Critical Privacy Factors of Internet of Things Services: An Empirical Investigation with Domain Experts

Tobias Kowatsch[1] and Wolfgang Maass[2]

[1] Institute of Technology Management, University of St.Gallen,
Dufourstrasse 40a, CH-9000 St.Gallen, Switzerland
tobias.kowatsch@unisg.ch

[2] Chair in Information and Service Systems, Department of Law and Economics,
Saarland University, P.O. 15 11 50, 66041 Saarbrcken, Germany
wolfgang.maass@iss.uni-saarland.de

Abstract. Internet of Things (IOT) services provide new security and privacy challenges in our everyday life. But no empirical instrument has been developed for the class of IOT services that identifies privacy factors that predict usage intentions and individuals' willingness to provide personal information. The contribution of this paper is to address this lack of research. The proposed research model integrates the Extended Privacy Calculus Model and the Technology Acceptance Model and is pre-tested with 30 IOT experts. Results indicate that intentions to use IOT services are influenced by various factors such as perceived privacy risks and personal interest. It is further assumed that factors such as legislation, data security or transparency of information use influence the adoption of IOT services. Accordingly, further research must focus on a better understanding of these factors to increase the adoption of both useful and secure IOT services.

Keywords: Privacy, Security, Internet of Things, Extended Privacy Calculus Model, Technology Adoption Model, Empirical Study.

1 Introduction

With the increasing amount of Internet of Things (IOT) services, i.e. sensor-based IS services facilitated by identification technologies such as barcode, radio frequency or global satellite communication, people face new security and privacy challenges in their private and business life [23]. For example, mobile applications such as Foursquare, Facebook Places, Google Places or Groupon track the location of their users to provide an added value by the underlying contract: give up a little of your privacy, and you get worthwhile information. In case of the above-mentioned examples, the tracking of location-based information becomes obvious to a user, as she is aware of it by intentionally using them. However, sometimes it is not obvious which kind of information gets tracked at which time,

H. Rahman et al. (Eds.): MCIS 2012, LNBIP 129, pp. 200–211, 2012.

e.g., when those services are running in the background or when the user forgets to terminate them. Serious consequences might be, for instance, when that information is linked to Twitter or Facebook and is then used to commit crimes such as breaking into an empty home. Nevertheless, there exist also situations in which personal information is being intentionally recorded in the background. For example, a health monitoring service must track constantly critical health parameters of an individual without notifying her about it all the time.

In this regard, it is therefore of utmost importance to better understand usage patterns and perceptions from an end-user perspective such that IOT services can be designed with appropriate privacy and security standards in mind. Accordingly, the relevance of privacy and security-related topics has been addressed by prior IS research to a great extent. In particular, an IS Security Design framework, IS security guidelines [21] and IS security objectives [9] have been identified primarily in the context of (business) organizations. An in-depth review of literature on information privacy in the IS field is provided by [5].

However, to the best of our knowledge, no empirical instrument has been developed and tested for the class of IOT services that reveals significant predictors of IOT service usage in business situations and private situations. IOT services differ particularly from other IT-related applications in traditional office or home office situations due to their ubiquitous and embedded characteristics that pervade everyday life. Thus, privacy concerns due to unobtrusive data collection methods are more critical for this class of applications and appropriate evaluation instruments are required.

From a theoretical point of view, we ground the current work on utility maximization theory [3,20] and the privacy calculus model [10,16]. We hereby argue that as long as IOT services are perceived as being useful and the higher the individual or organizational interest in using them are the lower are privacy concerns and thus, the higher are adoption rates of such kind of services.

The contribution of this paper is therefore to present results of an empirical study on privacy concerns, rationales and potential ways of overcoming the privacy fears of IOT services that are currently discussed in the European IOT community. This paper will further provide a detailed plan of how an impact assessment of the initially identified IOT services can be carried out. For that purpose, a corresponding research model is proposed and empirically pre-tested with 31 IOT experts. This research model comprises critical factors that predict usage intentions of IOT services and individuals' willingness to provide personal information in order to use them appropriately.

In the following, the research model and hypotheses are presented. Accordingly, two empirical models from privacy research — the Extended Privacy Calculus Model [10] — and from IT adoption research — the Technology Acceptance Model [7] — are combined and tailored to the concept of IOT services. In a next step, the research methodology is described and the results are then presented. This paper concludes with a discussion of the results and gives an outlook on future work.

2 Research Model and Hypotheses

The research model and hypotheses of the current study are depicted in Fig. 1. The rational for the hypothesized relationships among the constructs is given in the following paragraphs.

The theoretical constructs and their relationships are primarily derived from the Extended Privacy Calculus Model (EPCM) [10]. EPCM has been successfully tested in the domain of electronic commerce and proposes the following privacy factors that influence the willingness to provide personal information for Internet transactions: perceived Internet privacy risk, Internet privacy concerns, Internet trust and personal Internet interest. The underlying assumption of EPCM is grounded in two contradicting predictors that both influence the willingness to provide personal information positively and negatively at the same time. That is, perceived Internet privacy risks and Internet privacy concerns are risk beliefs that negatively influence the willingness to provide personal information for Internet transactions, whereas Internet trust and personal Internet interest have a positive relationship with the willingness of providing personal information. Overall, these constructs from EPCM can be appropriately tailored to the concept of an IOT service as the latter can also trigger transactions of information on the Internet but with the help of interconnected physical objects.

In addition, two constructs from the Technology Acceptance Model (TAM) [7] were considered in the current work. That is, perceived usefulness and the intention to use IT. Having its roots in the Information Systems discipline, TAM describes determinants of technology adoption and was published in various variations in the past [8,13,22]. TAM is rooted in the social sciences, in particular, the theory of reasoned action [2] and its successor, the theory of planned behavior [1]. Both theories fundamentally state that individuals beliefs influence behavioral intentions that, in turn, have an effect on actual behavior. The target behavior of interest in the IS community was then the adoption of IS artifacts and their sustainable usage that might have positive effects on organizational key performance indicators.

Both EPCM and TAM have been incorporated in the current research to address critical privacy factors and technology factors that are relevant to social acceptance and impact evaluation of IOT services. The definitions of the seven constructs are adapted from [10, p.64] and [7, p.320ff] such that they apply to the concept of IOT services. Hereby, IOT services are defined as sensor-based IS services that support people in business situations and private situations. The five definitions as adapted from EPCM to IOT services are listed in the following:

- *Perceived IOT service privacy risk* is a perceived risk of opportunistic behavior related to the disclosure of personal information of IOT service users in general.
- *Privacy concerns against IOT service* are concerns about opportunistic behavior related to the personal information transferred to the IOT service by the individual respondent in particular.

- *Trust in organization providing the IOT service* is a trust belief reflecting confidence that personal information transferred to the IOT service organization will be handled competently, reliably, and safely.
- *Personal interest in IOT service* reflects the cognitive attraction to an IOT service while overriding privacy concerns.
- *Willingness to provide personal information* for IOT service represents the degree to which an individual is likely to provide personal information such as location-based information or financial information required to complete transactions of a particular IOT service.

The following two constructs are adapted from TAM whereby perceived usefulness was reworded as expected usefulness due to the prospective character of the current study on future IOT services:

- *Expected Usefulness of IOT service* is defined as the degree to which a person believes that using this IOT service would enhance his or her overall performance in everyday situations.
- *Intention to use IOT service* reflects behavioral expectations of individuals that predict their future use of the IOT service.

Two modifications were made in order to combine EPCM and TAM. First, intention to use was included as construct that mediates the impact on the willingness to provide personal information. The rationale for this relationship lies in the fact that an individual person would not provide his or her personal information for a particular IOT service without intending to use that service [1]. In line with theory of planned behavior, usage intention predicts therefore actual usage of an IOT service that also involves divulging personal information such as financial information or location-based information. Second, expected usefulness of an IOT service was added as construct that influences intentions to use that service. The rationale here is that IOT services are more likely to be adopted when they are perceived useful. This relationship was directly adopted from TAM [7]. It must be noted that perceived ease of use from TAM is not used in the current work as the focus lies on future IOT services. It is therefore not possible to measure ease of use at this early stage of investigation, i.e. without a prototypical implementation that could be physically tested.

In summary, the eight hypotheses as depicted in Fig. 1 are derived from EPCM, TAM and the assumptions discussed above. Additionally, it is investigated how contextual factors may influence these relationships. Three approaches are considered. First, it was done exploratory by varying the type of situations in which an IOT service is being used. Hereby, we contrast business situations, e.g., using an IOT service for business traveling purposes, with private situations, e.g., using an IOT service in a smart home environment. Second, we further investigate which kind of legislative body should be involved when it comes to privacy policies and data protection. And finally, we also evaluate information transparency, i.e. the detail of information and frequency of notification a user of an IOT service should get such that tracking of personal data is transparent enough.

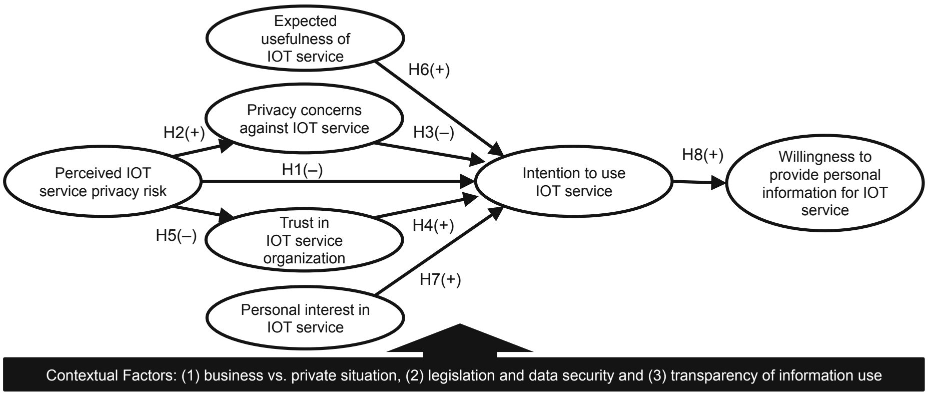

Expected usefulness of IOT service
Privacy concerns against IOT service
Perceived IOT service privacy risk
Trust in IOT service organization
Personal interest in IOT service
Intention to use IOT service
Willingness to provide personal information for IOT service
H1(–)
H2(+)
H3(–)
H4(+)
H5(–)
H6(+)
H7(+)
H8(+)
Contextual Factors: (1) business vs. private situation, (2) legislation and data security and (3) transparency of information use

Fig. 1. Research Model

3 Method

In order to pre-test the research model, a questionnaire-based survey was developed. For this reason, four IOT services embedded in two business situations and two private situations were identified from a pool of more than 50 IOT situations [19]. The services have been selected and adapted from several EU projects, including SmartSantander, SENSEI, eSENSE, EXALTED, FLORENCE, PROSENSE, LOLA and MIMOSA. The rationale behind the evaluation of situational descriptions of IOT services is based on a design method, in which situational descriptions are evaluated as an early step of the development of a Ubiquitous Information System [12].

The identification of relevant IOT services was conducted in two steps. First, an overall relevance score was calculated for each IOT service based on data from an existing online survey [19]. In that survey, 211 subjects selected some of the proposed IOT services and indicated their (1) degree of interest in that IOT service, (2) the degree to which the IOT service might increase the quality of life, (3) the relevance of that IOT service to society, (4) the relevance of the IOT service to business, (5) the market maturity and finally, (6) the technology maturity related to that particular IOT service. Hereby, five-point Likert scales ranging from low (1) to high (5) were employed. First, the means of each of the six statements were calculated. Then, each mean value was multiplied with the number of responses that reflects the relevance of a particular IOT situation. This intermediary score was then multiplied by one, two or three in case the mean value lies significantly above the neutral scale value of three (neither) at the .05, .01 or .001 level by applying one-sample t-tests. The resulting raw relevance score was therefore higher the higher the mean values of the questionnaire items, the more responses an IOT service had and the higher the significance level was. Finally, the overall relevance score was calculated by the sum of the six scores for each statement as described above.

In the second step, the resulting IOT services were ranked according to the overall relevance score. The following four best-ranked IOT services embedded in business situations and private situations have been chosen for the current study:

1. *Public Transport Payment (PTP) Service:* You are taking the bus to work or during a business trip and you receive a message via your mobile phone that you will be charged once you get off the bus based on the number of zones you cross. The information also displays the cost per zone. Payment is performed automatically via your mobile phone. (Business Situation)
2. *Navigation (Nav) Service:* You just finished your morning routine and are getting ready to leave your home for a business trip. You receive detailed information about traffic conditions including traffic accidents, traffic jams, weather conditions and parking possibilities directly integrated into your personal navigation service. It routs you — including driving, walking, public transport and car-pooling — in the most efficient way and as close as possible to your destination. Persons (incl. you), cars and public transport share their location-based information together with other data relevant for the navigation service in the Internet cloud. (Business Situation)
3. *Smart Home (SH) Service:* The Smart Home service provides the complete control of your house. It switches the lights automatically on when you enter and switches them off when you leave a room. Arriving home after work, your face is recognized at the entrance and the electronic key in your pocket is detected. This service triggers the heating system, by combining data from outdoor and indoor temperature, weather forecast from the Internet, and user preferences. It adjusts the house energy consumption to the real needs of the family, and most importantly it helps you save money. It also recognizes which appliances (washing machine, dishwasher, water heater, heating system, etc.) are turned on at a given time and synchronizes them to ensure the best energy efficiency taking into account the pricing structure of utility companies. (Private Situation)
4. *Health Monitoring (HM) Service:* Recently the doctors have diagnosed that Johns Alzheimer disease is taking a turn for the worse. As a result, his children have decided to upgrade the monitoring solution with sensor applications that enable the monitoring of his locations, posture and mental conditions at home and in the neighborhood. So John retains his private and social life, which is very important for coping with his condition and happiness. (Private Situation)

The questionnaire items of the EPCM constructs were adapted from [10] whereas expected usefulness and intention to use were adapted from [13] and [22]. Items for the contextual factors, i.e. legislative aspects on privacy and data security as well as information transparency, have been developed from scratch for this study (see also Fig. 2, Fig. 3 and Fig. 4). Finally, demographic data was collected. The complete survey instrument for each of the four IOT services can be obtained from [15].

4 Results

Overall, 26 male and 5 female subjects have evaluated the four IOT services during the IOT week in Barcelona in June 2011. This evaluation took 40 minutes on average. The subjects were domain experts as they were involved in IOT-related EU projects IOT-Architecture, IOT-Initiative or SmartSantander. Their age ranged from 25 to 64.

Descriptive statistics of the questionnaire items are listed in Table 1. With one exception, Cronbachs Alpha lies over the recommended threshold of .70 indicating good reliability of the scales employed [18]. Accordingly, aggregated means for each theoretical construct were calculated. Additionally, one-sample t-tests were used for each aggregated variable to indicate whether the means differ significantly from the neutral scale value of three. That is, one-sample t-tests show whether subjects have rated the constructs rather positively, neutral or negatively.

Table 1. Descriptive statistics. Format: Alpha, Mean, Std.Dev; * $p < .05$, *** $p < .001$, p-values from one-sample t-tests with test value = 3, N=31.

Construct	1. PTP Service			2. Nav Service			3. SH Service			4. HM Service		
Privacy risk	.866	3.32	0.92	.909	3.39*	0.89	.915	3.15	0.95	.906	2.90	0.94
Privacy concerns	.899	3.33	1.00	.960	3.38*	0.96	.931	3.35	0.96	.907	3.08	0.95
Trust in organization	.778	3.56***	0.69	.839	3.05	0.73	.906	3.27	0.86	.738	3.67***	0.71
Expected usefulness	.940	3.92***	0.90	.961	3.89***	0.72	.934	3.61***	0.77	.892	4.28***	0.55
Personal interest	.889	3.35	1.01	.922	3.35*	0.87	.942	3.25	0.96	.850	4.09***	0.56
Intention to use	.897	3.74***	0.91	.922	3.70***	0.92	.909	3.59***	0.76	.926	4.08***	0.61
Will. to provide info.	.860	3.03	1.13	.806	2.80	1.13	.721	2.89	0.98	.444	n/a	n/a

Consistent with prior research [13,14], partial least squares (PLS) analysis was used for data analysis of our research model. PLS belonging to structural equation modeling (SEM) was chosen over regression analysis, because SEM can analyze all of the paths in one analysis [4,11]. PLS allows analyzing the structural model for assessing the relationships among the theoretical constructs and the measurement model for assessing the validity and reliability of the questionnaire items. In our research, all theoretical constructs were modeled as reflective, because their items are manifestations of them [4] and are expected to correlate with each other [6].

In order to test the validity of our constructs, we performed a confirmatory factor analysis using SEM with the R package PLS-PM (Version 0.1-11) and the bootstrapping resample procedure with 400 iterations. Although one item had a factor loading below the recommended value of .70 (WP2 of the health monitoring service, for details on the item wording see [15]), we retained it to maintain continuity with the other three IOT services. All the other items loaded on their assigned latent variables. Thus, our scales show good convergent validity. The PLS path coefficients together with their significance levels for each hypothesis are shown in Table 2. These results show that only hypotheses H2 and H8 are supported by the empirical data for all four IOT services. H4 is to be rejected. The remaining hypotheses are only partly supported by the data.

Table 2. PLS path coefficients. Note: * $p < .05$, ** $p < .01$, *** $p < .001$, N=31.

Hypothesis	1. PTP Service	2. Nav Service	3. SH Service	4. HM Service	Result
H1: PR x IU	−.29	−.38*	−.69**	−.03	(accepted)
H2: PR x PC	.83***	.88***	.82***	.88***	accepted
H3: PC x IU	.08	.03	−.57*	−.14	(accepted)
H4: TO x IU	.01	−.02	.07	.04	rejected
H5: PR x TO	−.56**	−.38	−.52***	−.44*	(accepted)
H6: EU x IU	.54***	.36*	.63***	.22	(accepted)
H7: PI x IU	.20	.44*	.15	.55*	(accepted)
H8: IU x WP	.74***	.72***	.67***	.68***	accepted

The explained variances (R^2) for the dependent variables are shown in Table 3. Hereby, the predicting factors of perceived privacy concerns and the intention to use an IOT service explain a high degree of variance.

Table 3. Explained variances (R^2) from PLS analysis

Construct	1. PTP Service	2. Nav Service	3. SH Service	4. HM Service
Privacy concerns	.697	.773	.672	.776
Trust in organization	.345	.186	.288	.222
Intention to use	.805	.817	.735	.670
Will. to provide info.	.556	.523	.457	.469

Furthermore, descriptive statistics related to the questionnaire items on legislation and data security are presented in Fig. 2. Additionally, it was reported by an IOT expert that it is crucial to use only personal information where it is really necessary, i.e. organizations should not request and save personal information for its on sake or potential future use. Moreover, results on the preferred level of detail of notifications on personal information use are depicted in Fig. 3, whereas feedback regarding the frequency of notifications is shown in Fig. 4. One IOT expert reported that details on personal information use should only be made available to the user on request. By contrast, another expert pointed out that the user must confirm actively each transaction that transfers personal information to a third-party organization. With regard to the frequency of notification, one expert discussed the option that users should also be informed when the way of personal information use is being changed. A detailed discussion of these results is presented in the next section.

5 Discussion

5.1 Determinants of IOT Service Use

First, it can be stated that all four IOT services are perceived as relevant by the subjects of this pretest. That is, the values for expected usefulness of the four IOT services and intention to use these services lie all significantly above the neutral test value of three (cf. Table 1).

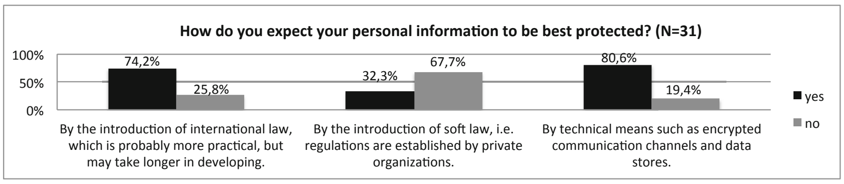
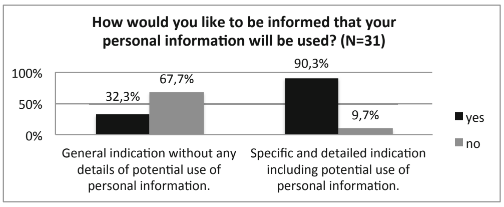


Fig. 2. Legislation and data security



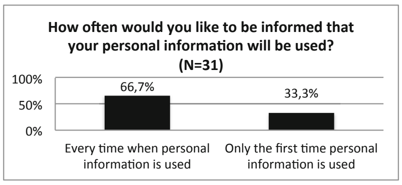


Fig. 3. Detail of notification

Fig. 4. Frequency of Notification

Second, though all of these IOT services are perceived as relevant, subjects have no distinct position on whether to provide personal information for those services or not. This fact is based on the construct willingness to provide personal information for IOT use that lies neither significantly above nor below the neutral scale value (cf. Table 1). Therefore, subjects are uncertain in terms of providing access to their personal information in general. It could only be shown for one item of the Health Monitoring service that subjects were willing to provide personal information. However, this result could be explained by the fact that subjects had to rate this item indirectly for another person, i.e. as a family member of John who suffers from Alzheimer disease and is not able to decide for himself.

Third, the current study has adapted the Extended Privacy Calculus Model [10] to the IOT domain with a focus on IOT services. This model describes critical privacy factors and was further extended with two constructs from the Technology Adoption Model [7]. In contrast to the proposed and hypothesized relationships, it could not be shown that the contradicting predictors — i.e. perceived IOT service privacy risk and privacy concerns against an IOT service on the one hand and trust in an organization providing the IOT service, expected usefulness of the IOT service and personal interest in the IOT service on the other hand — have a significant negative or positive impact on the intention to use that IOT service. One reason may be the different purposes of the IOT services. For example, a public transport payment service must be useful in the first instance to be adopted but for a smart home service also privacy concerns must be taken into account. Moreover, it can even be observed that trust in a service providing organization has no influence at all according to these results. That is, trust relative to, for example, expected usefulness is less important for the domain experts of the current pretest. Its effect size is probably too small to be identified by the current sample size of 31, too. Furthermore it is assumed that a more concrete description of the service providing organization would result in different findings.

Fourth, it must be noted that there exists no obvious pattern that distinguishes subjects evaluations of IOT services in business situations from private situations. A potential reason may be the fact that IOT services foster the convergence of both types of situations, i.e. they are permanently available no matter whether a person is at home, at the office or elsewhere. This fuzzy interference of perceptions might therefore also influence the perceptions of privacy risks and privacy concerns.

Finally and with regard to the high variances explained for privacy concerns and usage intentions (Table 3), it is argued that the privacy factors investigated in the current study are good predictors as far as they show a significant relationship in Table 2.

5.2 Legislation, Data Security and Transparency of Information Use

Results on legislation, data security (Fig. 2) and transparency of information use (Fig. 3 and Fig. 4) provide additional guidelines for the design and implementation of IOT services [9,21]. Accordingly, subjects expect their personal information to be primarily protected by international law, which is probably more practical, but may take longer in developing in contrast to soft law introduced by private organizations. In addition to these legislative aspects, personal information should be protected by technical means (Fig. 2). Thus, state of the art encryption and security standards should be incorporated and promoted together with the pure functionality of IOT services as such.

Furthermore, subjects made a point of requesting specific and detailed statements with regard to personal information use. Thus, brief and more general statements should be avoided when an IOT service is deployed or they should at least point to a detailed description such that users are able to request this information on demand (Fig. 3).

The majority of subjects, i.e. 66.7%, stated also that they want to be informed every time when personal information is used by an IOT service. However, also 33.3% of the subjects want to be informed only the first time. The default option should therefore be a trigger that informs users of an IOT service every time personal information is forwarded to a third-party organization. But IOT service providers should also provide the option to change this trigger (Fig. 4).

5.3 Limitations

The current study has several limitations. First, the results are biased in the sense that primarily male and technology-savvy persons have participated, i.e. subjects were experts in the field. But even though experts may adopt the proposed IOT services first, support from a more equally distributed sample is strongly required to increase external validity of the current findings. Second, with 31 subjects the sample size is quite limited to identify small effects. Thus, using PLS for hypotheses testing might not render significant path coefficients even though these coefficients differ obviously from zero (cf. Table 2, H5 of the Navigation Service). And third, because IOT experts can rely on their experience in the field, external validity of the results is limited with regard to the textual descriptions of IOT situations compared to drawings, video clips, or lab experiments that would all increase subjects understanding of the IOT services and thus the quality of evaluations. In particular, the construct trust in organization requires subjects to think about potential providers of those services, which adds a common method bias to the results.

6 Conclusion and Outlook

In this paper on critical privacy factors of future IOT services, the Extended Privacy Calculus Model [10] has been combined with the Technology Acceptance Model [7] and was pre-tested in the IOT domain by conducting a survey with 31 domain experts. As a result, preliminary factors have been identified that influence the adoption of IOT services and thus, might be critical in the design process of those services.

Future work will extend this research by conducting further studies in order to cross-check the current findings and thus, to increase the external validity and quality of implications. In doing so, the guiding research question remains: How can IOT services be designed such that they are not only useful and technically secure but also address privacy concerns of their users?

Acknowledgments. This work was co-funded by the European Union as part of the Internet of Things Initiative (IoT-I, FP7ICT20095257565).

References

1. Ajzen, I.: The theory of planned behavior. Organizational Behavior and Human Decision Processes 50(2), 179–211 (1991)
2. Ajzen, I., Fishbein, M.: Understanding Attitudes and Predicting Social Behaviour. Prentice Hall, Inglewood Cliffs (1980)
3. Awad, N.F., Krishnan, M.S.: The personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to be Profiled Online for Personalization. MIS Quarterly 30(1), 13–28 (2006)
4. Barclay, D., Thompson, R., Higgins, C.: The partial least squares (PLS) approach to causal modeling: Personal computer adoption and use an illustration. Technology Studies 2(2), 285–309 (1995)
5. Bélanger, F., Crossler, R.E.: Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. MIS Quarterly 35(4), 1017–1041 (2011)
6. Chin, W.W.: Issues and Opinion on Structural Equation Modeling. MIS Quarterly 22(1), vii–xvi (1998)
7. Davis, F.D.: Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. MIS Quarterly 13(3), 319–339 (1989)
8. Davis, F.D., Venkatesh, V.: Toward preprototype user acceptance testing of new information systems: Implications for software project management. IEEE Trans. on Engineering Management 51(1), 31–46 (2004)
9. Dhillon, G., Torkzadeh, G.: Value-focused assessment of information system security in organizations. Information Systems Journal 16(3), 293–314 (2006)

10. Dinev, T., Hart, P.: An Extended Privacy Calculus Model for E-Commerce Transactions. Information Systems Research 17(1), 61–80 (2006)
11. Gefen, D., Straub, D., Boudreau, M.-C.: Structural Equation Modeling Techniques and Regression: Guidelines for Research Practice. Communications of the Association for Information Systems 7(7), 1–78 (2000)
12. Janzen, S., Kowatsch, T., Maass, W.: A Methodology for Content-Centered Design of Ambient Environments. In: Winter, R., Zhao, J.L., Aier, S. (eds.) DESRIST 2010. LNCS, vol. 6105, pp. 210–225. Springer, Heidelberg (2010)
13. Kamis, A., Koufaris, M., Stern, T.: Using an Attribute-Based Decision Support System for User-Customized Products Online: An Experimental Investigation. MIS Quarterly 32(1), 159–177 (2008)
14. Komiak, S.Y.X., Benbasat, I.: The Effects of Personalization and Familiarity on Trust and Adoption of Recommendation Agents. MIS Quarterly 30(4), 941–960 (2006)
15. Kowatsch, T., Maass, W., Weber, R., Weber, R.: The Internet of Things Initiative (IOT-I) Deliverable 2.2: Initial Social Acceptance and Impact Evaluation, FP7 ICT project, contract number: 257565 (2011)
16. Laufer, R.S., Wolfe, M.: Privacy as a concept and a social issue: A multidimensional developmental theory. J. Soc. Issues 33(3), 22–42 (1977)
17. Moore, G.C., Benbasat, I.: Development of an instrument to measure the perceptions of adopting an information technology innovation. Information Systems Research 2(3), 192–222 (1991)
18. Nunnally, J.C.: Psychometric Theory. McGraw-Hill, New York (1967)
19. Presser, M., Krco, S.: The Internet of Things Initiative (IOT-I) Deliverable 2.1: Initial report on IoT applications of strategic interest, FP7 ICT project, contract number: 257565 (2011)
20. Rust, R.T., Kannan, P.K., Peng, N.: The Customer Economics of Internet Privacy. Journal of the Academy of Marketing Science 30(4), 455–464 (2002)
21. Siponen, M.T., Iivari, J.: IS Security Design Theory Framework and Six Approaches to the Application of IS Security Policies and Guidelines. Journal of the Association for Information Systems 7(7), 445–472 (2006)
22. Venkatesh, V., Morris, M.G., Davis, G.B., Davis, F.D.: User acceptance of information technology: Toward a unified view. MIS Quarterly 27(3), 425–478 (2003)
23. Weber, R.: Internet of Things - New security and privacy challenges. Computer Law & Security 23(1), 23–30 (2010)
24. Wixom, B.H., Todd, P.A.: A Theoretical Integration of User Satisfaction and Technology Acceptance. Information Systems Research 16(1), 85–102 (2005)