. Our results do not indicate that the items developed by Malhotra et al. (2004) have a higher loading for other constructs, apart from Item 5 of *risk beliefs* which we removed. This particular item has a loading with a higher magnitude for *trusting beliefs*. With regard to our own construct, *willingness to share*, discriminant validity is also given, as the items would not be adequate for any of the other constructs (see Table 3). Another method for assessing discriminant validity is the Fornell-Larcker criterion (Fornell and Larcker, 1981). This criterion indicates that discriminant validity is achieved when the square root of the AVE is larger than the maximum of the correlation between the considered construct and any other construct in the model. All constructs pass this discriminant validity test (cf. Table 2).

Table 2 Reliability and validity measures.

	Mean	SD	AVE	AWR	COLL	CTRL	IUIPC	RSK	TRST	WTS
AWR	14.20	3.35	0.842	**0.918**						
COLL	16.77	3.87	0.749	0.646	**0.865**					
CTRL	11.52	2.43	0.705	0.680	0.513	**0.840**				
IUIPC	0.00	1.00	1.000	0.901	0.865	0.811	**1.000**			
RSK	15.38	3.51	0.756	0.390	0.535	0.327	0.497	**0.870**		
TRST	16.37	4.36	0.731	-0.028	-0.101	0.081	-0.031	-0.050	**0.855**	
WTS	8.76	3.00	0.752	-0.193	-0.270	-0.074	-0.221	-0.175	0.368	**0.867**

SD = Standard Deviation
AVE = Average Variance Extracted
AWR = Awareness
COLL = Collection
CTRL = Control
IUIPC = Internet Users Information Privacy Concern
RSK = Risk Beliefs
TRST = Trusting Beliefs
WTS = Willingness to Share
The second part of the matrix is used for the Fornell-Larcker criterion: the bold values represent the square root of AVE, while the values under the main diagonal represent construct cross-correlations.

Table 3. Loadings and cross loadings for the items of the constructs

Items / Constructs	AWR	COLL	CTRL	IUIPC	RSK	TRST	WTS
AWR_01	**0.924**	0.575	0.626	0.823	0.352	-0.035	-0.170
AWR_02	**0.924**	0.567	0.634	0.821	0.347	-0.023	-0.159
AWR_03	**0.905**	0.635	0.613	0.837	0.373	-0.019	-0.203
COLL_01	0.470	**0.820**	0.377	0.672	0.459	-0.114	-0.252
COLL_02	0.630	**0.863**	0.505	0.796	0.421	-0.053	-0.206
COLL_03	0.599	**0.910**	0.459	0.789	0.477	-0.105	-0.257
COLL_04	0.522	**0.867**	0.423	0.728	0.499	-0.080	-0.225
CTRL_01	0.448	0.322	**0.802**	0.572	0.208	0.151	0.017
CTRL_02	0.578	0.436	**0.875**	0.698	0.284	0.087	-0.054
CTRL_03	0.661	0.510	**0.840**	0.753	0.318	-0.012	-0.130
IUIPC	0.901	0.865	0.811	**1.000**	0.497	-0.031	-0.221
RSK_01	0.328	0.446	0.281	0.418	**0.841**	-0.046	-0.147
RSK_02	0.252	0.408	0.227	0.354	**0.852**	0.003	-0.109
RSK_03	0.341	0.500	0.285	0.449	**0.908**	-0.057	-0.168
RSK_04	0.410	0.492	0.329	0.487	**0.876**	-0.061	-0.172
TRST_01	-0.039	-0.134	0.059	-0.057	-0.083	**0.854**	0.336
TRST_02	0.052	-0.048	0.130	0.040	-0.050	**0.881**	0.297
TRST_03	0.012	-0.071	0.096	0.003	-0.056	**0.877**	0.294
TRST_04	-0.043	-0.061	0.046	-0.031	0.022	**0.796**	0.301
TRST_05	-0.089	-0.106	0.026	-0.075	-0.039	**0.863**	0.338
WILL_BNF_COMP	-0.252	-0.292	-0.122	-0.270	-0.173	0.349	**0.909**
WILL_BNF_ME	0.007	-0.131	0.049	-0.041	-0.116	0.276	**0.770**
WILL_BNF_OTHER	-0.223	-0.262	-0.096	-0.237	-0.159	0.328	**0.915**
Cronbach's ∝	0.906	0.888	0.792	1.000	0.893	0.908	0.833
Composite Reliability	0.941	0.923	0.877	1.000	0.925	0.931	0.901

Table 3. Loadings and cross loadings for the items of the constructs

AWR = Awareness
COLL = Collection
CTRL = Control
IUIPC = Internet Users Information Privacy Concern
RSK = Risk Beliefs
TRST = Trusting Beliefs
WTS = Willingness to Share

4.2 Structural Model and Hypothesis Testing

Before assessing the results of the structural model, collinearity must be checked. Collinearity is present if two predictor variables are highly correlated with each other. To address this issue, we assess the inner variance inflation factor (inner VIF). All VIF values above 5 indicate that collinearity between constructs is present. For our model, the highest VIF is 1.002. Thus, collinearity is apparently not an issue.

The IUIPC construct yields large and statistically significant effects on *collection, control* and *awareness* (

Figure 3). The values are comparable to those obtained by Malhotra et al. (2004) for the USA sample. Our conclusion is that the IUIPC construct is also applicable in Japan for all of its three domains. However, our results differ in contrast to those obtained by Malhotra et al. (2004) with respect to *Hypothesis 1*. Specifically, despite a statistical significance, the impact of the IUIPC construct on *trusting beliefs* is negligible, with a coefficient value of -0.031. These results indicate that this relationship is not relevant for the case of Japan.

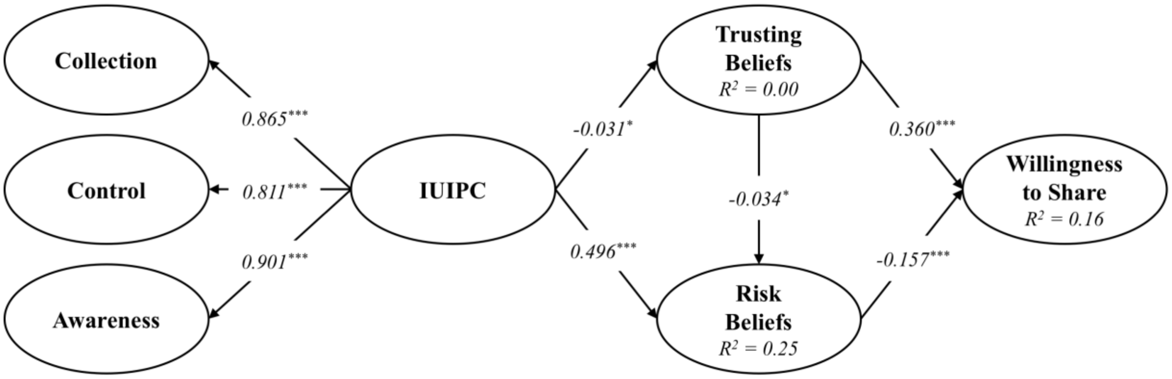

Figure 3. IUIPC model reproduction. Own figure. * p < 0.05, ** p < 0.01, *** p < 0.001

The relationship between IUIPC and the *risk beliefs* (*Hypothesis 2)* is positive and significant as in the original paper by Malhotra et al. (2004). However, the effect size for our Japanese sample is large (0.496), while the effect has only a medium size in the USA (0.26) (Malhotra et al., 2004). Testing *Hypothesis 3* – pertaining to the relationship between *trusting beliefs* and *risk beliefs* – yields different results from those obtained in the USA. Despite the fact that the *trust beliefs* have a statistically significant impact on *risk beliefs*, the impact is small enough to be negligible. Our results with respect to *Hypothesis 4* indicate a similarity between Japan and the USA. Specifically, our results are in line with those obtained by Malhotra et al. (2004) with a statistically significant positive medium-sized effect of *trusting beliefs* on the *willingness to share* and *behavioral intention,* respectively (0.36 and 0.23). Analyzing the impact of the *risk beliefs* on the *willingness to share* (*Hypothesis 5*) yields results decidedly different from the original paper (Malhotra et al. 2004). Namely, the effect, while significant and negative, is only medium in size in Japan (-0.157) compared to the large effect observed in the USA. A summary of the hypotheses can be found in Table 4.

Table 4 Hypothesis summary

Hypothesis	Result
1: IUIPC – negative –> Trusting Beliefs	Rejected (negligible effect)
2: IUIPC – positive –> Risk Beliefs	Confirmed
3: Trusting Beliefs – negative –> Risk Beliefs	Rejected (negligible effect)
4: Trusting – positive –> Willingness to Share	Confirmed
5: Risk Beliefs – negative –> Willingness to Share	Confirmed

With respect to fitting the data, this model yields an R^2 value of 0.16 for *willingness to share*. The *trusting beliefs* and *risk beliefs* have R^2 levels lower than those indicated by Malhotra et al. (2004). The lower R^2 levels provide a further indication that the Japanese users express their privacy concerns via different channels compared to their USA counterparts. In terms of model fit, the Normed Fit Index (Bentler & Bonett, 1980) has a value of 0.505 within the possible interval [0…1], where 1 applies to the perfect fit. The Standardized Root Mean Square Residual, which also takes values in the interval [0…1], with 0 being the best, has a value of 0.085. Other model fit measures, reported by Malhotra et al. (2004), are χ^2, the comparative fit index (CFI), goodness of fit index (GFI), root mean square error of approximation (RMSEA), and the consistent Akaike information criterion (CAIC). We calculated the indices with the *lavaan* package in R (Rosseel, 2012) (Table 5).

Table 5 Goodness of Fit indices with quality thresholds adapted from Malhotra et al. (2004)

Goodness of fit index (GFI)	Quality threshold	Current replication	Malhotra et al. (2004, p. 347)
χ^2	-	8449.77	290.36
CFI	> 0.95	0.94	0.95
GFI	> 0.90	0.91	0.93
RMSEA	< 0.06	0.066	0.059
CAIC	-	539600.5	567.53

Table 6 Assessment of effect sizes f^2 and q^2

Variables	f^2	q^2
Endogenous Exogenous	WTS	WTS
TRST	0.154	0.807
RSK	0.029	0.149

The f^2 effect size measures the impact of a construct on the endogenous variable by omitting it from the analysis and assessing the resulting change in the R^2 value. The values are assessed based on thresholds by Cohen (1988), who defines effects as small, medium and large for values of 0.02, 0.15 and 0.35, respectively. Table 6 shows the results of the f^2 evaluation. The results correspond to those of the previous analysis of the path coefficients, with TRST having a medium-sized effect on WTS and RSK having only a small effect on WTS.

The final step of the structural model assessment is the evaluation of the predictive relevance Q^2 and the associated effect sizes q^2. The Q^2 measure indicates the out-of-sample predictive relevance of the structural model with regard to the endogenous latent variables based on a blindfolding procedure. We used an omission distance of d=7. Recommended values for d are between five and ten (Hair, Ringle, & Sarstedt, 2011). Furthermore, we report the Q^2 values of the cross-validated redundancy approach, since this approach is based on both the results of the measurement model as well as of the structural model. For further information see Chin (1998). For our model, Q^2 is calculated for WTS. Values above 0 indicate that the model has the property of predictive relevance. In our case, the Q^2 value is equal to 0.114. Since it is larger than zero, predictive relevance of the model is established.

The assessment of q^2 (see Table 6) follows the same logic as the one of f^2. It is based on the Q^2 values of the endogenous variables and calculates the individual predictive power of the exogenous variables by omitting them and comparing the change in Q^2. The effect sizes have to be calculated with the following formula (Hair, Hult, Ringle, & Sarstedt, 2017):

$$q^2_{X \to Y} = \frac{Q^2_{included} - Q^2_{excluded}}{1 - Q^2_{included}}$$

All individual values for q^2 are calculated with an omission distance d of seven. The thresholds for the f^2 interpretation can be applied here, too. The results correspond to the previous results. *Trusting beliefs* have a strong predictive relevance for the *willingness to share*, whereas *risk beliefs* have only a small to medium-sized predictive relevance.

Our replication of the analysis by Zukowski and Brown (2007), regarding *covariate effects,* only confirmed the effects of gender on the privacy concerns in Japan. This finding is also reported by Tschersich et al. (2016). Specifically, a t-test for the gender shows a statistically significant difference in privacy concern levels of men and women. Specifically, women are found to be, on average, more concerned with respect to their privacy. Different from our study, Zukowski and Brown (2007, p. 201) do not observe this statistically significant gender difference.

5 Discussion and Conclusions

In this section, we present a brief discussion of the results, limitations to our study as well as a conclusion with implications for future work.

Interestingly, the effect of IUIPC on *trusting beliefs* is quite weak (*Hypothesis 1*). The other studies draw an inhomogeneous picture. Sipior et al. (2013) could not confirm a relationship between IUIPC and *trusting beliefs* (as well as *risk beliefs*). Okazaki et al. (2009, 2012) find this connection, but in the latter paper nothing depends on trust and in the earlier paper the relation between trust and the behavioral intention is not significant (2009). Yang and Miao (2008) also observed this relationship but they did not *consider risk beliefs*. Harborth and Pape (2018, 2019) found a relationship between IUIPC and *trust beliefs* in the case of PETs. In summary, it is not clear where this relatively small effect stems from and further research might be needed to investigate the trust concept in more depth. One possible explanation is that this is a consequence from broadening the scope, since we were not specific about the information type and the scenario (e.g. users could consider e-commerce, but others could also consider social media sites). In particular, Branzei et al. (2007) found that collectivists and individualists have distinct ways of building trust. Collectivists tend to rely more on situational signs than individualists who rely more on dispositional signs. Since users might have different trust levels towards different kinds of service providers, this could also weaken the connection in the model. However, since the relationship between IUIPC and *trust beliefs* could be observed in studies in other Asian countries, it is unlikely that it can be only attributed to cultural effects such as collectivism. Nevertheless, since none of the three other studies is an exact replication, this cannot be completely ruled out.

Considering the larger effect of IUIPC on *risk beliefs* (*Hypothesis 2*) as well as the lower effect of *risk beliefs* on the *willingness to share* (*Hypothesis 5*) compared to the original study, this means that even with an increase in *risk beliefs*, users still tend to share more information. Several possible explanations come to mind. This could be explained by the effects of collectivism where individuals have some *risk beliefs* but those stay mostly unconsidered when they share information (cf. Chow et al., 1999). On the other hand, we conducted the study more than 10 years later, thus it is also possible that the behavior of the population changed over time. Privacy concerns are not a static concept, they may change over time and they also may depend on the environment. While individuals might be more concerned, it could also happen that they become more insensitive due to daily media coverage or that they simply accept the loss of privacy associated with using online services (Hargittai and Marwick, 2016). An indication of this might be that the explanatory power of IUIPC was far lower than in the original paper by Malhotra et al. (2004) (cf. the R^2 values).

Interestingly, we found only a negligible effect (-0.03) of *trusting beliefs* on *risk beliefs* (*Hypothesis 3*) whereas the original study from Malhotra et al. (2004) indicated a small effect (-0.15). The only studies from Japan conducted by Okazaki et al. (2009, 2012) reported a larger and smaller effect size (-0.17 respectively -0.09) than the findings of Malhotra et al. However, Okazaki et al. did not use the trust construct from

Malhotra et al. but adapted a construct from Schlosser et al. (2006) instead, which referred to trust towards mobile advertisers. Therefore, the results cannot be compared directly. Yang and Miao (2008) conducted a study with IUIPC in China, but did not consider risk beliefs. In 2013, Sipior et al. aimed to reassess the IUIPC construct and could confirm the effect. They also had a small sample size from the USA and used a regression model, thus the effect size is not directly comparable. In three studies with international users of privacy enhancing technologies, Harborth and Pape (2018, 2019, 2020) found medium effect sizes (-0.33, -0.30, -0.27). Further literature with other constructs suggests that trust can reduce the perception of risk (cf. McCole et al., 2010; Jarvenpaa et al., 2000). However, Mayer et al (1995, p. 711) state that no consensus on the relationship of risk with trust exists: “It is unclear whether risk is an antecedent to trust, is trust, or is an outcome of trust.” This still seems to be the case nowadays. Therefore, further research is needed to investigate if the negligible effect is spurious, can be based on cultural aspects, or depends on variables not considered within our model.

The effect of *trusting beliefs* on the *willingness to share* (*Hypothesis 4*) is larger than in the original study. This fits to the effects of collectivism described in the discussion of Hypotheses 2 and 5 where individuals have some *risk beliefs* but those stay mostly unconsidered when they share information (cf. Chow et al., 1999). As a consequence, the relationship with *trusting beliefs* could gain importance for the *willingness to share* information. However, we can still not rule out that it is rather a result of a behavior change over time than a cultural influence.

Considering privacy concerns, the willingness to share information and trust and risk beliefs, one can assume that all of those change over time. Devices change, are ubiquitously integrated into the environment and one can suspect that people might get used to the devices as well as to sharing their data and therefore become less sensitive towards potential risks of sharing information. On the other hand, a rising number of data breaches (cf. Clement, 2019) and reports about them within the mainstream media could have an opposite effect of increasing concerns and risk beliefs and therefore lead to a decreased willingness to share data. While the necessity of longitudinal studies on privacy concerns (Keith et al., 2014) has already been recognized, most studies only cover a considerably short period (Boyd, 2011; Keith et al., 2014; ARF, 2019). The longest period, 5 years, was covered by Tsay-Vogel et al. (2018) who investigated Facebook users. They observe a more relaxed privacy attitude in general but an increased risk perception by heavy Facebook users. However, their user group was very specific and all participants were between 18 and 25 with 28% males. Thus, we are far from results which can be generalized. In summary, there is still the need of longitudinal studies, which is most likely the consequence of the difficulty to collect longitudinal information disclosure data.

Even though the correlation of IUIPC with age is significant, we consider it negligible in magnitude (0.113). Zukowski and Brown again obtain a different result from what we observed in Japan by accepting their hypothesis of an effect of age. Similarly, our correlation of IUIPC with the education and personal income levels yields negligible values of 0.03, and -0.05 respectively. Zukowski and Brown, however, do identify an effect of education, but also reject the effect of income.

5.1 Limitations and Threats to Validity

Despite the fact that our study benefits from a very large sample, the survey was conducted online compared to the face-to-face approach by Malhotra et al. (2004). Szolnoki and Hoffmann (2013) claim that face-to-face surveys deliver representative samples with the caveat that they tend to underrepresent individuals with university degrees. In contrast to this, better educated people with higher incomes tend to be overrepresented in online studies (cf. Szolnoki and Hoffmann, 2013; Hoogendorn and Daalmans, 2009). However, this bias does not seem to be an issue for our analysis (cf. Section 3.1).

According to Zukowski and Brown (2007) age as well as education have an effect on IUIPC, while gender, income level, and the internet experience do not. Even though the study of Zukowski and Brown (2007) was conducted in South Africa and we do not know whether their results can be transferred to Japan and/or the USA, we would have liked to compare the age distribution and the distribution of the education level to the distribution of the original study by Malhotra et al. (2004). Unfortunately, Malhotra et al. (2004) only provide the average age of their respondents (35 years), but did not provide any age distribution. As discussed in Section 3.1, our sample was not a perfect match to Japanese Internet users but had only a slight difference in the sample age distribution. Considering the education level, our sample was slightly below the education level of the entire Japanese population (no education level of Japanese Internet users was available) and considerably below the education level of the original study by Malhotra et al. (2004). Thus, effects from differences in the samples regarding age and education level cannot completely be ruled out.

Another limitation is that we adapted the behavioral intention from “intention to give/reveal information” to *willingness to share* and did not include the “type of information”. Since we were aiming for a more general scenario, the rationale why a user might share his or her information might be different from that in the original model.

In addition, we had to remove one item of the *risk beliefs* construct (IUIPC_RSK_05) since its loading was not above 0.7 at a 95% significance and it showed a higher loading for *trust beliefs*. However, given that this is a reverse scored item and the wording sounds already similar to the items of *trust beliefs* this is not too surprising. It may also be that the translation process made this issue worse. However, in none of the other studies we could find a report about this behavior.

5.2 Conclusion and Implications for Future Work

The main aim of the present study was to verify the applicability of the IUIPC model of Malhotra et al. (2004) in Japan, especially focusing on the comparison to the original USA sample as well as on changes due to differences in time when conducting the studies (difference of eleven years). Our results indicate that the IUIPC construct with its components *awareness, collection and control* is valid and reliable when applied within a Japanese sample. Its relationship to the behavioral intention construct (in our case *willingness to share*) is nonetheless not as clear as in the original paper about the USA. We observe that the connection between IUIPC and *trusting beliefs* is almost non-existent, in comparison to the medium-sized effect observed by Malhotra et al. (2004). Sipior et al. (2013) also observe no such relationship, but since their sample is relatively small and they do not use structural equation modelling, more research is needed in both Japan and the USA. Additionally, *trusting beliefs* has almost no impact *on risk beliefs* for our Japanese sample which was not the case in the USA.

The results of our first model confirmed our hypothesis that the Japanese privacy situation is different from that of the USA, as seen in the low R^2 of the dependent variable, *willingness to share*. The insight is that the standard IUIPC model is not sufficient to explain how the concerns of Japanese users affect their decision to share. The insights with respect to privacy concerns in Japan could be enhanced via studies analyzing the effect of other factors. For example, the existing literature indicates the potential of demographic aspects, cultural dimensions, situational cues etc. The influence of negative legal events could also be quantified as a construct in an extended model. Furthermore, the study at hand could be replicated in other countries to provide deeper insights with respect to cultural differences.

The implications of a better understanding of the factors and relationships of IUIPC can potentially enhance the protection of individual privacy. Additionally, it could facilitate the tailoring of public or corporate policies, trade agreements, international standardization, and the harmonization of laws for the online environment.

References

Adams, A. A., Murata, K., & Orito, Y. (2009). The Japanese sense of information privacy. *AI & society*, 24(4), 327–341.

Advertising Research Foundation (ARF) (2019). 2nd Annual ARF Privacy Study. White Paper. Retrieved from https://cdn.thearf.org/ARF_Knowledgebase/ARF%20WhitePapers/2019-Privacy-Study.pdf.

Belanger, F., & Crossler, R.E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly*, 35(4), 1017–1041.

Bentler, P. M., & Bonett, D. G. (1980). Significance tests and goodness of fit in the analysis of covariance structures. *Psychological Bulletin*, *88*(3), 588–606.

Boyd, A. W. (2011). A longitudinal study of social media privacy behavior. Retrieved from https://arxiv.org/pdf/1103.3174.

Branzei, O., Vertinsky, I., & Camp II, R. D. (2007). Culture-contingent signs of trust in emergent relationships. *Organizational Behavior and Human Decision Processes*, 104(1), 61-82.

Chin, W. W. (1998). The partial least squares approach to structural equation modeling. *Modern Methods for Business Research*, 295(2), 295-336.

Clement, J. (2019). Cyber crime: Number of breaches and records exposed 2005-2018. Retrieved from https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/.

Chow, C.W., Harrison, G.L., McKinnon, J.L., & Wu, A. (1999). Cultural influences on informal information sharing in Chinese and Anglo-American organizations: an exploratory study. *Accounting, Organizations and Society*, *24*(7), 561–582.

Cockcroft, S., & Heales, J. (2005). National culture, trust and internet privacy concerns. Paper presented at the *16th Australasian Conference on Information Systems*.

Cohen, J. (2013). *Statistical Power Analysis for the Behavioral Sciences*. Academic Press.

Duffy, B., Smith, K., Terhanian, G., & Bremer, J. (2005). Comparing data from online and face-to-face surveys. *International Journal of Market Research*, 47(6), 615–639.

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

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing Theory and Practice*, 19(2), 139–152.

Harborth, D. & Pape, S. (2018). JonDonym Users' Information Privacy Concerns. Paper presented at the *33rd IFIP International Conference on ICT Systems Security and Privacy Protection*, Poznan, Poland.

Harborth, D. & Pape, S. (2019). How privacy concerns and trust and risk beliefs influence users' intentions to use privacy-enhancing technologies – the case of Tor. Paper presented at the *52nd Hawaii International Conference on System Sciences (HICSS)*.

Harborth, D., & Pape, S. (2020). How privacy concerns, trust and risk beliefs, and privacy literacy influence users' intentions to use privacy-enhancing technologies: The case of Tor. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, 51(1), 51-69.

Hargittai E, & Marwick A (2016). 'What can I really do?' Explaining the privacy paradox with online apathy. *International Journal of Communication,* 10(4), 3737–3757.

Hong, W., & Thong, J. (2013). Internet privacy concerns: An integrated conceptualization and four empirical studies. *MIS Quarterly, 37*(1), 275–298.

Hoogendorn, A.W., & Daalmans, J. (2009). Nonresponse in the requirement of an Internet panel based on probability sampling. *Survey Research Methods*, *3*(2), 59–72.

Ishii, K., & Komukai, T. (2016). A comparative legal study on data breaches in Japan, the US, and the UK. Paper presented at the *IFIP International Conference on Human Choice and Computers*.

Jarvenpaa, S. L., Tractinsky, N., & Vitale, M. (2000). Consumer trust in an Internet store. *Information Technology and Management*, 1(1-2), 45-71.

Keith, M. J., Babb, J. S., & Lowry, P. B. (2014). A longitudinal study of information privacy on mobile devices. Paper presented at the *47th Hawaii International Conference on System Sciences*.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, 15(4), 336–355.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review*, 20(3), 709-734.

McCole, P., Ramsey, E., & Williams, J. (2010). Trust considerations on attitudes towards online purchasing: The moderating effect of privacy and security concerns. *Journal of Business Research*, 63(9-10), 1018-1024.

Miyashita, H. (2011). The evolving concept of data privacy in Japanese law. *International Data Privacy Law*.

Mizutani, M., Dorsey, J., & Moor, J. H. (2004). The internet and Japanese conception of privacy. *Ethics and Information Technology*, *6*(2), 121–128.

Monecke, A., & Leisch, F. (2012). semPLS: Structural equation modeling using partial least squares. *Journal of Statistical Software*, 48(3), 1–32.

M.H. Morris, D.L. Davis, & J.W. Allen (1994). Fostering corporate entrepreneurship: Cross-cultural comparisons of the importance of individualism and collectivism. *Journal of International Business Studies,* 25(1), 65–89.

Nakada, M., and Tamura, T. (2005). Japanese conceptions of privacy: An intercultural perspective. *Ethics and Information Technology*, *7*(1), 27–36.

Nensyu Labo (2014). 年収階層分布図. Retrieved from https://nensyu-labo.com/heikin_kaisou.htm.

Nov, O., & Wattal, S. (2009). Social computing privacy concerns: Antecedents and effects. Paper presented at the *SIGCHI Conference on Human Factors in Computing Systems*.

OECD. (2016). Adult education level (indicator). Retrieved from https://data.oecd.org/eduatt/adult-education-level.htm.

Ofcom. (2015). Distribution of internet users in Japan as of August 2015, by age group and gender. Retrieved from https://www.statista.com/statistics/276045/age-distribution-of-internet-users-in-japan/.

Okazaki, S., Li, H., & Hirose, M. (2009). Consumer privacy concerns and preference for degree of regulatory control. *Journal of Advertising*, 38(4), 63–77.

Okazaki, S., Molina, F. J., & Hirose, M. (2012). Mobile advertising avoidance: Exploring the role of ubiquity. *Electronic Markets*, 22(3), 169–183.

Orito, Y., & Murata, K. (2005). Privacy protection in Japan: Cultural influence on the universal value. Paper presented at *Ethicomp*.

Osatuyi, B., (2015). Empirical examination of information privacy concerns instrument in the social media context. *AIS Transactions on Replication Research*, 1, Paper 3, 1–14.

R Core Team, R Foundation for Statistical Computing (2017). *R: A language and environment for statistical computing.* R Foundation for Statistical Computing.

Ralston, D. A., Holt, D. H., Terpstra, R. H., & Kai-cheng, Y. (1997). The impact of natural culture and economic ideology on managerial work values: A study of the United States, Russia, Japan, and China. *Journal of International Business Studies*, 28(1), 177–207.

Ringle, C. M., Wende, S., & Becker, J.-M. (2015). *SmartPLS 3*. Bönningstedt.

Rosseel, Y. (2012). lavaan: An R Package for Structural Equation Modeling. *Journal of Statistical Software*, 48(2), 1–36.

Schlosser, A. E., White, T. B., & Lloyd, S. M. (2006). Converting web site visitors into buyers: How web site investment increases consumer trusting beliefs and online purchase intentions. *Journal of Marketing*, 70(2), 133-148.

Shin, S.K., Ishman, M. & Sanders, G.L. (2007). An empirical investigation of socio-cultural factors of information sharing in China. *Information & Management*, 44(2), 165–174.

Sipior, J. C., Ward, B. T., & Connolly, R. (2013). Empirically assessing the continued applicability of the IUIPC construct. *Journal of Enterprise Information Management*, 26(6), 661–678.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly,* 20(2), 167–196.

Stewart, K. A., & Segars, A. H. (2002). An empirical examination of the concern for information privacy instrument. *Information Systems Research,* 13(1), 36–49.

Szolnoki, G. and Hoffmann, D. (2013). Online, face-to-face and telephone surveys—Comparing different sampling methods in wine consumer research. *Wine Economics and Policy*, 2(2), 57–66.

Tsay-Vogel, M., Shanahan, J., & Signorielli, N. (2018). Social media cultivating perceptions of privacy: A 5-year analysis of privacy attitudes and self-disclosure behaviors among Facebook users. *New Media & Society*, 20(1), 141-161.

Tschersich, M., Kiyomoto, S., Pape, S., Nakamura, T., Bal, G., Takasaki, H., & Rannenberg, K. (2016). On gender specific perception of data sharing in Japan. Paper presented at *IFIP International Conference on ICT Systems Security and Privacy Protection*.

Wang, Y., Norice, G., & Cranor, L. F. (2011). Who is concerned about what? A study of American, Chinese and Indian users' privacy concerns on social network sites. Paper presented *at International Conference on Trust and Trustworthy Computing*.

Wickham, H. (2009). *ggplot2: Elegant Graphics for Data Analysis*. Springer Science & Business Media.

Wilson, B., & Henseler, J. (2007). Modeling reflective higher-order constructs using three approaches with PLS path modeling: A Monte Carlo comparison. Paper presented at the *Australian and New Zealand Marketing Academy Conference*.

Yang, H. L., & Miao, X. M. (2008). Concern for information privacy and intention to transact online. Paper presented at the *4th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM'08)*.

Zukowski, T., & Brown, I. (2007). Examining the influence of demographic factors on internet users' information privacy concerns. Paper presented at the Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on IT Research in Developing Countries (SAICSIT '07).

Appendix - Questionnaire Items

Awareness: items are taken from Malhotra et al. (2004, pp. 351-352)

- Companies seeking information online should disclose the way the data are collected, processed, and used. [IUIPC_AWR_01]
- A good consumer online privacy policy should have a clear and conspicuous disclosure. [IUIPC_AWR_02]
- It is very important to me that I am aware and knowledgeable about how my personal information will be used. [IUIPC_AWR_03]

Collection: items are taken from Malhotra et al. (2004, pp. 351-352)

- It usually bothers me when online companies ask me for personal information. [IUIPC_COLL_01]
- When online companies ask me for personal information, I sometimes think twice before providing it. [IUIPC_COLL_02]
- It bothers me to give personal information to so many online companies. [IUIPC_COLL_03]
- I'm concerned that online companies are collecting too much personal information about me. [IUIPC_COLL_04]

Control: items are taken from Malhotra et al. (2004, pp. 351-352)

- Consumer online privacy is really a matter of consumers' right to exercise control and autonomy over decisions about how their information is collected, used, and shared. [IUIPC_CTRL_01]
- Consumer control of personal information lies at the heart of consumer privacy. [IUIPC_CTRL_02]
- I believe that online privacy is invaded when control is lost or unwillingly reduced as a result of a marketing transaction. [IUIPC_CTRL_03]

Risk beliefs: items are taken from Malhotra et al. (2004, pp. 351-352)

- In general, it would be risky to give (the information) to online companies. [IUIPC_RSK_01]
- There would be high potential for loss associated with giving (the information) to online firms. [IUIPC_RSK_02]
- There would be too much uncertainty associated with giving (the information) to online firms. [IUIPC_RSK_03]
- Providing online firms with (the information) would involve many unexpected problems. [IUIPC_ RSK_04]
- I would feel safe giving (the information) to online companies. [IUIPC_RSK_05]

Trusting beliefs: items are taken from Malhotra et al. (2004, pp. 351-352)

- Online companies would be trustworthy in handling (the information). [IUIPC_TRST_01]
- Online companies would tell the truth and fulfil promises related to (the information) provided by me. [IUIPC_TRST_02]
- I trust that online companies would keep my best interests in mind when dealing with (the information). [IUIPC_TRST_03]
- Online companies are in general predictable and consistent regarding the usage of (the information). [IUIPC_TRST_04]
- Online companies are always honest with customers when it comes to using (the information) that I would provide. [IUIPC_TRST_05]

The items for the *willingness to share* construct are:

- If I see a benefit for myself, I am in general willing to share personal information with online companies. [WILL_BNF_ME]
- I am in general willing to share personal information with online companies. [WILL_BNF_OTHER]
- I'm in general willing to share personal information with online companies, if I see a benefit for them. [WILL_BNF_COMP]

About the Authors

Sebastian Pape is a senior researcher working at the Chair of Mobile Business & Multilateral Security at Goethe University Frankfurt. He successfully completed diplomas in mathematics (Dipl.-Math.) and computer science (Dipl.-Inform.) at Darmstadt University of Technology and holds a doctoral degree (Dr. rer. nat.) from the University of Kassel. From 2005 to 2011, he worked as research and teaching assistant at the Database Group (lead by Prof. Dr. Lutz Wegner) at the University of Kassel. From 2011 to 2015, he was a senior researcher and teaching assistant at the Software Engineering for Critical Systems Group (lead by Prof. Dr. Jan Jürjens) at TU Dortmund University. From October 2014 to January 2015, he was a visiting researcher (of Prof. Dr. Fabio Massacci) at the security group at the University of Trento. From October 2018 to August 2019 he was standing in as a professor for business informatics at Regensburg University.

Ana Ivan obtained her M. Sc. with specializations in Information Management and Finance at the Goethe University in Frankfurt. Her Master thesis focused on identifying the impact of constructs such as the privacy concerns on the behavioral intention of mobile app usage, using a SEM approach. She held a Student Assistant position at the Chair of Mobile Business and Multilateral Security during her studies, and now works as a data scientist.

David Harborth works at the Chair of Mobile Business & Multilateral Security at Goethe University Frankfurt am Main as a research assistant and PhD student since 2015. His major area of research deals with the socio-economic and technical issues of Augmented Reality (AR) as well as privacy-enhancing technologies and the related human aspects. He published his research in outlets like the International Conference on Information Systems, IEEE International Symposium on Mixed and Augmented Reality, Proceedings on Privacy Enhancing Technologies Symposium or Behaviour & Information Technology.

Toru Nakamura was born in 1983. He received the B.E., M.E., and Ph.D degree from Kyushu University, in 2006, 2008, and 2011, respectively. In 2011, he joined KDDI and in the same year he moved to KDDI R&D Laboratories, Inc. (currently renamed KDDI Research, Inc.). In 2018, he moved to Advanced Telecommunications Research Institute International(ATR). Since 2020, he is a researcher in KDDI Research, Inc. again. He received CSS2016 SPT Best Paper Award. His current research interests include security, privacy, and trust, especially privacy enhanced technology and analysis of privacy attitudes. He is a member of IEICE and IPSJ.

Shinsaku Kiyomoto received his B.E. in engineering sciences and his M.E. in Material Science from Tsukuba University, Japan, in 1998 and 2000, respectively. He joined KDD (now KDDI) and has been engaged in research on stream ciphers, cryptographic protocols, and mobile security. He is currently a senior researcher at the Information Security Laboratory of KDDI Research, Inc. He was a visiting researcher of the Information Security Group, Royal Holloway University of London from 2008 to 2009. He received his doctorate in engineering from Kyushu University in 2006. He received the IEICE Young Engineer Award in 2004 and Distinguished Contributions Awards in 2011. He is a member of IEICE and JPS.

Haruo Takasaki received the Bachelor of Laws from Tohoku University, Sendai, Japan, in 1980, and Ph.D. degrees in economics from Kyushu University, Fukuoka, Japan in 2018. In 1980, he joined Kokusai Denshin Denwa (KDD, later changed to KDDI) and has a lot of experience in the field of telecommunication. He has moved to KDDI Research Institute in 2005. Since then, he has researched in the field of privacy regulation and economics of privacy. He was certified as Privacy Design Ambassador from Privacy Commissioner of Ontario, Canada, in 2014.

Kai Rannenberg holds the Chair of Mobile Business & Multilateral Security at Goethe University Frankfurt since 2002. He is also a visiting professor at the National Institute for Informatics (Tokyo, Japan) since 2012, chair of the CEPIS Legal & Security Issues Special Interest Network since 2003 and an vice president of IFIP since 2015. Since 2007 he is convenor of ISO/IEC JTC 1/SC 27/WG 5 "Identity management & privacy technologies". From 2004-2013 he was academic expert in the Management Board of EU Network and Information Security Agency, ENISA and from 2013 till 2020 member of ENISA's Advisory Group. Kai has coordinated several leading EU research projects, e.g. the Network of Excellence "Future of Identity in the Information Society (FIDIS)" and the Integrated Project "Attribute based Credentials for Trust" (ABC4Trust). Currently he is coordinating CyberSec4Europe, a pilot for the European Cybersecurity Competence Network the EU is aiming for. Kai's research interests include: mobile and embedded systems and multilateral security; privacy and identity management, especially attribute based authorization; communication infrastructures and devices; Security and privacy standardisation, evaluation, and certification.