IOT – i

The Internet of Things Initiative

D2.2: Initial Social Acceptance and Impact Evaluation

Project acronym:	IOT-I
Project full title:	The Internet of Things Initiative
Grant agreement no.:	257565
Doc. Ref.:	IOT-I_DEL_D2.2_v1.5-110824.docx
Responsible:	HSG
Editor(s):	Kowatsch, T. and Maass, W. (HSG)
List of contributors	Kowatsch, T., Maass, W. (HSG), Weber, Rolf and Weber, Romana (UZH)
Reviewers	Presser, M. (AI) and F. Carrez (UniS)
Date of issue:	31/08/2011
Status:	Final
Security:	Public

Table of Contents

Table of Figures

Table of Tables

Section 1: Introduction

With regard to the description of work (DOW), this initial report contributes to the overall objective of Task 2.2 to evaluate the social acceptance and regulatory impact of IOT applications: "T2.2 will focus on non technical aspects of the IoT like societal, ethical and regulatory concerns and generate recommendations that would lead to a reduction of issues linked to the use of the IoT, resulting ultimately in a wider acceptance by the end-user" (IOT-I DOW, Proposal Part B, p. 17)

In particular, this deliverable "documents the initial results on an interactive study concerning potential privacy invasion of IoT technology. It will outline a set of concerns, rationales and potential ways of overcoming the privacy fears. It will further provide a detailed plan of how an impact assessment of the initially identified application areas can be carried out" (ibid., p. 30). Consistently, the relevance of privacy issues in combination with IT artefacts, and in particular IOT-based applications, has been addressed by prior research (Anderson and Moore, 2009; Angst and Agarwal, 2009; Dinev and Hart, 2006; Kosta and Dumortier, 2008; Little, 2008; Malhotra et al., 2004; Pramatari and Theotokis, 2009; Spiekermann, 2009; Weber, 2010). However and to the best of our knowledge, no empirical privacy instrument has been adapted to the class of IOT applications, which differ from other IT-related applications in traditional office or home office situations due to their ubiquitous and embedded characteristics that pervade every-day situations. Thus, privacy concerns due to unobtrusive data collection methods are more critical for this class of applications and appropriate evaluation instruments are required.

In order to address this lack of research and thus, the objectives of the DOW, a corresponding research model with a focus on privacy issues is proposed and empirically evaluated by a first user study with domain experts. This research model comprises critical privacy factors that predict the behavioural acceptance of IOT applications and the individuals' willingness to provide personal information for those applications. In addition, an instrument is presented and employed to measure the impact on legislative and regulatory aspects.

In the following, research model and hypotheses of the current study are presented. Hereby two empirical models from privacy research, the Extended Privacy Calculus Model (Dinev and Hart, 2006), and from IT adoption research, the Technology Acceptance Model (Davis, 1989) are combined and tailored to the concept of IOT services. In a next step, the research methodology is described in detail before the results are presented. This deliverable concludes with a discussion of the results and gives an outlook on the final D2.4 report "Social Acceptance and Impact Evaluation", in which the findings of the current report will be used to revise and cross-check both research model and instrument for impact assessment on regulatory bodies by conducting an empirical follow-up study.

Section 2: Research Model and Hypotheses

The research model and hypotheses of the current study are depicted in Figure 1. The theoretical constructs and their relationships are primarily derived from the Extended Privacy Calculus Model (EPCM, Dinev and Hart, 2006). EPCM 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 basic rationale behind EPCM is grounded in two contradicting predictor effects 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 believes 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 (ibid.).

In addition, two theoretical constructs from the Technology Acceptance Model (TAM, Davis, 1989), i.e. *perceived usefulness* and the *intention to use IT*, were adapted and integrated into EPCM. Having its roots in the Information Systems discipline, TAM describes determinants of technology adoption and was published in various variations in the past (Davis and Venkatesh, 1996; Davis and Venkatesh, 2004; Kamis et al., 2008; Kowatsch and Maass, 2010; Maass and Kowatsch, 2008; Moore and Benbasat, 1991; Venkatesh and Davis, 2000; Venkatesh et al., 2003; Wixom and Todd, 2005). TAM is rooted in the social sciences theory of reasoned action (Ajzen and Fishbein, 1980) and its successor, the theory of planned behaviour (Ajzen, 1991).

Both EPCM and TAM have been incorporated in the current research in order to address critical privacy and technology factors that are relevant to social acceptance and impact evaluation of IOT services. The definitions of the seven constructs are adapted from Dinev and Hart (2006, p.64, Table 1) and Davis (1989, p. 320ff) such that they apply to the concept of IOT services. Hereby, IOT services are defined as sensor-based IT services that support people in every-day business and private situations. The five construct definitions as adapted from EPCM are listed in the following:

- **Perceived IOT service privacy risk:** Perceived risk of opportunistic behaviour related to the disclosure of personal information of IOT service users in general.
- **Privacy concerns against IOT service:** Concerns about opportunistic behaviour related to the personal information transferred to the IOT service by the individual respondent in particular.
- **Trust in organization providing the IOT service:** Trust believes reflecting confidence that personal information transferred to the IOT service organization will be handled competently, reliably, and safely.
- **Personal interest in IOT service:** Personal interest or cognitive attraction to IOT service overriding privacy concerns.

- **Willingness to provide personal information for IOT service:** Willingness to provide personal information that is 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:** Expected usefulness of an 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 every day situations.
- **Intention to use IOT service:** The intention to use an IOT service reflects behavioural expectations of individuals that predict their future use of the IOT service.

Two modifications were conducted in order to combine EPCM and TAM for the current study. First, *intention to use* was included as construct that mediates the impact on the willingness to provide personal information for a particular IOT service. 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 (Ajzen, 1991). Second, *expected usefulness* of an IOT service was added as construct that influences the behavioural intention to use that service. The rationale behind this effect is that IOT services are more likely to be adopted when they are perceived useful. This relationship was adopted directly from TAM (Davis, 1989; Wixom and Todd, 2005).

In summary, the following eight hypotheses are proposed based on the discussion of EPCM and TAM above (see also Figure 1):

H1: Perceived IOT service privacy risk has a negative relationship with the intention to use that IOT service.

H2: Perceived IOT service privacy risk has a positive relationship with expected usefulness of that IOT service.

H3: Perceived IOT service privacy risk has a positive relationship with privacy concerns against that IOT service.

H4: Trust in the organization that provides an IOT service has a positive relationship with the intention to use that IOT service.

H5: Perceived IOT service privacy risk has a negative relationship with trust in the organization that provides that IOT service.

H6: Expected usefulness of an IOT service has a positive relationship with the intention to use that IOT service.

H7: Personal interest in an IOT service has a positive relationship with the intention to use that IOT service.

H8: The intention to use an IOT service has a positive relationship with the willingness to provide personal information for that IOT service.

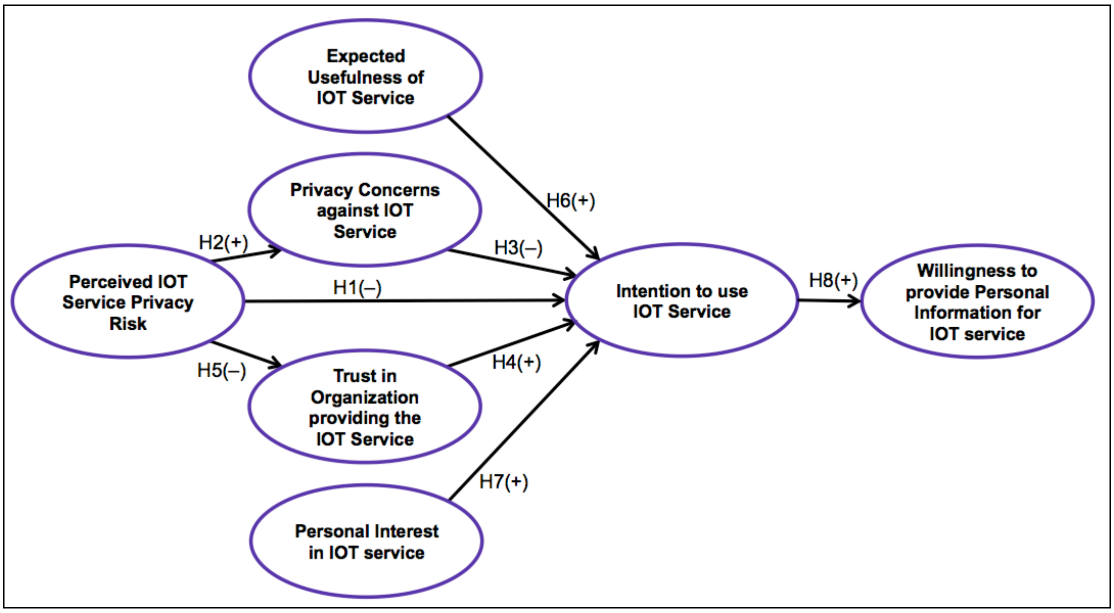

Expected Usefulness of IOT Service
Privacy Concerns against IOT Service
Perceived IOT Service Privacy Risk
Trust in Organization providing the IOT Service
Personal Interest in IOT service
Intention to use IOT Service
Willingness to provide Personal Information for IOT service
H1(–)
H2(+)
H3(–)
H4(+)
H5(–)
H6(+)
H7(+)
H8(+)

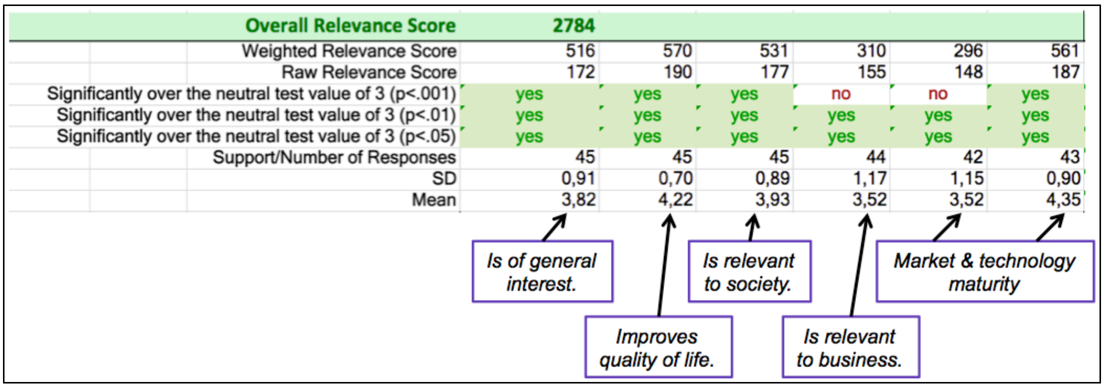
Figure 1. Research model of the current study. Note: this model was adapted from (Dinev and Hart, 2006)

The research model and its hypotheses as depicted in Figure 1 are now used to identify predicting factors that significantly influence the behavioural intention to use particular IOT services directly and the willingness to provide personal information for those services indirectly through behavioural intentions. Corresponding results will inform the design and implementation of future IOT services with regard to privacy aspects such that they are likely to be accepted. A detailed description of the evaluation method is given in the next section of this deliverable.

Section 3: Method

In order to test the research model, a questionnaire-based survey was developed. Four IOT services in every-day situations have been identified from the IOT-I survey that was conducted as part of IOT-I Task 2.1. The rationale behind the evaluation of situational descriptions is based on the methodology SiDIS (formerly known as CoDesA) (Janzen et al., 2010; Maass and Janzen, 2011) in which situational descriptions are one of the first steps towards the design of IT artefacts such as IOT services.

The identification of relevant situations was conducted in several steps whereby an overall relevance score was calculated for each scenario. The calculation was conducted as shown in Figure 2 for an example IOT situation. First, the mean values of the questionnaire items[1] from IOT-I D2.1 (Presser and Krco, 2011) (i.e. general interest, quality of life, relevance to society, relevance to business, market maturity and technology maturity) ranging from strongly disagree (1) to strongly agree (5) were multiplied with the number of responses that indicate relevance in terms of participant's interest in a scenario. This score (e.g., 172 for general interest) was then multiplied by one, two or three in case the mean value lies significantly above the neutral scale value of three (no answer) 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 and the higher the significance level were. Finally, the overall relevance score represents the sum of the six raw relevance scores.



Overall Relevance Score	2784					
Weighted Relevance Score	516	570	531	310	296	561
Raw Relevance Score	172	190	177	155	148	187
Significantly over the neutral test value of 3 (p<.001)	yes	yes	yes	no	no	yes
Significantly over the neutral test value of 3 (p<.01)	yes	yes	yes	yes	yes	yes
Significantly over the neutral test value of 3 (p<.05)	yes	yes	yes	yes	yes	yes
Support/Number of Responses	45	45	45	44	42	43
SD	0,91	0,70	0,89	1,17	1,15	0,90
Mean	3,82	4,22	3,93	3,52	3,52	4,35

Figure 2. Relevance score calculation for the identification of relevant IOT-I services

The resulting list of IOT services were then ranked according to the overall relevance scores and the two best-performing business situations and private situations have been chosen accordingly. The resulting IOT services together with their situational descriptions are presented in Table 1.

[1] The answer "no option" from D2.1 was adopted as the neutral scale value three on the five-point Likert-scale of the current study.

No	IOT-I service	Situation (narrative)	Focus
1	Public Transport Payment	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 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 Service	The Home Central Control (HCC) 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 recognised at the entrance and the electronic key in your pocket is detected. The HCC 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. The HCC recognizes which appliances (washing machine, dishwasher, water heater, heating system, etc.) are turned on at a given time and synchronises them to ensure the best energy efficiency taking into account pricing structure of the utility companies.	Private situation
4	Healthcare Monitoring Service	Recently the doctors have diagnosed that John's 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 neighbourhood. So John retains his private and social life, which is very important for coping with his condition and happiness.	Private situation

Table 1. IOT-I services with situational descriptions and focus (business vs. private)

The questionnaire items of the theoretical constructs have been adapted from prior research. In particular, the following constructs have been adapted from Dinev and Hart (2006): (1) perceived IOT service privacy risk (from perceived Internet privacy risk), (2) privacy concerns against IOT service (from Internet privacy concerns), (3) Trust in organizations providing the IOT service (from Internet trust), (4) personal interest in IOT service (from personal Internet interest), and finally (5) Willingness to Provide Personal Information (from willingness to provide personal information to transact on the Internet).

In addition, questionnaire items from two constructs of technology acceptance research (Davis, 1989; Kamis et al., 2008; Moore and Benbasat, 1991; Venkatesh et al., 2003) have been incorporated into the current study. First, expected usefulness of IOT service has been adapted from the perceived usefulness scale used by Kamis et al. (2008). Second, willingness to use IOT service was adapted from the intention to use construct used by Venkatesh et al. (2003). Overall, the questionnaire items for each theoretical construct together with the scales employed are shown in Table 2.

Furthermore, questionnaire items on data security and legislation have been added as well as items on how a user of a IOT service should be informed about the use of personal information in terms of degree of detail and notification frequency. Those questionnaire items are listed in Table 3.

Finally, variables such as affinity to Information and Communication Technology (ICT), age, gender and country have been incorporated into the questionnaire to account for technological and socio-demographic biases (cf. questionnaire in the Appendix for details and item wording).

No.	Construct and scale item wording
	Perceived IOT service privacy risk ***Likert-scale: from very low risk (1) to very high risk (5)*** What do you believe is the risk due to the possibility that personal information tracked by this IOT service…
PR1	…could be sold to third parties?
PR2	…could be misused?
PR3	…could be made available to unknown individuals or companies without your knowledge?
PR4	…could be made available to governmental agencies?
PR5	…could be jeopardized by hacking activities?
	Privacy concerns against IOT service ***Likert-scale: from not at all concerned (1) to very concerned (5)***
PC1	I am concerned that the information recorded by this IOT service could be misused.
PC2	I am concerned that a person or authority can find private information about me when I use this IOT service.
PC3	I am concerned about information recorded by this IOT service, because of what others might do with it.
PC4	I am concerned about information recorded by this IOT service, because it could be used in a way I did not foresee.
	Trust in organizations providing the IOT service ***Likert-scale: from strongly disagree (1) to strongly agree (5)***
TO1	Organizations provide this IOT service in a safe way such that information can be exchanged with others.
TO2	Organizations provide this IOT service in a reliable way such that business transactions can be conducted.
TO3	Organizations that provide this IOT service handle personal information in a competent fashion.
	Expected usefulness of IOT service ***Likert-scale: from strongly disagree (1) to strongly agree (5)***
EU1	I expect that using this IOT service can improve my performance.
EU2	I expect that using this IOT service can improve my productivity.

EU3	I expect that using this IOT service can improve my effectiveness.
EU4	I expect that using this IOT service would be useful.
	Personal interest in IOT service ***Likert-scale: from strongly disagree (1) to strongly agree (5)***
PI1	I find that my personal interest in this IOT service overrides my concerns of possible risk or vulnerability that I may have regarding my privacy.
PI2	The greater my interest in this IOT service, the more I tend to suppress my privacy concerns.
PI3	In general, my need to use this IOT service is greater than my concern about privacy.
	Intention to use IOT service ***Likert-scale: from strongly disagree (1) to strongly agree (5)***
IU1	I intend to use this IOT service.
IU2	I would use this IOT service.
IU3	I could imagine using this IOT service.
	Willingness to Provide Personal Information ***Likert-scale: from strongly disagree (1) to strongly agree (5)***
WPI1	I would provide accurate and identifiable personal information for using this IOT service.
WPI2	I would provide personal financial information such as credit card information for using this IOT service.

Table 2. Questionnaire items. Note: For Healthcare Monitoring Service (IOT Service 4) a slightly different wording was used (cf. Appendix)

No.	**Item wording**
	Data security and legislation (multiple answers were allowed) ***How do you expect your personal information to be best protected?***
DSL1	By the introduction of international law, which is probably more practical, but may take longer in developing.
DSL2	By the introduction of soft law, i.e. regulations are established by private organizations.
DSL3	By technical means such as encrypted communication channels and data stores.
DSL4	Others: [free text feedback]
	Qualitative notification on personal information use (multiple answers were allowed) ***How would you like to be informed that your personal information will be used?***
QN1	General indication without any details of potential use of personal information.
QN2	Specific and detailed indication including potential use of personal information.
QN3	Others: [free text feedback]
	Frequency of notification on personal information use (only one answer was allowed) ***How often would you like to be informed that your personal information will be used?***
FN1	Every time when personal information is used.
FN2	Only the first time personal information is used.
FN3	Others: [free text feedback]

Table 3. Additional questionnaire items on data security, legislation and notification of personal information use

Section 4: Results

Overall, 26 male and 5 female subjects participated in the questionnaire-based survey that was conducted during the IOT-I week in Barcelona in June 2011 (cf. Figure 3). The distribution of the subjects' age is depicted in Figure 4. The subjects can be characterized as technically-savvy as they were either part of the IOT-I project or other IOT-related projects such as IoT-A, CASAGRAS2, SMART SANTANDER or the European Research Cluster on Internet of Things (IERC). Consistently, the mean value of the ICT affinity construct (two item-scale, Cronbach's Alpha = .897) is 4.29 and lies significantly above the neutral scale value of 3 (neither) by applying a one-sample t-test. The boxplot for the aggregated ICT construct is given in Figure 5, too.

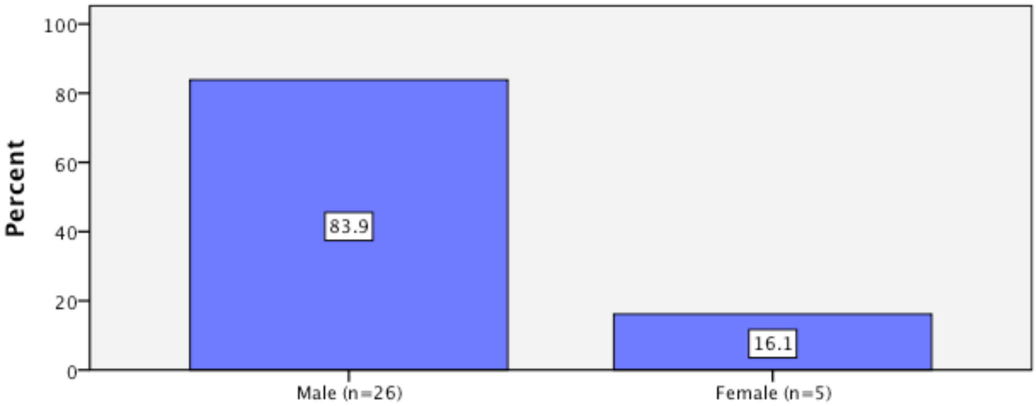


Figure 3. Distribution of male and female subjects (n=31)

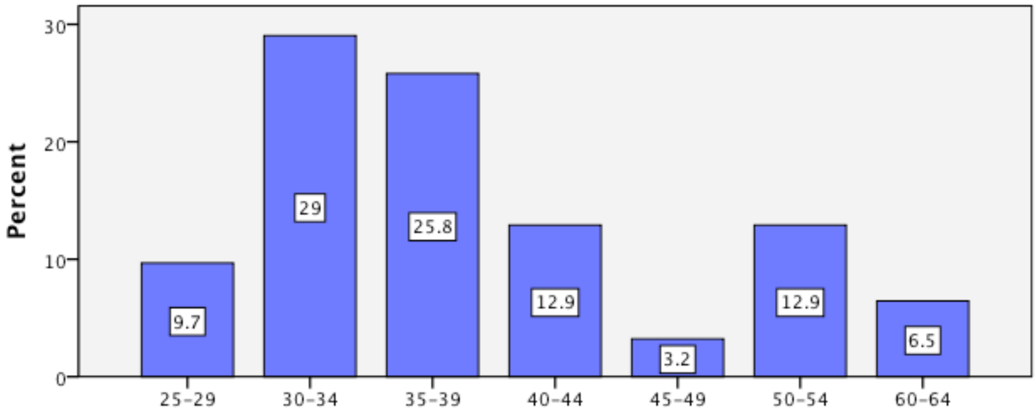


Figure 4. Distribution of subjects' age (n=31)

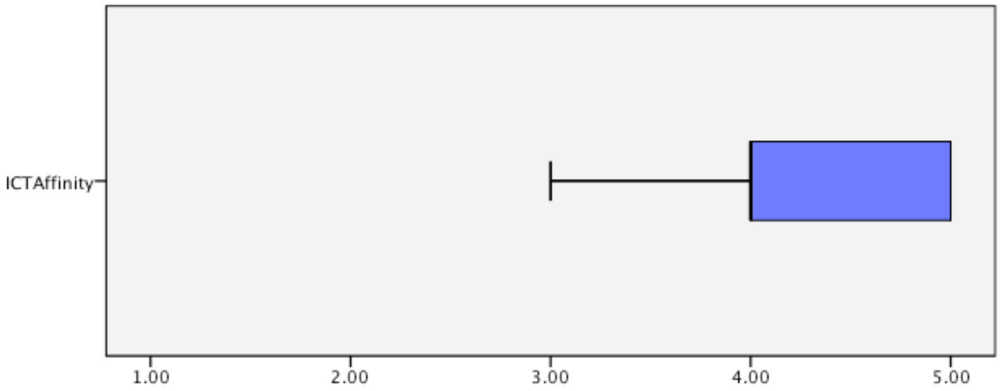


Figure 5. Boxplot of the ICT affinity construct (n=31)

The descriptive statistics of the questionnaire items and their underlying theoretical constructs perceived IOT service privacy risk, privacy concerns against IOT service, trust in organization providing the IOT service, personal interest in IOT service, expected usefulness of IOT service, willingness to use IOT service and willingness to provide personal information for IOT service are listed in Table 4. With one exception, i.e. the two-item scale WPI1 and WPI2, Cronbach' Alpha values for all other questionnaire items lie over the recommended threshold of .70 (Nunnally, 1967). Accordingly, aggregated variables for each scale have been calculated that represent the mean value of the single items per theoretical construct. Additionally, one-sample t-tests have been calculated for each aggregated variable to see whether the mean value lies significantly above or below the neutral scale value of three. That is, the one-sample t-tests show whether the subjects have rated the constructs rather positively, neutral or negatively.

Furthermore, descriptive statistics related to the questionnaire items on data security, legislation and notification of personal information use are presented in Figure 6. In addition to these pre-defined items (cf. items DSL1-3 in Table 3), it was reported 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.

In addition, results on the preferred level of detail of notifications on personal information use are depicted in Figure 7, whereas feedback regarding the frequency of notifications is shown in Figure 8. One subject reported hereby that details on personal information use should only be made available to the user on request. By contrast, another participant of the survey 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 participant added the option that users should also be informed when the way of personal information use is being changed.

Finally, Pearson correlation coefficients with two-tailed tests of significance have been calculated to test the hypotheses as depicted in the research model in Figure 1. The resulting coefficients that are shown in Table 5 indicate that five hypotheses are fully supported by the survey data for all evaluated

IOT services (H2 and H4-7) whereas three hypotheses are partly supported (H1, H3 and H8). With the lens on the evaluated IOT situations, the conclusion can be drawn that all hypotheses are supported for the public transport payment service and the navigation service, i.e. the two business situations.

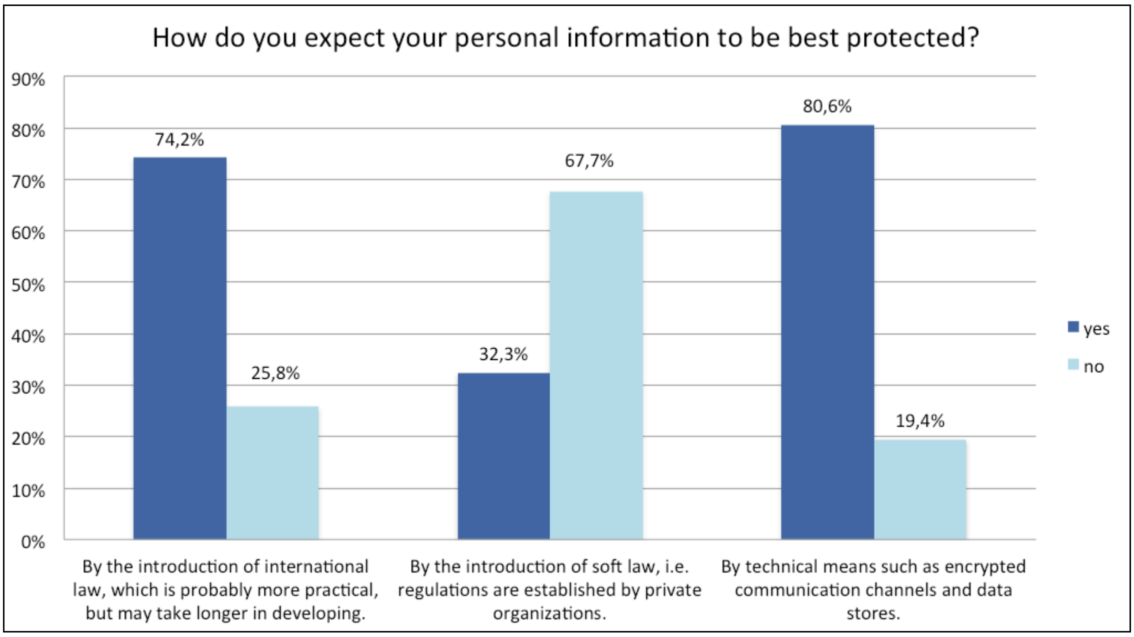


Figure 6. Descriptive statistics of the questionnaire items on data security, legislation and notification of personal information use (n=31)

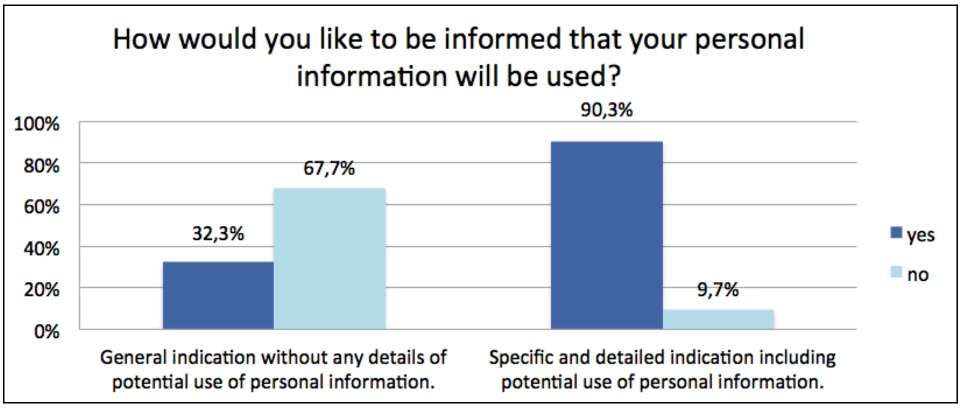


Figure 7. Preferred level of detail of notifications on personal information use (n=31)

Item	Public Transport Payment Service	Navigation Service	Smart Home Service	Healthcare Monitoring Service
Perceived IOT service privacy risk				
PR1	3.10 (1.25)	3.32 (1.01)	2.90 (1.11)	2.58 (1.06)
PR2	3.06 (1.15)	3.29 (0.94)	3.10 (1.17)	2.97 (1.11)
PR3	3.39 (1.15)	3.52 (1.06)	3.10 (1.04)	2.94 (1.15)
PR4	3.61 (1.09)	3.39 (1.09)	3.06 (1.09)	3.00 (1.16)
PR5	3.45 (1.09)	3.45 (1.10)	3.55 (1.09)	3.00 (1.07)
Alpha	.866	.909	.915	.906
PR	**3.32$^{n.s.}$ (0.92)**	**3.39* (0.89)**	**3.15$^{n.s.}$ (0.95)**	**2.90$^{n.s.}$ (0.94)**
Privacy concerns against IOT service				
PC1	3.29 (1.19)	3.32 (0.95)	3.23 (1.12)	2.94 (1.18)
PC2	3.39 (1.15)	3.26 (1.06)	3.26 (1.06)	3.10 (1.08)
PC3	3.29 (1.04)	3.45 (1.00)	3.32 (1.01)	3.06 (1.00)
PC4	3.39 (1.20)	3.48 (1.06)	3.58 (1.03)	3.23 (1.02)
Alpha	.899	0.96	.931	.907
PC	**3.33$^{n.s.}$ (1.00)**	**3.38* (0.96)**	**3.35$^{n.s.}$ (0.96)**	**3.08$^{n.s.}$ (0.95)**
Trust in organizations providing the IOT service				
TO1	3.23 (0.88)	2.90 (0.75)	3.16 (0.93)	3.48
TO2	3.94 (0.68)	3.26 (0.89)	3.45 (0.96)	3.74
TO3	3.52 (0.89)	3.00 (0.86)	3.19 (0.91)	3.77
Alpha	.778	.839	.906	.738
TO	**3.56*** (0.69)**	**3.05$^{n.s.}$ (0.73)**	**3.27$^{n.s.}$ (0.86)**	**3.67*** (0.71)**
Expected usefulness of IOT service				
EU1	4.00 (0.93)	3.87 (0.72)	3.55 (0.81)	4.32 (0.54)
EU2	3.71 (1.10)	3.87 (0.81)	3.45 (0.89)	4.19 (0.65)
EU3	3.81 (1.05)	3.87 (0.81)	3.58 (0.89)	4.16 (0.69)
EU4	4.16 (0.82)	3.94 (0.73)	3.87 (0.76)	4.45 (0.62)
Alpha	.940	0.961	.934	.892
EU	**3.92*** (0.90)**	**3.89*** (0.72)**	**3.61*** (0.77)**	**4.28*** (0.55)**
Personal interest in IOT service				
PI1	3.26 (1.21)	3.39 (0.92)	3.35	4.06 (0.68)
PI2	3.65 (1.02)	3.55 (0.89)	3.29	4.13 (0.56)
PI3	3.16 (1.13)	3.13 (1.00)	3.10	4.06 (0.68)
Alpha	.889	.922	.942	.850
PI	**3.35 (1.01)**	**3.35* (0.87)**	**3.25 (0.96)**	**4.09*** (0.56)**
Intention to use IOT service				
IU1	3.55 (1.06)	3.48 (0.96)	3.39	4.00
IU2	3.65 (1.05)	3.77 (0.96)	3.55	4.06
IU3	4.03 (0.88)	3.84 (1.04)	3.84	4.16
Alpha	.897	.922	.909	.926
IU	**3.74*** (0.91)**	**3.70*** (0.92)**	**3.59*** (0.76)**	**4.08*** (0.61)**
Willingness to Provide Personal Information				
WPI1	3.10 (1.14)	3.06 (1.24)	2.97 (1.14)	3.97*** (0.61)
WPI2	2.97 (1.28)	2.55 (1.23)	2.81 (1.08)	3.26 (1.15)
Alpha	.860	.806	.721	.444
WPI	**3.03$^{n.s.}$ (1.13)**	**2.80$^{n.s.}$ (1.13)**	**2.89$^{n.s.}$ (0.98)**	**n/a**

Table 4. Descriptive statistics of the theoretical constructs' items. Note: Mean (Standard deviation), n=31, * = p < .05 / ** = p < .01 / *** = p < .001, n.s. = not significant where the p-values are derived from one-sample t-test with a test value of 3.

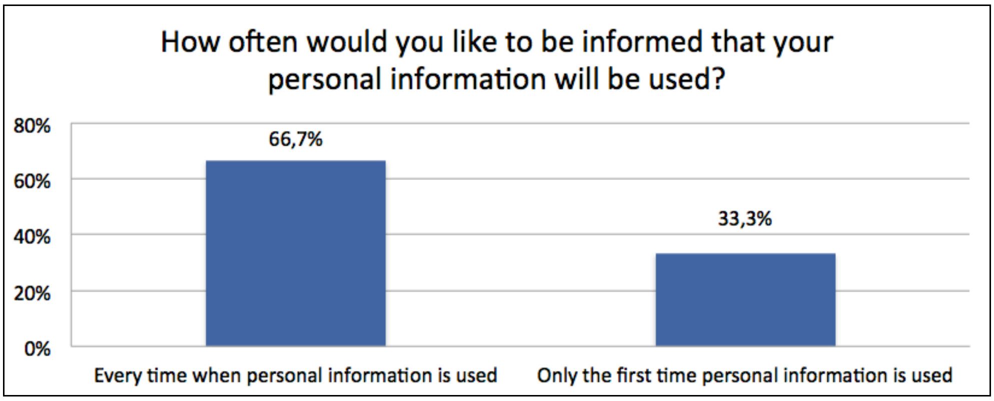


Figure 8. Preferred frequency of notification regarding personal information use (n=31)

Hypothesis	Public Transport Payment Service	Navigation Service	Smart Home Service	Healthcare Monitoring Service	Result
H1: PR * IU	–.558**	–.556**	–.274$^{n.s.}$	–.304$^{n.s.}$	Partly accepted
H2: PR * PC	.816***	.871***	.809***	.853***	Accepted
H3: PC * IU	–.516**	–.464**	–.085$^{n.s.}$	–.359*	Partly accepted
H4: TO * IU	.394*	.526**	.390*	.387*	Accepted
H5: PR * TO	–.536**	–.385*	–.517**	–.374*	Accepted
H6: EU * IU	.745***	.763***	.665***	.553**	Accepted
H7: PI * IU	.644***	.725***	.582***	.749***	Accepted
H8: IU * WPI	.715***	.677***	.660***	.673*** (WPI1) .305$^{n.s.}$ (WPI2)	Partly accepted

Table 5. Pearson correlation coefficients for the eight hypotheses. Note: n=31, * = p < .05 / ** = p < .01 / *** = p < .001, n.s. = not significant

Section 5: Discussion

Overall, the results of the IOT survey on critical privacy factors show that the 31 subjects' data and analyses support the proposed research model and corresponding hypotheses, as depicted in Figure 1. A detailed discussion of the results is presented in the following.

First, it can be stated that all four IOT situations that have been selected for evaluation from the IOT survey (cf. D2.1) are perceived as relevant by the subjects. That is, the constructs expected usefulness of the IOT services and willingness to use those IOT services lie all significantly above the neutral test value of three (cf. Table 4, EU row and IU row).

Second, even tough 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 4, WPI row). Therefore, subjects are uncertain in terms of providing access to their personal information. It could only be shown for item WPI1 of the Healthcare 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. the fictive person John who suffers from Alzheimer disease and is not able to decide for himself as described in the corresponding situation (cf. Table 1).

Third, the current study has adapted the extended privacy calculus model (Dinev and Hart, 2006) 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 (TAM, Davis, 1989). The proposed model was tested successfully for the two business situations because the data of the public transport payment service and a navigation service support all eight hypotheses. In particular, it could be shown that all contradicting predictors, i.e. perceived IOT service privacy risk and privacy concerns against an IOT service on the one hand and trust in 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 and positive impact on the behavioural intention to use that IOT service directly and on the willingness to provide personal information for the IOT service indirectly.

However, perceived privacy risks are not significant predictors of intention to use IOT services for smart home and healthcare monitoring situations. Additionally, privacy concerns are not significant predictors of intention to use the IOT service in the smart home situation. This can be explained by the fact that subjects may perceive theses risks to a lower extent because the service is employed primarily in a private environment compared to IOT services that are available in the public space and focus on business trips.

By contrast, only perceived risks do not significantly influence the intention to use the healthcare monitoring service even though both constructs, i.e. perceived risks and privacy concerns, are risk believes (cf. Dinev and Hart, 2006, p. 64 Table 1). One reason of this discrepancy may lie in the fact that particular concerns about opportunistic behaviour related to personal information use of the IOT service provider may override perceived privacy risks in general. Another reason may be that subjects have evaluated privacy risks for another person (John) as discussed above and that general risks are not as perceived as strong for another person than for oneself. This may also be the reason for the low Cronbach's Alpha reliability coefficient for the items (cf. Table 4, WPI1 and WPI2) and the resulting discrepancy of both significant and non-significant IU * WPI correlations (cf. Table 5). This identity problem, i.e. evaluating for a third person, should be addressed in future studies by a description of the IOT situation from a first-person perspective as it was done for the other three situations. But then, less severe though realistic diseases related to an IOT healthcare monitoring situation should be designed to retain the level of validity and, at the same time, to show respect for the ethical values of subjects that participate in the survey.

Moreover, results on legislation, data protection (Figure 6) and notification of personal information use (Figure 7 and Figure 8) provide clear guidelines for design and implementation of IOT services. Accordingly, subjects expect that their personal information should 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 also be protected by technical means (cf. Figure 6). Thus, state of the art encryption and security standards should be incorporated and advertised 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 the user is able to request this information on demand (cf. Figure 7).

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 the user 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 accordingly (cf. Figure 8).

The current study has several limitations. First, with regard to the over-average ICT affinity of the subjects (cf. Figure 5), results are biased in the sense that primarily male and technology-savvy persons have participated in the survey. Even though these persons may adopt innovative IOT services first, support from a more equally distributed sample would increase external validity of the findings. Second, the sample size is too low to identify small effects when testing the hypotheses with Pearson correlation coefficients and thus, some of the correlations might not render significant even though the coefficients differ from zero (cf. Table 5). Third, the limited sample size restricts also the application of covariance-based hypotheses testing methods with structural equation modelling tools such as AMOS or LISREL. Furthermore, external validity of the results is restricted with regard to the textual descriptions of the IOT situations compared to, for example, drawings, video clips, lab or real-life field experiments that would all increase subjects' understanding of the IOT services and thus the quality of evaluations. Nonetheless, the current results based on domain experts are a valid starting point into the investigation of IOT-based services.

An overview of the core findings of the current study is given in Table 6.

#	Finding
1	An empirical instrument that addresses privacy concerns, technology acceptance and legislation aspects has been proposed for the class of IOT applications.
2	The empirical instrument was tested with two business and two private IOT situations that were derived and adapted from D2.1 (Presser and Krco, 2011): • Public Transport Payment Service (Business) • Navigation Service (Business) • Smart Home Service (Private) • Healthcare Monitoring Service (Private)
3	The empirical instrument was tested successfully for the two business situations and can be pragmatically used to identify critical privacy factors relevant to the design and implementation of future IOT services as described in this deliverable.
4	There seems to be a trade-off between privacy concerns and perceived risks on the one hand and expected usefulness and personal interests on the other hand. Both factors influence the behavioural intention to use a particular IOT service and the willingness to provide personal information. However, in case of private situations, expected usefulness and personal interest may rather override privacy concerns and risks than in business situations.
5	International law and technical barriers should be of a primary concern to IOT-related stakeholders to protect personal information.
6	Potential early adopters of IOT services would like to be informed in detail about the use of their personal information.
7	The majority of the participants of the current study would like to be informed every time when personal information is being used by a particular IOT service.
8	The major limitation of the current work is the lack of external validity. Thus, the findings of the current study require a validation based on a more equally distributed and non-technical sample.

Table 6. Overview of the current study's core findings

Section 6: Conclusion and Outlook

In this initial report on social acceptance and impact of future IOT services, the extended privacy calculus model from Dinev and Hart (2006) has been combined with the Technology Acceptance Model (Davis, 1989) and was tested successfully in the IOT domain by conducting a questionnaire-based survey. As a result, critical factors have been identified that influence the adoption of IOT services and thus, are critical in the design process and implementation of those services. Furthermore, several practical implications have been discussed with regard to data security, legislation and notification of personal information use, all relevant for the development of IOT services such that they are probably accepted by society.

Future work will extend the preliminary results of this report by conducting further studies in order to cross-check the current findings and thus, to increase the validity and quality of implications. Those results will then be available and published in the final IOT deliverable D2.4 on social acceptance and impact evaluation due in August 2012.

Section 7: References

Ajzen, I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes, 50 (2), 179-211.

Ajzen, I. and Fishbein, M. (1980). Understanding Attitudes and Predicting Social Behaviour Prentice Hall, Inglewood Cliffs, NJ.

Anderson, R. and Moore, T. (2009). Information security: where computer science, economics and psychology meet. Philosophical Transactions of the Royal Society A - Mathematical, Physical & Engineering Sciences, 367, 2717-2727.

Angst, C.M. and Agarwal, R. (2009). Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion. MIS Quarterly, 33 (2), 339-370.

Davis, F.D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. MIS Quarterly, 13 (3), 319-339.

Davis, F.D. and Venkatesh, V. (1996). A critical assessment of potential measurement biases in the technology acceptance model: Three experiments. International Journal of Human-Computer Studies, 45 (1), 19-45.

Davis, F.D. and Venkatesh, V. (2004). Toward preprototype user acceptance testing of new information systems: Implications for software project management. IEEE Transactions on Engineering Management, 51 (1), 31-46.

Dinev, T. and Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions. Information Systems Research, 17 (1), 61-80.

Janzen, S., Kowatsch, T. and Maass, W. "A Methodology for Content-Centered Design of Ambient Environments," in: *Global Perspectives on Design Science Research, 5th International Conference, DESRIST 2010, St. Gallen, Switzerland, June 4-5, 2010 Proceedings,* R. Winter, J.L. Zhao and S. Aier (eds.), Springer, Berlin, Germany, 2010, pp. 210-225.

Kamis, A., Koufaris, M. and Stern, T. (2008). Using an Attribute-Based Decision Support System for User-Customized Products Online: An Experimental Investigation. MIS Quarterly, 32 (1), 159-177.

Kosta, E. and Dumortier, J. (2008). Searching the man behind the tag: privacy implications of RFID technology. International Journal of Intellectual Property Management, 2 (3), 276-288.

Kowatsch, T. and Maass, W. (2010). In-store Consumer Behavior: How Mobile Recommendation Agents Influence Usage Intentions, Product Purchases, and Store Preferences. Computers in Human Behavior, 26 (4), 697-704.

Little, L. (2008). Privacy, trust, and identity issues for ubiquitous computing. Social Science Computer Review, 26 (1), 3-5.

Maass, W. and Janzen, S. "Pattern-Based Approach for Designing with Diagrammatic and Propositional Conceptual Models," in: *Service-oriented Perspectives in Design Science Research, 6th International Conference, DESRIST 2011, Milwaukee, WI, USA, May 5-6, 2011,* H.

Jain, A.P. Sinha and P. Vitharana (eds.), Springer, Heidelberg, Germany, 2011, pp. 192-206.

Maass, W. and Kowatsch, T. (2008). Adoption of Dynamic Product Information: An Empirical Investigation of Supporting Purchase Decisions on Product Bundles. In Proceedings of the 16th European Conference on Information Systems (ECIS), Galway, Ireland

Malhotra, N.K., Kim, S.S. and Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. Information Systems Research, 15 (4), 336-355.

Moore, G.C. and Benbasat, I. (1991). Development of an instrument to measure the perceptions of adopting an information technology innovation. Information Systems Research, 2 (3), 192-222.

Nunnally, J.C. (1967). Psychometric Theory McGraw-Hill, New York.

Pramatari, K. and Theotokis, A. (2009). Consumer acceptance of RFID-enabled services: a model of multiple attitudes, perceived system characteristics and individual traits. European Journal of Information Systems, 18, 541-552.

Presser, M. and Krco, S. (2011). The Internet of Things Initiative (IOT-I) Deliverable 2.1: Initial report on IoT applications of strategic interest, FP7 ICT project, contract number: 257565

Spiekermann, S. (2009). RFID and privacy: what consumers really want and fear. Personal Ubiquitous Computing, 13, 423-434.

Venkatesh, V. and Davis, F.D. (2000). A theoretical extension of the Technology Acceptance Model: Four longitudinal field studies. Management Science, 46 (2), 186-204.

Venkatesh, V., Morris, M.G., Davis, G.B. and Davis, F.D. (2003). User acceptance of information technology: Toward a unified view. MIS Quarterly, 27 (3), 425-478.

Weber, R. (2010). Internet of Things - New security and privacy challenges. Computer Law & Security Review, 26, 23-30.

Wixom, B.H. and Todd, P.A. (2005). A Theoretical Integration of User Satisfaction and Technology Acceptance. Information Systems Research, 16 (1), 85-102.

Section 8: Appendix – Survey Instrument

Survey on Critical Privacy Factors of Internet of Things Services

Instructions

The information collected by this survey is used for the purpose of investigating critical privacy factors of IOT services for the IOT-i project (www.iot-i.eu). The survey follows a simple pattern of presenting you four IOT services by a brief situational description and several statements for each IOT service. It will take you approx. 20 minutes to complete this survey.

Your feedback is highly relevant for the design and implementation of future IOT services. You will be able to see the results of this survey on the project website after the evaluation is completed.

Enjoy the survey now!

Disclaimer and Privacy Statement

The IOT situations have been selected and adapted from several EU projects, including SmartSantander, SENSEI, e-SENSE, EXALTED, FLORENCE, PROSENSE, LOLA and MIMOSA. Your answers will be treated anonymously, but we retain information about your age, gender and country of residence to analyse the results of the questionnaire and remove any bias. We will strictly follow the EU directive 95/46/EC ("Protection of personal data") and national guidelines.

1st IOT Situation: Public Transport Payment 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.

1. What do you believe is the risk due to the possibility that personal information tracked by this IOT service…

a) … could be sold to third parties?

○	○	○	○	○
very low risk	low risk	neither	high risk	very high risk

b) … could be misused?

○	○	○	○	○
very low risk	low risk	neither	high risk	very high risk

c) … could be made available to unknown individuals or companies without your knowledge?

○	○	○	○	○
very low risk	low risk	neither	high risk	very high risk

d) … could be made available to governmental agencies?

○	○	○	○	○
very low risk	low risk	neither	high risk	very high risk

e) … could be jeopardized by hacking activities?

○	○	○	○	○
very low risk	low risk	neither	high risk	very high risk

2. Privacy Concerns

a) I am concerned that the information recorded by this IOT service could be misused.

○	○	○	○	○
not at all concerned	not concerned	neither	concerned	very concerned

b) I am concerned that a person or authority can find private information about me when I use this IOT service.

○	○	○	○	○
not at all concerned	not concerned	neither	concerned	very concerned

c) I am concerned about information recorded by this IOT service, because of what others might do with it.

○	○	○	○	○
not at all concerned	not concerned	neither	concerned	very concerned

d) I am concerned about information recorded by this IOT service, because it could be used in a way I did not foresee.

○	○	○	○	○
not at all concerned	not concerned	neither	concerned	very concerned

3. Trust in Organizations

a) Organizations provide this IOT service in a safe way such that information can be exchanged with others.

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

b) Organizations provide this IOT service in a reliable way such that business transactions can be conducted.

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

c) Organizations that provide this IOT service handle personal information in a competent fashion.

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

4. Usefulness

a) I expect that using this IOT service can improve my performance.

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

b) I expect that using this IOT service can improve my productivity.

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

c) I expect that using this IOT service can improve my effectiveness.

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

d) I expect that using this IOT service would be useful.

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

5. Personal Interest

a) I find that my personal interest in this IOT service overrides my concerns of possible risk or vulnerability that I may have regarding my privacy.

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

b) The greater my interest in this IOT service, the more I tend to suppress my privacy concerns.

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

c) In general, my need to use this IOT service is greater than my concern about privacy.

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

6. Intention to Use

a) **I intend to use this IOT service.**

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

b) **I would use this IOT service.**

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

c) **I could imagine using this IOT service.**

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

7. Willingness to Provide Personal Information

a) **I would provide accurate and identifiable personal information for using this IOT service.**

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

b) **I would provide personal financial information such as credit card information for using this IOT service.**

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

2nd IOT Situation: Healthcare Monitoring Service

Recently the doctors have diagnosed that John’s 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 neighbourhood. So John retains his private and social life, which is very important for coping with his condition and happiness.

Note: Please rate the following statements as if you were solely responsible for John.

1. What do you believe is the risk due to the possibility that personal information tracked by this IOT service…

a) … could be sold to third parties?

○	○	○	○	○
very low risk	low risk	neither	high risk	very high risk

b) … could be misused?

○	○	○	○	○
very low risk	low risk	neither	high risk	very high risk

c) … could be made available to unknown individuals or companies without your knowledge?

○	○	○	○	○
very low risk	low risk	neither	high risk	very high risk

d) … could be made available to governmental agencies?

○	○	○	○	○
very low risk	low risk	neither	high risk	very high risk

e) … could be jeopardized by hacking activities?

○	○	○	○	○
very low risk	low risk	neither	high risk	very high risk

2. Privacy Concerns

a) I am concerned that the information recorded by this IOT service could be misused.

○	○	○	○	○
not at all concerned	not concerned	neither	concerned	very concerned

b) I am concerned that a person or authority can find private information about John while using this IOT service.

○	○	○	○	○
not at all concerned	not concerned	neither	concerned	very concerned

c) I am concerned about information recorded by this IOT service, because of what others might do with it.

○	○	○	○	○
not at all concerned	not concerned	neither	concerned	very concerned

d) I am concerned about information recorded by this IOT service, because it could be used in a way I did not foresee.

○	○	○	○	○
not at all concerned	not concerned	neither	concerned	very concerned

3. Trust in Organizations

a) Organizations provide this IOT service in a safe way such that information can be exchanged with others.

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

b) Organizations provide this IOT service in a reliable way such that business transactions can be conducted.

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

c) Organizations that provide this IOT service handle personal information in a competent fashion.

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

4. Usefulness

a) I expect that using this IOT service can improve John’s individual performance.

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

b) I expect that using this IOT service can improve John’s individual productivity.

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

c) I expect that using this IOT service can improve John’s individual effectiveness.

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

d) I expect that using this IOT service would be useful for John.

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

5. Personal Interest

a) Being responsible for John, I would find that John’s interest in this IOT service overrides his concerns of possible risk or vulnerability that he may have regarding his privacy.

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

b) The greater John’s interest in this IOT service would be, the more he would suppress his privacy concerns.

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

c) In general, I think that John’s individual need to use this IOT service is greater than his concerns about privacy.

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

6. Intention to Use

a) **Being responsible for John, I think that he would intend to use this IOT service.**

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

b) **Being responsible for John, I think that he would use this IOT service.**

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

c) **Being responsible for John, I think that he could imagine using this IOT service.**

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

7. Willingness to Provide Personal Information

a) **Being responsible for John, I think that he would provide accurate and identifiable personal information for using this IOT service.**

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

b) **Being responsible for John, I think that he would provide personal financial information such as credit card information for using this IOT service.**

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

3rd IOT Situation: Navigation 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.

1. What do you believe is the risk due to the possibility that personal information tracked by this IOT service…

a) … could be sold to third parties?

○	○	○	○	○
very low risk	low risk	neither	high risk	very high risk

b) … could be misused?

○	○	○	○	○
very low risk	low risk	neither	high risk	very high risk

c) … could be made available to unknown individuals or companies without your knowledge?

○	○	○	○	○
very low risk	low risk	neither	high risk	very high risk

d) … could be made available to governmental agencies?

○	○	○	○	○
very low risk	low risk	neither	high risk	very high risk

e) … could be jeopardized by hacking activities?

○	○	○	○	○
very low risk	low risk	neither	high risk	very high risk

2. Privacy Concerns

a) **I am concerned that the information recorded by this IOT service could be misused.**

○	○	○	○	○
not at all concerned	not concerned	neither	concerned	very concerned

b) **I am concerned that a person or authority can find private information about me when I use this IOT service.**

○	○	○	○	○
not at all concerned	not concerned	neither	concerned	very concerned

c) **I am concerned about information recorded by this IOT service, because of what others might do with it.**

○	○	○	○	○
not at all concerned	not concerned	neither	concerned	very concerned

d) **I am concerned about information recorded by this IOT service, because it could be used in a way I did not foresee.**

○	○	○	○	○
not at all concerned	not concerned	neither	concerned	very concerned

3. Trust in Organizations

a) **Organizations provide this IOT service in a safe way such that information can be exchanged with others.**

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

b) **Organizations provide this IOT service in a reliable way such that business transactions can be conducted.**

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

c) **Organizations that provide this IOT service handle personal information in a competent fashion.**

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

4. Usefulness

a) **I expect that using this IOT service can improve my performance.**

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

b) **I expect that using this IOT service can improve my productivity.**

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

c) **I expect that using this IOT service can improve my effectiveness.**

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

d) **I expect that using this IOT service would be useful.**

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

5. Personal Interest

a) **I find that my personal interest in this IOT service overrides my concerns of possible risk or vulnerability that I may have regarding my privacy.**

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

b) **The greater my interest in this IOT service, the more I tend to suppress my privacy concerns.**

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

c) **In general, my need to use this IOT service is greater than my concern about privacy.**

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

6. Intention to Use

a) I intend to use this IOT service.

○ strongly disagree ○ disagree ○ neither ○ agree ○ strongly agree

b) I would use this IOT service.

○ strongly disagree ○ disagree ○ neither ○ agree ○ strongly agree

c) I could imagine using this IOT service.

○ strongly disagree ○ disagree ○ neither ○ agree ○ strongly agree

7. Willingness to Provide Personal Information:

a) I would provide accurate and identifiable personal information for using this IOT service.

○ strongly disagree ○ disagree ○ neither ○ agree ○ strongly agree

b) I would provide personal financial information such as credit card information for using this IOT service.

○ strongly disagree ○ disagree ○ neither ○ agree ○ strongly agree

4th IOT Situation: Smart Home Service

The Home Central Control (HCC) 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 recognised at the entrance and the electronic key in your pocket is detected. The HCC 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. The HCC recognizes which appliances (washing machine, dishwasher, water heater, heating system, etc.) are turned on at a given time and synchronises them to ensure the best energy efficiency taking into account pricing structure of the utility companies.

1. **What do you believe is the risk due to the possibility that personal information tracked by this IOT service…**

a) … could be sold to third parties?

○	○	○	○	○
very low risk	low risk	neither	high risk	very high risk

b) … could be misused?

○	○	○	○	○
very low risk	low risk	neither	high risk	very high risk

c) … could be made available to unknown individuals or companies without your knowledge?

○	○	○	○	○
very low risk	low risk	neither	high risk	very high risk

d) … could be made available to governmental agencies?

○	○	○	○	○
very low risk	low risk	neither	high risk	very high risk

e) … could be jeopardized by hacking activities?

○	○	○	○	○
very low risk	low risk	neither	high risk	very high risk

2. Privacy Concerns

a) **I am concerned that the information recorded by this IOT service could be misused.**

○	○	○	○	○
not at all concerned	not concerned	neither	concerned	very concerned

b) **I am concerned that a person or authority can find private information about me when I use this IOT service.**

○	○	○	○	○
not at all concerned	not concerned	neither	concerned	very concerned

c) **I am concerned about information recorded by this IOT service, because of what others might do with it.**

○	○	○	○	○
not at all concerned	not concerned	neither	concerned	very concerned

d) **I am concerned about information recorded by this IOT service, because it could be used in a way I did not foresee.**

○	○	○	○	○
not at all concerned	not concerned	neither	concerned	very concerned

3. Trust in Organizations

a) **Organizations provide this IOT service in a safe way such that information can be exchanged with others.**

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

b) **Organizations provide this IOT service in a reliable way such that business transactions can be conducted.**

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

c) **Organizations that provide this IOT service handle personal information in a competent fashion.**

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

4. Usefulness

a) I expect that using this IOT service can improve my performance.

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

b) I expect that using this IOT service can improve my productivity.

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

c) I expect that using this IOT service can improve my effectiveness.

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

d) I expect that using this IOT service would be useful.

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

5. Personal Interest

a) I find that my personal interest in this IOT service overrides my concerns of possible risk or vulnerability that I may have regarding my privacy.

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

b) The greater my interest in this IOT service, the more I tend to suppress my privacy concerns.

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

c) In general, my need to use this IOT service is greater than my concern about privacy.

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

6. Intention to Use

a) I intend to use this IOT service.

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

b) I would use this IOT service.

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

c) I could imagine using this IOT service.

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

7. Willingness to Provide Personal Information

a) I would provide accurate and identifiable personal information for using this IOT service.

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

b) I would provide personal financial information such as credit card information for using this IOT service.

○	○	○	○	○
strongly disagree	disagree	neither	agree	strongly agree

Final Evaluation and Questions

1. How do you expect your personal information to be best protected?
(Multiple answers are allowed)

□ By the introduction of international law, which is probably more practical, but may take longer in developing.

□ By the introduction of soft law, i.e. regulations are established by private organizations.

□ By technical means such as encrypted communication channels and data stores.

□ Others: ____

2. How would you like to be informed that your personal information will be used?
(Multiple answers are allowed)

□ General indication without any details of potential use of personal information.

□ Specific and detailed indication including potential use of personal information.

□ Others: ____

3. How often would you like to be informed that your personal information will be used?

○ Every time when personal information is used.

○ The first time personal information is used.

○ Others: ____

4. I am open-minded towards new technologies.

○ strongly disagree ○ disagree ○ neither ○ agree ○ strongly agree

5. Using new technologies is easy for me.

○ strongly disagree ○ disagree ○ neither ○ agree ○ strongly agree

6. Your gender?

○ female ○ male ○ no answer

7. Your age?

○ below 20 ○ 20 – 24 ○ 25 – 29

○ 30 – 34 ○ 35 – 39 ○ 40 – 44

○ 45 – 49 ○ 50 – 54 ○ 55 – 59

○ 60 – 64 ○ above 64 ○ no answer

8. What country do you live in? ________________________________

9. Any further comments?

____

____

____

____

____

Thank you very much for your participation!