
# IOT – i

*The Internet of Things Initiative*

# D2.4: 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_D2.4_vFINAL-(120430) |
| Responsible: | HSG |
| Editor(s): | Kowatsch, T. (HSG) and Maass, W. (HSG) |
| List of contributors | Kowatsch, T. (HSG), Maass, W. (HSG), van Kranenburg, R. and Jacobs, T. (NEC) |
| Reviewers | van Kranenburg, R. and Jacobs, T. (NEC) |
| Date of issue: | 30/04/2012 |
| Status: | Delivered |
| Security: | Public |

# Table of Contents

# List of Figures

# List of Tables

# Abstract

Internet of Things (IOT) services – namely sensor-based IS services facilitated by identification technologies such as barcode, radio frequency, IPv6, or global satellite communication – provide new security and privacy challenges in private and business situations of our everyday life. Accordingly, the relevance of privacy and security has been addressed in prior Information Systems research[1] and, as a result, design methodologies, guidelines and policies have been discussed and proposed. However, there still exists no robust empirical instrument that has been developed and successfully tested for the class of IOT services and that combines critical privacy factors and IT acceptance research. Thus, privacy factors need to be identified that have an impact on the behavioural intention to use IOT services, individuals' willingness to pay for these services and their willingness to provide personal information in business situations and private situations. The contribution of this report is therefore to address this lack of knowledge in order to provide policy makers, IT developers and IS researchers with recommendations on how to design IOT services. The proposed underlying research model is based on utility maximization theory and integrates theoretical constructs from the Extended Privacy Calculus Model and the Technology Acceptance Model. This model is empirically tested with 92 IT-savvy subjects via an online survey. Results indicate that behavioural intentions to use IOT services are influenced by various contradicting success factors such as perceived privacy risks and personal interests. That is, the driver of adoption results from the trade-off between these factors. Additionally, success factors depend on the underlying usage situation be it a business situation or a private situation. It can be further stated that contextual factors such as legislation and data security as well as transparency of information use influence the adoption of IOT services. Accordingly, further research must focus on a better understanding of these success factors to increase the adoption of both useful and secure IOT services in the future.


[1] The Information Systems (IS) discipline studies "the effective design, delivery, use and impact of information technology in organizations and society" (Avison and Fitzgerald, 1995, p. xi). One central purpose of IS is therefore to increase the effectiveness and efficiency of (business) organizations (Hevner et al., 2004).

# Section 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, IPv6 or global satellite communication, people face new security and privacy challenges in their private and business life (Weber, 2010). 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, e.g., when those services are running in the background, when the user forgets to terminate them or when there simply exist no fine-granular privacy settings (Scipioni and Langheinrich, 2011). 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 tracked in the background. For example, a healthcare 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 Information Systems (IS) research to a great extent (Anderson and Moore, 2009; Angst and Agarwal, 2009; Dhillon and Backhouse, 2001; Dinev and Hart, 2006; Johnston and Warkentin, 2010; Kosta and Dumortier, 2008; Lopes and de Sá-Soares, 2010; Malhotra et al., 2004; Pramatari and Theotokis, 2009; Siponen and Vance, 2009; Spiekermann, 2009; Warkentin et al., 2011; Weber, 2010). In particular, an IS Security Design framework, IS security guidelines (Siponen and Iivari, 2006), IS security objectives (Dhillon and Torkzadeh, 2006) and information security management standards (Siponen and Willison, 2009) have been primarily discussed and proposed in the context of (business) organizations.

However and to the best of our knowledge, no empirical IS 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 our 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 (Awad and Krishnan, 2006; Rust et al., 2002) and the privacy calculus model (Dinev and Hart, 2006; Laufer and Wolfe, 1977). 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 low privacy concerns are related to high adoption rates of IOT services, respectively.

The contribution of this report 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 report 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 evaluated by 92 subjects. This research model comprises critical factors that predict the behavioural usage intentions of IOT services and the individuals' willingness to provide personal information in order to use them appropriately.

Regarding the description of work (DOW) of IOT-I, this report contributes to the overall objective of Task 2.2, i.e. 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 report "documents the final results of the study concerning potential privacy invasion of IoT technology. It will also include the assessment of the potential impact of the identified strategic applications, and make recommendation on regulatory aspects and government actions for a wider adoption of IoT technology." (ibid., p. 30) In this sense, the current report builds upon the methodology and concepts introduced in IOT-I D2.2 Initial Social Acceptance and Impact Evaluation.

In the following, the research model and hypotheses are presented. Accordingly, two empirical models from privacy research – the Extended Privacy Calculus Model (Dinev and Hart, 2006) – and from IT acceptance research – the Technology Acceptance Model (Davis, 1989) – are combined and tailored to the concept of IOT services (cf. Section 2). In a next step, the research methodology is provided in Section 3 and the results are then presented in Section 4. Finally, the results are discussed in Section 5 before this paper concludes with a brief summary and an outlook on future work in Section 6.

# Section 2: Research Model and Hypotheses

The research model and hypotheses of the current study are depicted in Figure 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, Dinev and Hart, 2006). 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 tailored to the concept of an IOT service as the latter extends the transactions of information on the Internet to the physical world. However, it must be also noted here that EPCM can only serve as a base for the evaluation of IOT services. It needs refinements and additions of which this report provides a very first contribution.

Additionally, two constructs from the Technology Acceptance Model (TAM, Davis, 1989) 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 (Davis and Venkatesh, 2004; Kamis et al., 2008; Venkatesh et al., 2003). TAM is rooted in the social sciences, in particular, the theory of reasoned action (Ajzen and Fishbein, 1980; Fishbein and Ajzen, 1975) and its successor, the theory of planned behaviour (Ajzen, 1991). Both theories fundamentally state that individuals' believes influence behavioural intentions that, in turn, have an effect on actual behaviour. The target behaviour of interest in the IS community was then the adoption and sustainable usage of IS artefacts that might have positive effects on organizational key performance indicators.

Finally, we use the willingness to pay construct that has been adapted from the intention to purchase construct of existing TAM research (Kamis et al., 2008; Kowatsch and Maass, 2010). That is, with this construct more detailed information can be gathered whether people are even willing to pay for IOT services in addition to just indicating their behavioural intention to use them.

Consistent with EPCM, TAM was not originally developed for the evaluation of IOT services. Therefore, definitions of constructs and questionnaire items are revised carefully in the current work such that they apply to the IOT context, too.

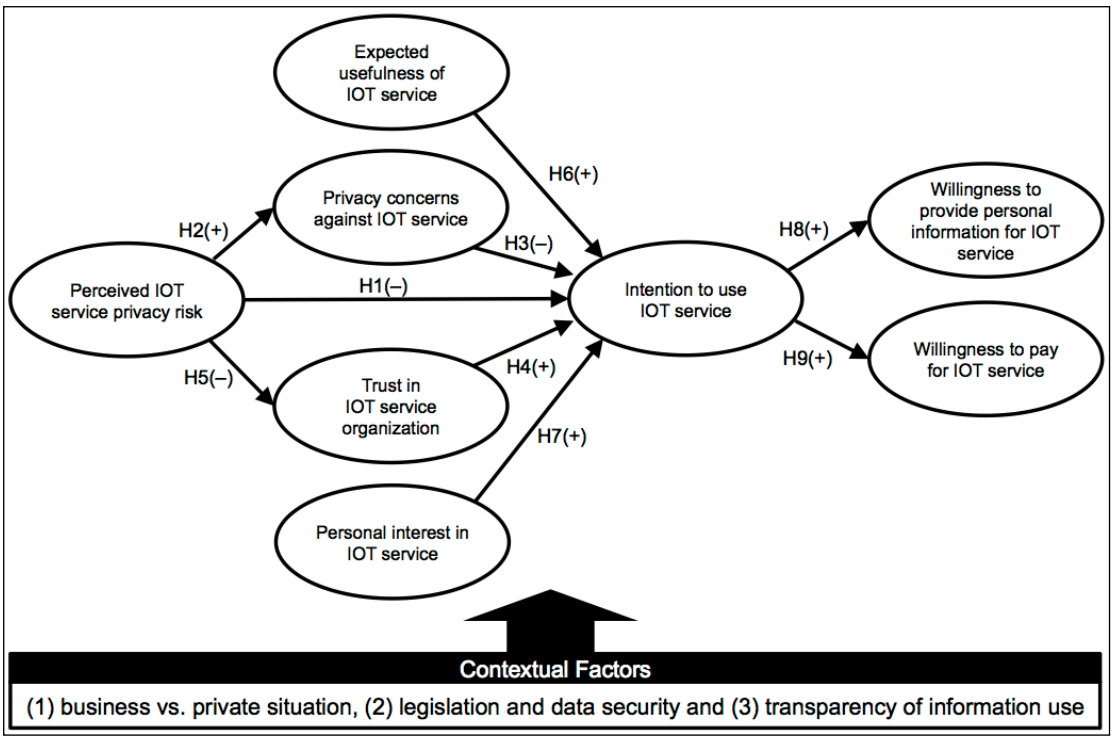


**Figure 1. Research model.**

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 eight constructs are adapted from Dinev and Hart (2006, p.64, Table 1), Davis (1989, p. 320ff) and Kamis et al. (2008) such that they apply to the concept of IOT services. Hereby, IOT services are defined as sensor-based IS services that support people in everyday situations, i.e. in business situations and private situations. The five construct definitions as adapted from EPCM to IOT services are listed in the following:

- **Perceived IOT service privacy risk** reflects perceived risk of opportunistic behaviour related to the disclosure of personal information of IOT service users. That is, perceived IOT service privacy risks are risk believes that are derived from a risk evaluation of IOT services *in general*.
- **Privacy concerns against IOT service** are concerns about opportunistic behaviour related to the personal information transferred to the IOT service by the individual respondent *in particular*. That is, privacy concerns reflect "an internalization of the possibility of loss … [and, the authors] is an assessment about what happens to the personal information that the user discloses" (Dinev and Hart, 2006, p. 65) while using an IOT service.
- **Trust in organization providing the IOT service** summarizes trust believes reflecting confidence that personal information transferred to the IOT service organization will be handled competently, reliably, and safely. Although trust believes can be seen as an opposite of risk believes (see above), it is assumed that both believes capture different perceptions and that they can exist in parallel. For example, one could generally trust an

IOT service provider but at the same time one might be aware of risks associated with personal information that are transferred electronically.

- **Personal interest in an IOT service** reflects the cognitive attraction to an IOT service while overriding privacy concerns. That is, "personal interest is a belief that reflects a level of enticement to transact." (Dinev and Hart, 2006, p. 67)
- **Willingness to provide personal information for an IOT service** reflects the degree to which individuals are likely to provide personal information such as location-based information or financial information required to complete transactions of a particular IOT service. This implies also that even though individuals are not willing to provide personal information they may have no choice (e.g., using a public transport payment service while having no car).

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

- **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 an IOT service** reflects behavioural expectations of individuals that predict their future use of the IOT service.
- **Willingness to pay for IOT service** is defined as the degree to which an individual is likely to pay for an IOT service.

Two modifications were made 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 and the willingness to pay for that IOT service. The rationale for this relationship lies in the fact that an individual person (1) would not provide his or her personal information for a particular IOT service or (2) would not be willing to pay for an 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 assumption 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).

It must be noted that the construct perceived ease of use from TAM was not adopted in the current study as the focus lies on potentially relevant IOT services that might be developed in the very near future. It is therefore not possible to measure ease of use at this early stage of investigation, i.e. without prototypes that could be physically tested. In summary, the following eight hypotheses are derived from EPCM, TAM and the assumptions as discussed above:

**H1:** Perceived IOT service privacy risk is negatively related to the intention to use that service.

**H2:** Perceived IOT service privacy risk is positively related to privacy concerns against that service.

**H3:** Privacy concerns against an IOT service are negatively related to the intention to use that service.

**H4:** Trust in the organization that provides an IOT service is positively related to the intention to use that service.

**H5:** Perceived IOT service privacy risk is negatively related to trust in the providing organization.

**H6:** Expected usefulness of an IOT service is positively related to the intention to use that service.

**H7:** Personal interest in an IOT service is positively related to the intention to use that service.

**H8:** Intention to use an IOT service is positively related to the willingness to provide personal information for that service.

**H9:** Intention to use an IOT service is positively related to the willingness to pay for that service.

In addition to these nine hypotheses, it is investigated how contextual factors may influence these relationships (cf. Figure 1). 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 quality of information and frequency of notification a user of an IOT service should get such that tracking of personal data is transparent enough.

# Section 3: Method

In order to test the research model, an online survey was developed. For this reason, four IOT services embedded in two business situations and two private situations were identified from a pool of 57 IOT situations that have been originally identified from the IOT-I survey conducted as part of IOT-I Task 2.1 (Presser and Krco, 2011). The rationale behind the evaluation of situational descriptions is based on the Situational Design Method for IS (SiDIS), formerly known as CoDesA (Janzen et al., 2010; Maass and Janzen, 2011). In SiDIS, situational descriptions are one of the first steps towards the design of IT artifacts such as IOT services.

The identification of relevant IOT situations was conducted in three steps.[2] First, an overall relevance score was calculated for each IOT situation based on results of a pretest survey. In that pretest, overall 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 a particular IOT service. Hereby, five-point Likert scales ranging from low (1) to high (5) were employed. The calculation was conducted as shown in Figure 2 for an example IOT situation. First, the mean values of each of the six questionnaire items[3] were calculated (cf. IOT-I D2.1 Presser and Krco, 2011). 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 of 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 and the two best-ranked business situations and private situations have been chosen (cf. IOT-I D2.2 Initial Social Acceptance and Impact Evaluation).

In the third and final step, a second pretest was conducted in which 12 IOT-I experts gave their feedback on the wording and consistency of situations that have been identified in Step 2. The resulting IOT-I services together with their situational descriptions are presented in Table 1.

[2] The three steps for the identification of relevant IOT situations has been developed exclusively for this IOT-I task because no related work could be adopted in this regard.
[3] 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.

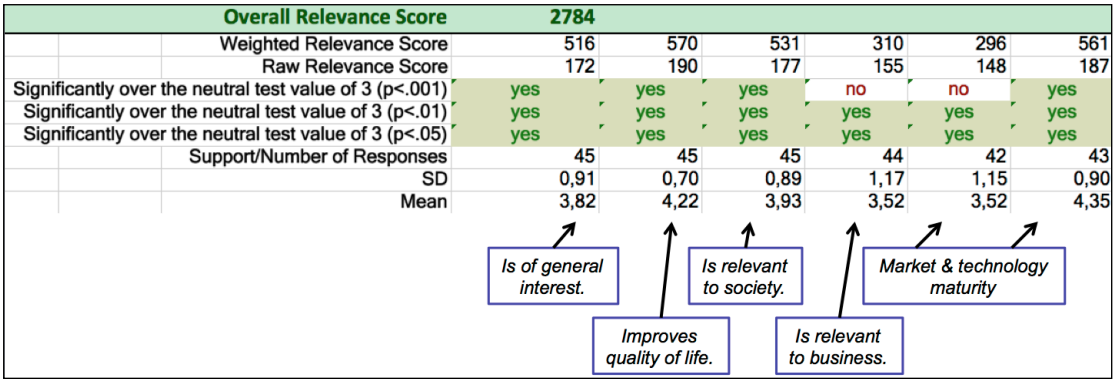


**Figure 2. Relevance score calculation for the identification of relevant IOT-I services**

| No | IOT service | Situation in the form of a narrative | Focus |
|---|---|---|---|
| 1 | Public Transport Payment Service | You are taking the bus to work and receive a message from the public transport company via your mobile phone. They offer you a payment service that charges you once you get off the bus based on the number of zones you cross. The information also displays the cost per zone. After your authorisation payment is performed automatically via your mobile phone. | Business situation |
| 2 | Navigation Service | You leave your home for a business trip and 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 information together with other personal data relevant for the navigation service in the Internet cloud. | Business situation |
| 3 | Smart Energy Service | You live in a modern house and the Smart Energy Service manages your energy consumption. It combines data from outdoor and indoor temperature, weather forecast from the Internet, and user preferences. It also recognizes which appliances (e.g., washing machine, dish washer, water heater, heating system) 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 your health condition is taking a turn for the worse. As a result, you have upgraded the current health monitoring solution with sensor applications that enable the monitoring of your location, posture and general health condition at home and in the neighborhood. As a result, you retain your private and social life, which is very important for coping with your condition and happiness. | Private situation |

**Table 1. IOT services, situations and focus**

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 three 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). And third, willingness to pay for an IOT service has been adapted from Kamis et al. (2008), Kowatsch and Maass (2010) and Kowatsch et al. (2011). 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 users of IOT services should be informed about the use of personal information in terms of degree of detail and notification frequency. In order to better understand individuals' concerns about the four IOT services, two qualitative statements have been added that ask for concerns and recommendations to overcome them. All of these questionnaire items are listed in Table 3.

Finally, variables such as technology affinity, 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).

The sampling of subjects was conducted online through various media channels of the IOT-I partner organizations in March and April 2012. Thus, invitations to participate in the online survey were communicated via the project websites of IOT-I and IOT-A, Twitter, IOT LinkedIn groups or the Internet of Things Council[4]. A lottery with five Amazon gift cards was used to motivate participation. Based on the feedback from the questionnaire-based study at IOT week in Barcelona in 2011 (cf. IOT-I D2.2 Initial Social Acceptance and Impact Evaluation) and because of time considerations of online studies in general, each participant was now randomly assigned to exactly one IOT service from Table 1 instead of asking her to evaluate all services step by step. As a result, empirical data entries of the four IOT services are independent from each other. Each subject had to read through the corresponding narrative of the IOT service and was then asked to evaluate this service with the help of the questionnaire items.

[4] For example: http://www.theinternetofthings.eu/tobias-kowatsch-iot-i-critical-privacy-factors-internet-things-services-request

| No. | Construct and scale item wording |
|---|---|
| | ***Perceived IOT service privacy risk***<br>*Likert-scale from very low risk (1) to very high risk (7)*<br><br>What do you think is the risk that personal information used by this 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***<br>*Likert-scale from not at all concerned (1) to very concerned (7)*<br><br>I am concerned … |
| PC1 | … that the information recorded by this service could be misused. |
| PC2 | … that a person or authority can find private information about me when I use this service. |
| PC3 | … about information used by this service, because of what others might do with it. |
| PC4 | … about information used by this service, because it could be used in a way I did not foresee. |
| | ***Trust in organizations providing the IOT service***<br>*Likert-scale from strongly disagree (1) to strongly agree (7)*<br><br>[Public transport companies \| Navigation system companies \| Home automation companies \| Health insurance companies] provide this service … |
| TO1 | … in a safe way such that information can be exchanged electronically. |
| TO2 | … in a reliable way such that transactions can be conducted. |
| TO3 | ... handle personal information in a competent fashion. |
| | ***Expected usefulness of IOT service***<br>*Likert-scale from strongly disagree (1) to strongly agree (7)*<br><br>I expect that using this service… |
| EU1 | … can improve my performance. |
| EU2 | … improve my productivity. |
| EU3 | … can improve my effectiveness. |
| EU4 | … would be generally useful. |
| | ***Personal interest in IOT service***<br>*Likert-scale from strongly disagree (1) to strongly agree (7)* |
| PI1 | I find that my personal interest in this service overrides my privacy concerns. |
| PI2 | The greater my interest in this service, the more I tend to suppress my privacy concerns. |
| PI3 | In general, my need to use this service is greater than my concern about privacy. |
| | ***Intention to use IOT service***<br>*Likert-scale from strongly disagree (1) to strongly agree (7)* |
| IU1 | I would use this service. |
| IU2 | I could imagine using this service. |
| | ***Willingness to Provide Personal Information***<br>*Likert-scale from strongly disagree (1) to strongly agree (7)* |
| WPI1 | I would provide accurate and identifiable personal information for using this service. |
| WPI2 | I would provide personal financial information (e.g. credit card information) in order to pay the service fees. |
| | ***Willingness to Pay for IOT service*** *(Note: It was additionally asked for the absolute amount in Euro; For the Public Transport Payment service it was also asked the amount relative to the ticket price in per cent for WP3) Likert-scale from very unlikely (1) to very likely (7)*<br><br>If you actually had the money how likely is it that you would pay ... |
| WP1 | … one time a fixed price for this service? |
| WP2 | … a monthly fee for this service? |
| WP3 | … a service fee for each usage? |

**Table 2. Questionnaire items. Note: Items vary slightly with respect to the IOT service (cf. Appendix A – Survey Instrument)**

| No. | Item wording |
|---|---|
| | ***Data security and legislation***<br>How would you like your personal information to be protected regarding this service? |
| DSL1 | By international law, which is probably more practical, but may take longer in developing. |
| DSL2 | By soft law, i.e. regulations are established by private organizations. |
| DSL3 | By technical means such as encrypted communication channels and data stores. |
| DSL4 | Other: [free text feedback] |
| | ***Qualitative notification on personal information use***<br>How would you like to be informed that your personal information will be used by this service? |
| QN1 | General indication without any details. |
| QN2 | Specific and detailed information. |
| QN3 | Other: [free text feedback] |
| | ***Frequency of notification on personal information use***<br>When would you like to be informed that your personal information will be used by this service? |
| FN1 | Only the first time personal information is used. |
| FN2 | Every time when personal information is used. |
| FN3 | On my own request. |
| FN3 | Other: [free text feedback] |
| | **Concerns about IOT services and recommendations to overcome them** |
| CON | What are your most serious concerns about this service? |
| REC | What are your personal recommendations – from an organizational, individual or technical point of view – to address your concerns? |

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

# Section 4: Results

## *4.1 Descriptive statistics*

Overall, 69 male and 23 female subjects participated in the online survey. The distribution by gender is shown in Figure 3. The age of the subjects ranged from 24 to 62 with a mean value of 35.4 and a standard deviation of 8.87. The boxplots[5] of the subjects' age is depicted in Figure 4. The distribution of subjects by country is shown in Figure 5. It indicates that the majority of subjects live in Germany and thus, results of the current study are biased in this regard. Furthermore, subjects can be characterized as technically savvy, because with 6.11 the mean value of the technology affinity construct (two-item scale, Cronbach's Alpha = .80) lies significantly above the neutral scale value of 4 on a 7-point Likert scale by applying a one-sample t-test. The boxplot for the technology affinity construct is given in Figure 6 for each service.

Moreover, subjects found that the instructions of the online survey were clear and understandable (Mean: 5.32, Std. Dev.: 1.42) and that the overall length was acceptable (Mean: 4.26, Std. Dev.: 1.62) which was measured on 7-point Likert scales ranging from strongly disagree (1) to strongly agree (7).

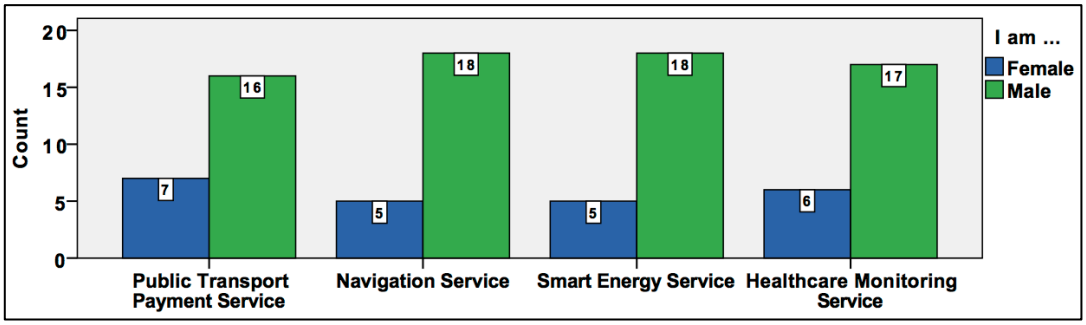


**Figure 3. Distribution of female and male subjects (n=92)**

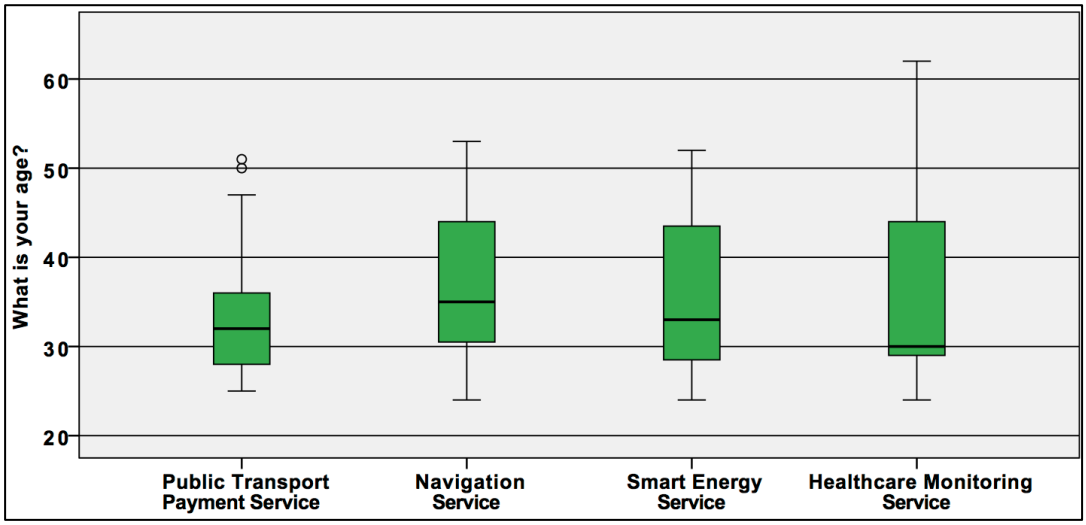


**Figure 4. Boxplot of subjects' age (n=92)**

[5] http://en.wikipedia.org/wiki/Box_plot

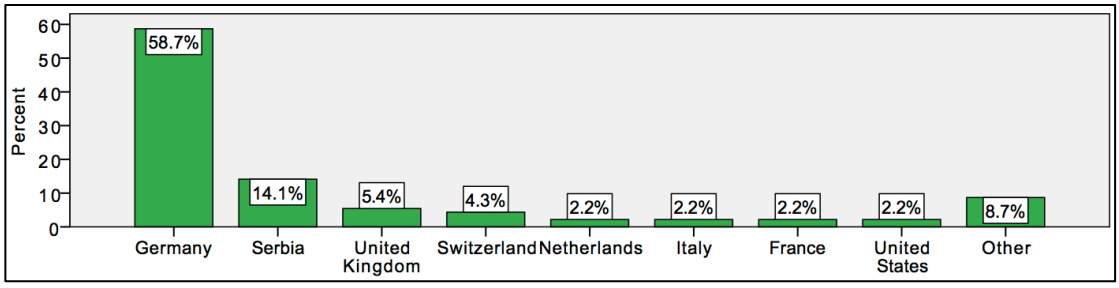


**Figure 5. Distribution of subjects by country (n=92)**

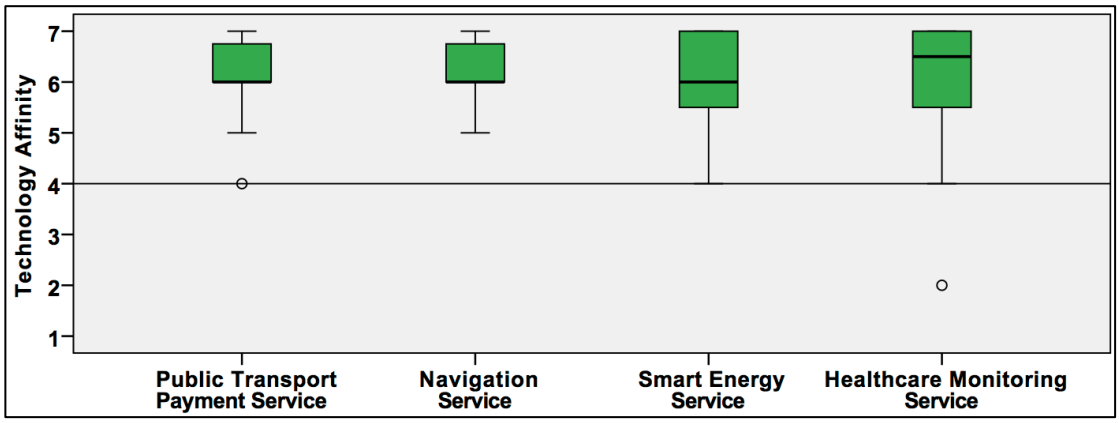


**Figure 6. Boxplot of subjects' technology affinity (n=92, 1=low, 7=high)**

The descriptive statistics of the questionnaire items and their underlying 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, intention to use IOT service, willingness to provide personal information for IOT service and willingness to pay for IOT service are listed in Table 4. Cronbach's Alpha lies over the recommended threshold of .70 (Nunnally, 1967) for all scales with four exceptions, where the value lies between .615 and .682. However, to be consistent with prior research (Dinev and Hart, 2006), the corresponding items were not dropped for further analysis. Accordingly, aggregated values were calculated for multi-item scales of the theoretical constructs. One-sample t-tests were additionally conducted for each aggregated value in order to indicate whether the mean value lies significantly above or below the neutral scale value of four. That is, one-sample t-tests show whether the subjects have rated the constructs rather positive, neutral or negative.

| Statistic | Public Transport Payment Service (n=23) | Navigation Service (n=23) | Smart Energy Service (n=23) | Healthcare Monitoring Service (n=23) |
|---|---|---|---|---|
| ***Perceived IOT service privacy risk*** | | | | |
| Items | | 5 | | |
| Alpha | .819 | .774 | .920 | .760 |
| Mean | **4.99** | **5.43** | **4.93** | **4.64** |
| St. Dev. | 1.12 | 1.00 | 1.49 | 1.16 |
| p-value | .000 | .000 | .007 | .015 |
| ***Privacy concerns against IOT service*** | | | | |
| Items | | 4 | | |
| Alpha | .914 | .867 | .947 | .913 |
| Mean | **4.96** | **5.49** | **5.05** | **5.10** |
| St. Dev. | 1.34 | .91 | 1.60 | 1.46 |
| p-value | .002 | .000 | .005 | .002 |
| ***Trust in organizations providing the IOT service*** | | | | |
| Items | | 3 | | |
| Alpha | .832 | .645 | .904 | .782 |
| Mean | **4.83** | 4.23 | **4.96** | 4.46 |
| St. Dev. | 1.22 | 1.06 | 1.42 | 1.20 |
| p-value | .004 | .304 | .004 | .076 |
| ***Expected usefulness of IOT service*** | | | | |
| Items | | 4 | | |
| Alpha | .915 | .859 | .865 | .943 |
| Mean | **5.78** | **5.57** | **5.48** | **5.91** |
| St. Dev. | 1.25 | .84 | .89 | 1.29 |
| p-value | .000 | .000 | .000 | .000 |
| ***Personal interest in IOT service*** | | | | |
| Items | | 3 | | |
| Alpha | .862 | .861 | .782 | .645 |
| Mean | 4.20 | 4.04 | 4.32 | 4.49 |
| St. Dev. | 1.63 | 1.35 | 1.29 | 1.33 |
| p-value | .557 | .879 | .250 | .088 |
| ***Intention to use IOT service*** | | | | |
| Items | | 2 | | |
| Alpha | .937 | .798 | .871 | .938 |
| Mean | **5.09** | **5.02** | **5.28** | **5.41** |
| St. Dev. | 1.64 | 1.07 | 1.10 | 1.28 |
| p-value | .004 | .000 | .000 | .000 |
| ***Willingness to Provide Personal Information*** | | | | |
| Items | | 2 | | |
| Alpha | .729 | .615 | .772 | .682 |
| Mean | 3.87 | 3.76 | 4.27 | 4.52 |
| St. Dev. | 1.42 | 1.55 | 1.72 | 1.70 |
| p-value | .663 | .468 | .633 | .154 |
| ***Willingness to Pay for IOT service*** | | | | |
| ***WP1 (fixed price)*** | | | | |
| Mean | 3.83 | **4.78** | 4.13 | 4.61 |
| St. Dev. | 1.97 | 1.65 | 1.66 | 1.92 |
| p-value | .676 | .033 | .710 | .144 |
| ***WP2 (monthly fee)*** | | | | |
| Mean | 3.39 | **3.00** | 4.39 | 4.26 |
| St. Dev. | 2.15 | 1.41 | 1.50 | 1.96 |
| p-value | .188 | .003 | .224 | .530 |
| ***WP2 (pay per use)*** | | | | |
| Mean | 4.13 | 3.96 | 4.78 | 4.61 |
| St. Dev. | 2.20 | 1.99 | 1.86 | 1.67 |
| p-value | .779 | .917 | .056 | .095 |

**Table 4. Statistics of the constructs. Note: p-values are derived from one-sample t-test with a test value of 4; mean values marked in green / red are rated significantly positive / negative by subjects.**

Results of the willingness to pay items where subjects had to indicate absolute values in Euro are depicted in Figure 7. Because of the low response rate of these particular items (n=10) – the items were only shown when subjects indicated that they were willing to pay for an IOT service (cf. WP1-3 in Table 4), general implications cannot be drawn from this data.

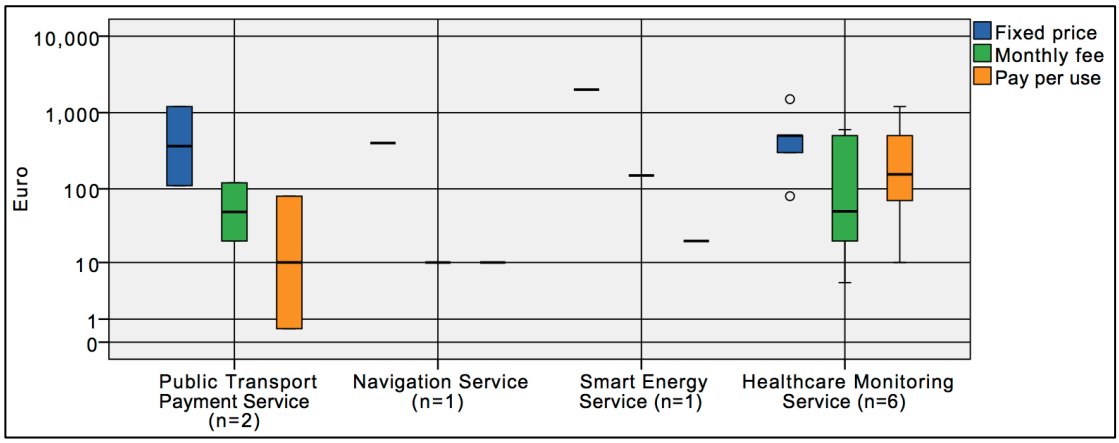


**Figure 7. Boxplot of willingness to pay for IOT service in Euro.**

## *4.2 Test of hypotheses*

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 three hypotheses are fully supported by the data for all evaluated IOT services (H2, H4 and H7) whereas the other six hypotheses are partly supported. Consistent with the research model and as an overview of these results, Figure 8 depicts significant, partly significant and non-significant correlation coefficients.

| Hypothesis | Public Transport Payment Service | Navigation Service | Smart Energy Service | Healthcare Monitoring Service | Result |
|---|---|---|---|---|---|
| **H1**: PR * IU | –.511* | –.504* | –.269$^{n.s.}$ | –.426* | Partly accepted |
| **H2**: PR * PC | .815*** | .626** | .826*** | .793*** | Accepted |
| **H3**: PC * IU | –.498* | –.169$^{n.s.}$ | –.375$^{n.s.}$ | –.398$^{n.s.}$ | Partly accepted |
| **H4**: TO * IU | .567** | .578** | .523* | .588** | Accepted |
| **H5**: PR * TO | –.383$^{n.s.}$ | –.351$^{n.s.}$ | –.443* | –.065$^{n.s.}$ | Partly accepted |
| **H6**: EU * IU | .714*** | .239$^{n.s.}$ | .592** | .327$^{n.s.}$ | Partly accepted |
| **H7**: PI * IU | .785*** | .621** | .415* | .546** | Accepted |
| **H8**: IU * WPI | .474* | –.045$^{n.s.}$ | .111$^{n.s.}$ | .726*** | Partly accepted |
| **H9:** IU * WP1 | .167 | –.460$^{*}$ | .066$^{n.s.}$ | .504* | Partly accepted |
| IU * WP2 | .125 | –.255$^{n.s.}$ | –.112$^{n.s.}$ | .655*** | |
| IU * WP3 | .531** | –.096$^{n.s.}$ | –.058$^{n.s.}$ | .399 | |

**Table 5. Pearson correlation coefficients for the nine hypotheses. Note: n=23 for each service, * = p < .05 / ** = p < .01 / *** = p < .001, n.s. = not significant**

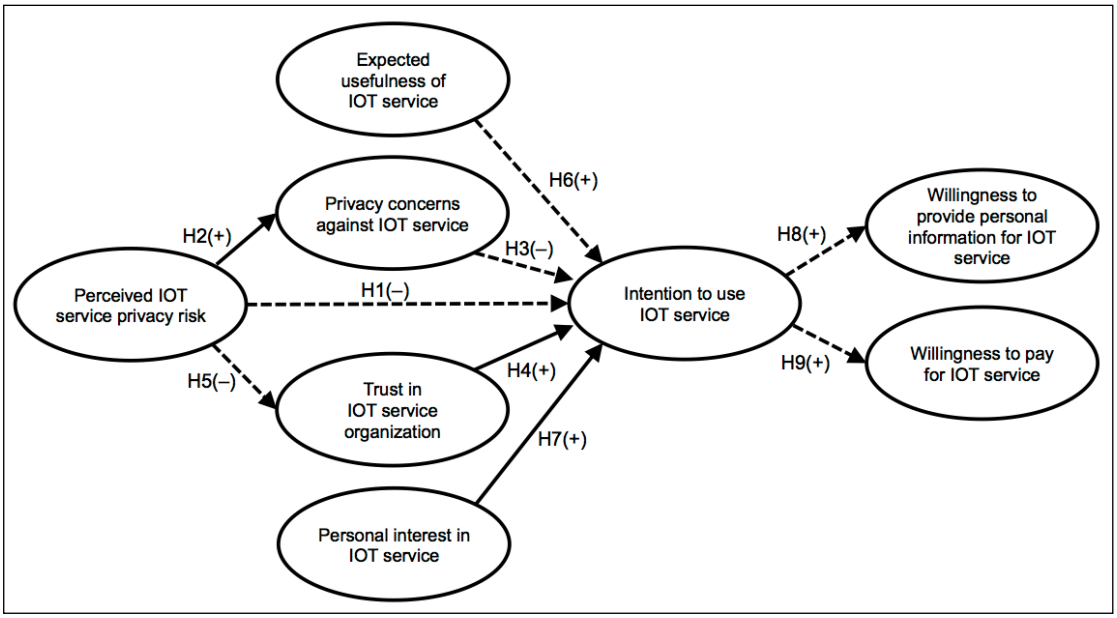


**Figure 8. Significant and partly significant (dashed) correlations.**

## *4.3 Contextual factors*

Descriptive statistics related to the questionnaire items on legislation and data security are presented in Figure 9. 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. Subjects also reported that national law should be used to regulate the protection of personal information in addition to contracts and agreements from an individual point of view.

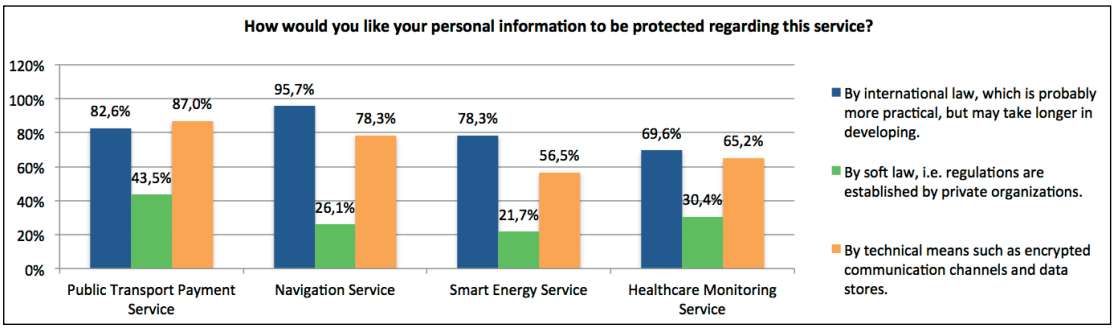


**Figure 9. Legislation and data security (n=23 for each service)**

Results on the preferred level of detail of notifications on personal information use are depicted in Figure 10. It was also reported that trust into the IOT service provider could have a strong influence on these results and that details on personal information use should only be made available to the user the first few times. Another subject pointed out that the detail of notification should

be an option of the IOT service that can be individually changed according to users' preferences.

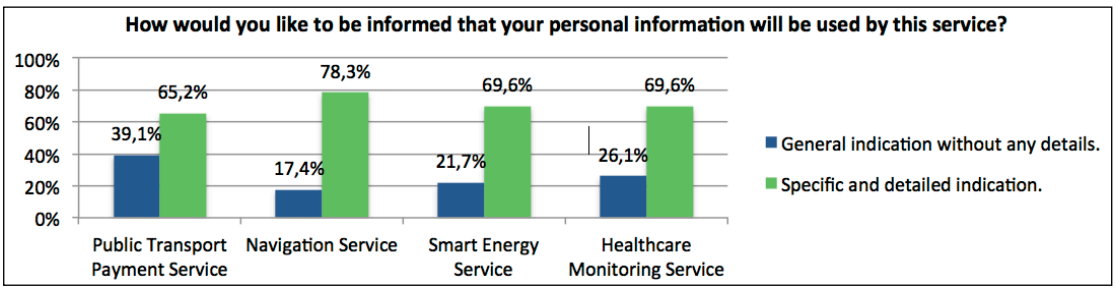


**Figure 10. Preferred level of detail of notifications on personal information use (n=23 for each service)**

Feedback regarding the frequency of notifications on personal information use is shown in Figure 11. It was further reported that the kind of frequency of notifications should be an editable option of the IOT service. Another feature that was requested is a list of the last transactions in form of a transaction history. Finally, subjects pointed out that rule-based notifications could help the identification of relevant new kind of data transactions.

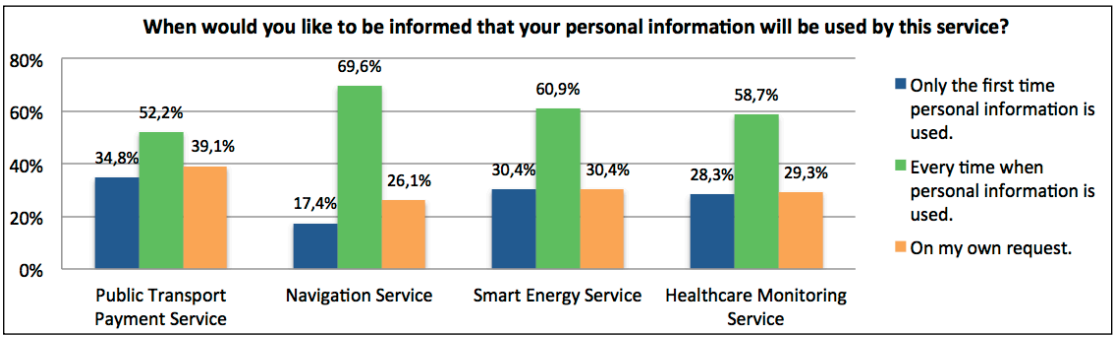


**Figure 11. Preferred frequency of notification regarding personal information use (n=23 for each service)**

Finally, the 92 subjects have listed 177 concerns and gave 134 recommendations or comments on how to address them. The detailed list for each of the four evaluated IOT services is provided in Appendix B of the current report.

# Section 5: Discussion

Overall, the results of the IOT survey on critical privacy factors show that the empirical data of the 92 subjects support the proposed research model and corresponding hypotheses. A detailed discussion of the results is presented in the following.

## *5.1 General implications*

First of all, all four IOT services, i.e. public transport payment service, navigation service, smart energy service and healthcare monitoring service, selected from the IOT survey in 2011 (Presser and Krco, 2011) are perceived as relevant by the subjects. That is, ratings of the two constructs expected usefulness and intention to use lie significantly above the neutral test value of four for all four IOT services (cf. Table 4). And thus, these services are potential candidates that are probably adopted in the very near future.

Second, tough all four IOT services are perceived as relevant, subjects are indifferent whether or not to provide personal information for using them. 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 of four (cf. Table 4). Therefore, subjects are uncertain in terms of providing access to their personal information. With a mean value of 4.52, there is only a positive tendency of ratings that subjects would provide their personal information for using the healthcare monitoring service. This finding is consistent with the results of the initial report IOT-I D2.2 (Kowatsch and Maass, 2011). It could be explained by the fact that the healthcare monitoring service addresses a serious disease, a situation, in which subjects might be more concerned with their state of health than with privacy intrusion.

Third, there exist significant perceived privacy risks and privacy concerns with regard to all four IOT services. The descriptive statistics of Table 4 support this statement because all evaluations of perceived privacy risks and privacy concerns lie significantly above the neutral scale value of four. The numerous concerns listed in Appendix B underline this finding, too. It is therefore strongly recommended to take these privacy risks and privacy concerns seriously into account during the design and implementation of such kind of IOT services, because they might be a major barrier of IOT service adoption. Comparing these results with the indifference on whether or not to provide personal information from above, there must exist other factors that mitigate risk believes and that are described below (e.g. trust in IOT organizations and personal interest in IOT services).

Fourth, subjects are generally indifferent on whether or not to pay for the four services. The reason for that may lie in the fact that the evaluated IOT services were presented in the form of brief textual descriptions and thus, subjects were not able to test their utility and practicability in everyday situations. It is therefore assumed that subjects have rated this construct with caution. Nevertheless, results from Table 4 show that the revenue model of the navigation service should be based on a fixed one-time price and definitely not a monthly fee. By contrast, the public transport payment service and the smart

energy service should be rather priced on the pay-as-you-use principle, whereas subjects preferred a fixed pricing model and the pay-as-you-use for the healthcare monitoring service.

Fifth, 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. It was further extended with three constructs from the Technology Acceptance Model (TAM, Davis, 1989). All in all, the proposed research model was tested successfully. That is, all hypotheses are supported by the empirical data either completely – by all IOT services (H2, H4 and H7) – or at least by one IOT service (H1, H3, H5-6 and H8-9). It can be also stated that there are no obvious differences between the IOT services used in the (1) business situations with the public transport payment service and navigation service, or (2) the private situations with the smart energy service and the healthcare monitoring service. In particular, it could be shown that perceived privacy risk and privacy concerns have a positive relationship at the .001 level of significance. However, these constructs do not consistently predict the behavioural intention to use IOT services. By contrast, the behavioural intention to use IOT services is significantly influenced by trust in the service providing (business) organizations and the personal interest in the IOT service at least on the .05 level of significance. Thus, it can be concluded that trust and personal interest are more important factors for end users than privacy risks and privacy concerns. This result is consistent with the findings of Dinev and Hart (2006) who studied the behaviour of individuals in the context of electronic commerce transactions. They also state that a "high level of behavioral intention must be preceded by higher levels of confidence and enticement beliefs than the levels of general and specific privacy risk believes. Higher levels of privacy risk beliefs would suggest user resistance to personal information disclosure" (ibid, p. 73) which is assumed to be a reason for this finding, too. Accordingly, organizations should primarily address trust and personal interests in the development process and marketing activities of their IOT services such that the acceptance in the society can be increased.

Sixth, results on legislation and data security (Figure 9) as well as the preferred level of detail and frequency of notification of personal information use (Figure 10 and Figure 11) provide clear guidelines for design and implementation processes of IOT services. Accordingly, approximately 82% of the 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 for which circa 30% of the subjects voted. In addition to these legislative aspects, personal information should be also protected by technical means as indicated by 72% of the subjects (cf. Figure 9). Thus, state of the art encryption and security standards should be incorporated and advertised together with the pure functionality of IOT services.

Seventh, 71% of the 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 10). Another but related approach would be a system that matches privacy preferences of individuals with the privacy policies of IOT service providers. A mobile application that implements this approach is the Privacy Coach (Broenink et al., 2010).

Eighth, the majority of subjects – approximately 60% – stated that they want to be informed every time when personal information is used by an IOT service. However, also 30% of the subjects want to be informed only the first time personal information is used and 31% would like to actively request that information (cf. Figure 11). Even though the default option should be a trigger that informs users of an IOT service every time personal information is forwarded to a third-party organization, this makes particularly only sense for IOT services that are used rather infrequently, i.e. once a month or less. It is thus recommended to provide an option that allows changing the trigger of notification individually and to decide on the default option based on the frequency of average IOT service usage.

Finally, we recommend IOT service providers to conduct a privacy impact assessment (PIA) as proposed in prior work for applications that use radio-frequency identification technology (RFID) (European Commission, 2011; Oetzel et al., 2011). It must be only taken into account that IOT services might not only use RFID but also other sensor technologies such as the global positioning system (GPS) or indoor-tracking technologies. A decision tree as depicted in Figure 12 can help in the initial analysis whether and to which degree a PIA should be conducted. Based upon this initial analysis, the PIA methodology can be adopted for IOT services as depicted in Figure 13. Further details on PIA and its methodology can be found in Oetzel et al. (2011).

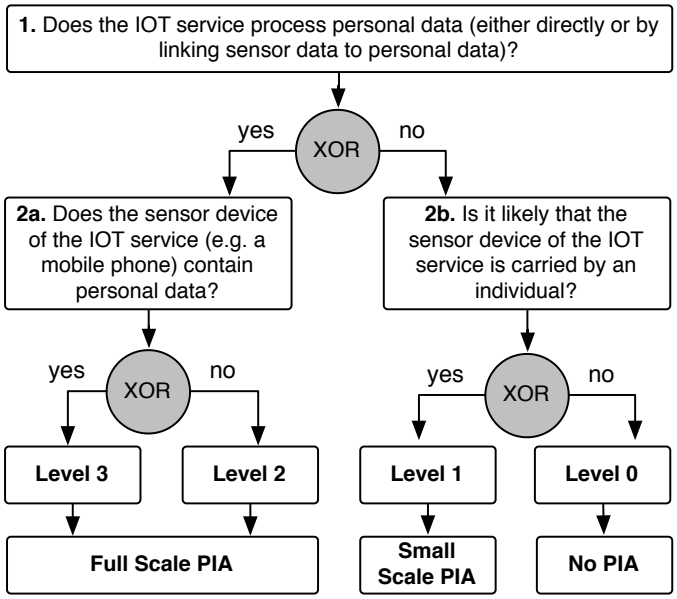


**Figure 12. Decision tree for initial analysis whether and to which degree a privacy impact assessment (PIA) should be conducted. Note: the figure was adapted from (European Commission, 2011) to IOT services; XOR means exclusive OR**

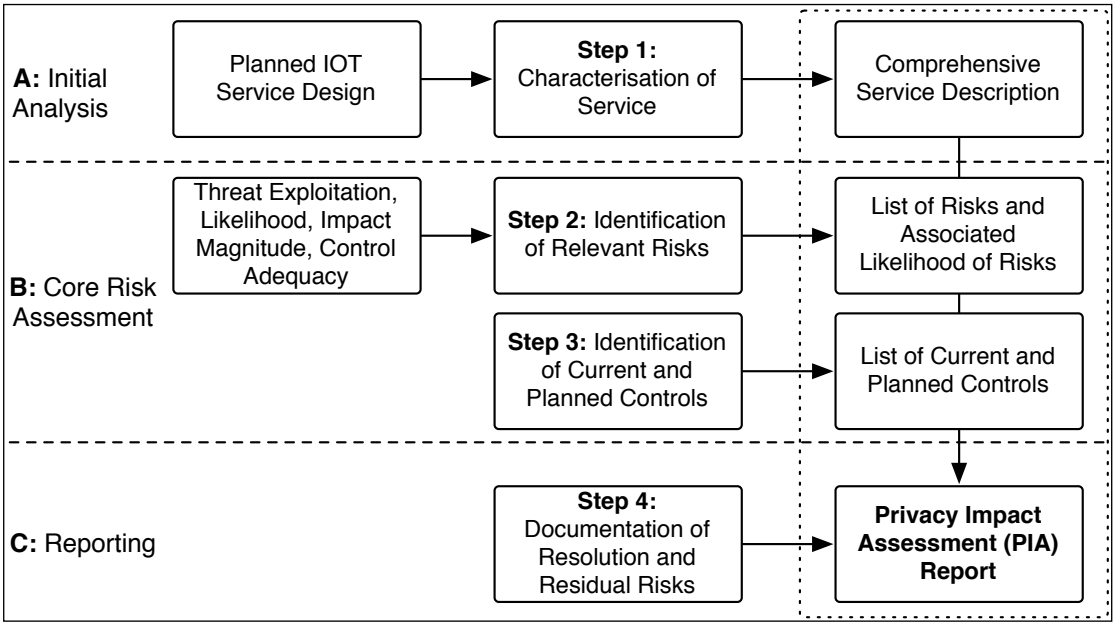


**Figure 13. Privacy Impact Assessment (PIA) process reference model for IOT services. Note: the figure has been adapted from Oetzel et al. (2011)**

## *5.2 Limitations*

The current study has several limitations. First, with regard to the over-average ICT affinity of the subjects (cf. Figure 6), results are biased in the sense that primarily male and technology-savvy persons have participated in the online 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 experiments or field experiments that would all increase subjects' understanding of the IOT services and thus the quality of evaluations. In addition to that, findings of the current study are biased towards the origin of the subjects, i.e. almost 60% live in Germany.

Nevertheless, the results of the current report are a valid starting point into the investigation of IOT-based services bearing in mind the restrictions discussed above.

## *5.3 Summary of core findings*

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

| # | Finding |
|---|---|
| 1 | An empirical instrument has been proposed for the class of IOT applications, i.e. the research model in Figure 1 and the questionnaire items in Table 2 and Table 3. It addresses perceived privacy concerns and technology adoption aspects not only in the business context and private context but considers also other contextual factors such as legislation and data security as well as transparency of information use. This instrument can be reused for IOT-related services. |
| 2 | The following four IOT services used in business and private situations have been identified as potential candidates that are going to be adopted in the very near future (cf. also Kowatsch and Maass, 2011; Presser and Krco, 2011):<br>• Public Transport Payment Service (Business Situation)<br>• Navigation Service (Business Situation)<br>• Smart Energy Service (Private Situation)<br>• Healthcare Monitoring Service (Private Situation) |
| 3 | The empirical instrument was tested successfully, i.e. all hypothesized relationships were supported by the empirical data of at least one of the four IOT services. Overall, none of the hypothesized relationships was rejected. Thus, relevant privacy factors have been identified for the design and implementation of future IOT services. |
| 4 | There seems to be a trade-off between privacy concerns and perceived privacy risks on the one hand and trust in IOT service organizations, expected usefulness of and personal interests in IOT services on the other hand. All factors influence the behavioural intention to use a particular IOT service but trust and personal interest are more significant predictors of IOT service adoption. |
| 5 | International law and technical barriers should be of a primary concern to IOT-related stakeholders in order to protect personal information. |
| 6 | Potential 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. Lab experiments and field experiments are also recommended such that IOT services can be tested physically in everyday situations. |
| 9 | A general privacy impact assessment is recommended to IOT service providers such that the likelihood of individual privacy risks and can be identified early in the design process and adequate controls can be implemented accordingly. |

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

# Section 6: Conclusion and Outlook

In this final IOT-I report on social acceptance and impact evaluation 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 an online survey with 92 participants. 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 legislation, data security and notification of personal information use, all relevant for the design and development of IOT services such that they are probably accepted by society.

Future work should test the current results with a wider data basis by conducting further studies. The overall objective should be then to cross-check the current findings by adding external validity and thus, to increase the quality of implications. Nevertheless, organizations should generally perform privacy impact assessments as described in prior work (European Commission, 2011; Oetzel et al., 2011) such that their IOT services are not only useful but also technically secure and address the privacy concerns of their users.

# 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.

Avison, D. and Fitzgerald, G. (1995). Information Systems Development: Methodologies, Techniques and Tools. (2nd ed.) McGraw-Hill, London, UK.

Awad, N.F. and Krishnan, M.S. (2006). 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.

Broenink, G., Hoepman, J.-H., van 't Hof, C., van Kranenburg, R., Smits, D. and Wisman, T. (2010) The Privacy Coach: Supporting customer privacy in the Internet of Things. http://arxiv.org/abs/1001.4459v1

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

Dhillon, G. and Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. Information Systems Journal, 11 (2), 127-153.

Dhillon, G. and Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. Information Systems Journal, 16 (3), 293-314.

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

European Commission (2011). Privacy and Data Protection Impact Assessment Framework for RFID Applications.

Fishbein, M. and Ajzen, I. (1975). Belief, Atitude, Intention and Behaviour: An Introduction to Theory and Research Addison-Wesley, Reading, MA.

Hevner, A.R., March, S.T., Park, J. and Ram, S. (2004). Design Science in Information Systems Research. MIS Quarterly, 28 (1), 75-105.

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.

Johnston, A.C. and Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. MIS Quarterly, 34 (3), 549-566.

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.

Kowatsch, T. and Maass, W. (2011). The Internet of Things Initiative (IOT-I) Deliverable 2.2: Initial report on Social Acceptance and Impact Evaluation, FP7 ICT project, contract number: 257565

Kowatsch, T., Maass, W. and Fleisch, E. (2011). The Role of Product Reviews on Mobile Devices for In-store Purchases: Consumers' Usage Intentions, Costs and Store Preferences. International Journal of Internet Marketing and Advertising, 6 (3), 226-243.

Laufer, R.S. and Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. J. Soc. Issues, 33 (3), 22-42.

Lopes, I.M. and de Sá-Soares, F. (2010). Information Systems Security Policies: A Survey in Portugese Public Administration. In Proceedings of the IADIS International Conference Information Systems 2010, Porto, Portugal.

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.

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.

Oetzel, M.C., Spiekermann, S., Grüning, I., Kelter, H. and Mull, S. (2011). Privacy Impact Assessment Guideline for RFID Applications, Bundesamt für Sicherheit in der Informationstechnik.

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

Rust, R.T., Kannan, P.K. and Peng, N. (2002). The Customer Economics of Internet Privacy. Journal of the Academy of Marketing Science, 30 (4), 455-464.

Scipioni, M.P. and Langheinrich, M. (2011). Towards a New Privacy-Aware Location Sharing Platform. Journal of Internet Services and Information Security, 1 (4), 1-12.

Siponen, M. and Vance, A. (2009). Neutralization: New Insight into the Problem of Employee Information Systems Security Policy Violations. MIS Quarterly, 34 (3), 487-502.

Siponen, M.T. and Iivari, J. (2006). 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.

Siponen, M.T. and Willison, R. (2009). Information Security Management Standards: Problems and Solutions. Information & Management, 46 (5), 267-270.

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

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.

Warkentin, M., Johnston, A.C. and Shropshire, J. (2011). The Influence of the Informal Social Learning Environment on Information Privacy Policy Compliance Efficacy and Intention. European Journal of Information Systems, 20 (3), 267-284.

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 A – Survey Instrument

- Print version attached
  **IOT-I_DEL_D2.4_Appendix-SurveyInstrument-Print.pdf**

- LimeSurvey 1.92+ XML survey file attached
  **IOT-I_DEL_D2.4_Appendix-limesurvey_survey.lss**

- queXML survey XML format attached (from Lime Survey 1.92+)
  **IOT-I_DEL_D2.4_Appendix-survey.xml**

# Section 9: Appendix B – Concerns and recommendations

## *9.1 Public Transport Payment Service*

| # | Concern | Recommendation, solution or comment |
|---|---|---|
| 1 | That it is not reliable enough in a way wrong deduction may happen | Having a guarantee that no wrong deduction can happen, and if that case happened the user of the service will be compensated for any loss. |
| 2 | It will end up costing me more than the normal way, for example 2 buses can take me to my work place but each one crosses different route where one of the routes is longer and I may end up paying more to reach the same place just because the route was different! | Calculating cost based on the shortest distance between two points not the crossed zones. |
| 3 | My information may end up hacked or used by other parties. | Having a guarantee that my information won't be used by any party and it is next to impossible to hack it. |
| 4 | track my position where I am | do not store positions, but only zones crossed |
| 5 | stolen credit card data | offer also paying via invoice or manual credit card payment each month |
| 6 | offer to third parties for direct advertisement | do not offer to third parties, do not store personal information with the service (e.g. age, gender etc. => not necessary) |
| 7 | that the data would not be properly anonymized | |
| 8 | increases average cost of public transport | none |
| 9 | less transparent pricing structure | third party services / apps that help to choose lowest fares |
| 10 | fragmentation of / incompatible solutions between transport service providers | standardization |
| 11 | Secured storage of payment info. | Build it over a secure platform. |
| 12 | Easy to subscribe, pay, etc. | Don't ask too may questions, go strait to the point (i.e., paying your ticket). |
| 13 | Use of personal info for spam (or worse). | Gather minimal information about the user and don't use this information for anything else than the service requires. |
| 14 | I do not want to share my personal information | how to guarantee the location privacy of users technically? |
| 15 | I feel that somebody can track me and know where I am | Maybe we can design a privacy-preserving solution. |
| 16 | The benefit I can get from using this service may not be that much to motivate me to compromise my privacy | user motivation maybe be problematic. |
| 17 | Privacy | The public transport company should work with a trustfully payment company |
| 18 | No trust in a securely payment system | Long time test phase |
| 19 | Bad application, bugs etc. | Work together with Non Profit Company for securing the privacy |
| 20 | don't want to have to interact each time with service when using public transport regularly | once the service is activated, the ticket billing is done without further interaction during the trip |
| 21 | That the correct fee is charged | provide up-to-date information on the charges incurred |
| 22 | That the credit card details are safe | use adequate security solutions |
| 23 | There is only one serious concern regarding Public Transport Payment Service and it is related to security mechanism related to my credit card and personal information misuse. | Payment process should be as fast as possible. It is something people would really appreciate and it would most certainly bring service to wider adoption. |
| 24 | my personal information could be made availa- | Payment process should be as fast as possible. It is |

| # | Concern | Recommendation, solution or comment |
|---|---|---|
| | ble to unknown individuals or companies without my knowledge | something people would really appreciate and it would most certainly bring service to wider adoption. |
| 25 | Tracking of individuals | Assure that no credit card data are exchanged, but intermediary data |
| 26 | Security issues during the payment phase | Assure that the information on localisation is only processed by the personal device and not retransmitted to the overall system. |
| 27 | Misuse of the service | Communicate! |
| 28 | On one hand this service is of greater value for (foreign) people using once or unregularly this Public Transport System but they may be reluctant to give all their data for these few travels. On the other way, regular customers may register and give their data, but the service is not so interested for them as they may register for a flat-rate use of the transportation system. | |
| 29 | Tracking my ways, offering adds | |
| 30 | Data security is still a huge problem, so misuse is not excludable at all - it will never be, unless this service is really expensive | |
| 31 | This system exists in a similar way in South Korea - you buy a so called t-money card charge it with a certain amount, then check in and out stations calculate the costs... it is easy, small and fast | |
| 32 | If I go traveling I might not want to use my phone, I don't think it is a good idea to integrate all kind of services in a phone | |
| 33 | However in the end I might use it, depending on the data involved in that process | |
| 34 | If linked to credit cards, hacker will try to get in. It should be linked to the phone bill instead | This exists in North Belgium (using SMS I believe), see delijn.be. They said to have sold 50000 tickets in one month! This is cheaper than buying a ticket on the bus! |
| 35 | Accountability is potentially a problem if there are not specific day/monthly statements about usage and price | |
| 36 | Security concerns | Each user should get a "dummy" account that is connected to ones real profile (the way PayPal functions) |
| 37 | Misuse of the data I generate as a user | |
| 38 | Misuse of personal information by companies, | Implementing such a kind of service independent of using a mobile phone or a credit card (paying in advance, ticket scanned when entering public transport, uploading simply possible) |
| 39 | Chance to find out when I leave home and using this information for criminal reasons (breaking in my house) | |
| 40 | Selling of data to marketing enterprises | |
| 41 | Credit card details hacked | Data at rest and in transit needs encryption |
| 42 | Data supplied provided leaked to third parties | Appropriate policies in place to safeguard data (beyond statutory) |
| 43 | Cost of service | Service should be free charged as txp fee from payment provider to public transport service passed through to customer |
| 44 | Service fees are too high | Service fees should not be more than 10 per cent of the ticket fees |
| 45 | To complicated services for the elderly | Ease of use should be high, maybe on demand support |
| 46 | Observation by third-party organizations and other people | It should be an anonymized system without individual identification (maybe with the help of a pre-paid credit card) |

## 9.2 Navigation Service

| # | Concern | Recommendation, solution or comment |
|---|---|---|
| 1 | Hacking attacks leading to denial-of-service, waste of times, jokes being played, ... | Definitely improve the legal framework to enable providing such a service, but also ensuring privacy |
| 2 | Government agencies misusing the information, especially in countries which have no democratic and/or independent jurisdiction | Improve technology to help securing the services and the privacy of the data |
| 3 | Trust | Improve trust in such services |
| 4 | There is no need to collect so much personal data to provide such kind of a service | I think the service as such with the integration of sensors and other systems like weather or traffic jam reports is good but I don't see any improvement when using personal data. |
| 5 | Interoperability between different providers | |
| 6 | Some of these things are already done by navigation software providers e.g. avoiding traffic jams | |
| 7 | Compromising data | Apply HQ data-security mechanisms, and review them regularly |
| 8 | Reselling data to advertisers | Guarantee that the collected location/personal data is only used to provide this navigation services, and that the Navigation Service does not exploit other (enabling) services based on data that is collected from the users of the service |
| 9 | Privacy | If overviews of the usage of the Navigation Service are generated, obfuscate the origin and destination location. |
| 10 | Misuse of the gathered information for personalized advertisement "services". | The ability of a company to say "no" to an easy additional profit. Not quite likely. |
| 11 | Use of the gathered information to fight or "prevent" crimes or the information to be sold to other companies for evaluation (see http://www.engadget.com/2011/04/27/tomtom-user-data-sold-to-danish-police-used-to-determine-ideal/) | If the government officials request the movement patterns of a large amount of customers, or someone else is willing to pay for them, remember what data protection laws are for. |
| 12 | That the providers of this service will not be able to provide accurate enough information for the trip assistance to be useful. One pool car that is not where it is expected, one missed connection because of circumstances that should have been known, but are not (e.g. a strike) would pretty much destroy the trust in the service (and the willingness to pay larger sums for it) | Be better than my expectations :) |
| 13 | Navigation companies DO SELL DATA, so they are not only providing information because they have to legally but they do this for money. ASK TomTom they have given data to authorities, so they know where they will get most Return of Invest, when they look out for people driving to fast. So it's not a question if I fear somebody will hack there systems... | To include the most important question when I want to travel somewhere: HOW MUCH LUGGAGE DO I HAVE WITH ME. It's nice to get routes that say: You save 10 minutes by walking 2Km instead of using a Taxi or Public transportation. But that might not be true with a lot of luggage. |

| | | |
|---|---|---|
| 14 | I don't see any point why the Navigation company would ask for my Credit Card Details. If they do so, they clearly show they do not worry about the safety of my data. Otherwise they would just use InAppBuys using the infrastructure of already existing "App Stores". Asking to store information on how to get money from me in additional locations is a clear sign how much they "value" the principal of not collecting more information than required for their service | |
| 15 | Privacy | Generate a random identifier for each usage |
| 16 | Misuse of the data through Governmental organisations | Secure that the data after service usage will be used only in aggregated form |
| 17 | Provide the data to 3rd Party | Secure that die data is deleted after the service usage |
| 18 | Effectiveness in situation | Transparency |
| 19 | Compliance with company rules | Open standards |
| 20 | Cost | See tomtom go live or kindle concept -> connectivity via cellular networks transparent for user (he doesn't need cellular contract) |
| 21 | Connectivity in buildings, subway tubes or due to roaming | |
| 22 | Indoor navigation | |
| 23 | Check in or luggage time depends on situation on airport | |
| 24 | Taxi is flexible anyway | |
| 25 | Service is driven be timetables already available on the Internet - why should I pay in additional | |
| 26 | Marketing usage of travelling habits in order to improve customer targeting | |
| 27 | Provided information is not misused | Enforce security considerations |
| 28 | Provided personal information is secure | Control accessibility to information shared by the users |
| 29 | Provided service is confident and accurate | Provide service that meets user’s expectations |
| 30 | Price | |
| 31 | Privacy | |
| 32 | Efficiency | |
| 33 | Misuse of personal financial information | Billing via SMS pay service |
| 34 | Misuse of personal information connected with using the service | Using only GPS info for locating connected to a one-time identification nr. for each service use |
| 35 | Misuse of other personal information hold on my smartphone (e.g. hacking) | |
| 36 | Private data being given away | Giving full information on how the data is treated |
| 37 | Location being tracked all the time | Detailed feedback on how the tools used work |
| 38 | External control of what I am doing | Constant information of costumers |
| 39 | The handling of private data | Build up trust in the customer by ensuring safety measures |
| 40 | The possibility that private data gets into the wrong hands | |
| 41 | Misuse of private data | |
| 42 | Selling the data to third party | |
| 43 | Misuse of information | Such system should require personal information on a very low level. |
| 44 | Sale of information | |
| 45 | Same as for GPS and W-LAN tracking of cell phones: third-parties gain profiles of movement | Strict privacy policy, only absolutely necessary data collected, "switch off" possible also for parts of the way, delete information timely afterwards |
| 46 | Complete transparency needed on my personnel abilities/preferences of mobility for the service to choose best multi-modal transport routes (car sharing, walking, train,...) | Same (only necessary information asked, forget by default, etc.) |

| | | |
|---|---|---|
| 47 | Number of interfaces required (with mobility providers, railway system, etc.) seems to increase vulnerability for hacking | Clearly inform about exchange of information ("System will now connect to the following external provider: Allow/Cancel") |
| 48 | The service is able to identify me while routing, knows my current location and my goal | Use of pseudonymization |
| 49 | Data sources are unreliable and lead to malfunction of service. Today's example: TMC service often unreliable due to old data sets | Quality check of data sources, combination of sources |
| 50 | Tracking where I were | Why Navigation Service needs personal data? |
| 51 | Service provider sold my personal data (e.g. which shops I visited) to other companies (e.g. advertising agencies) | Maybe the service should be provided in an "anonymous mode" |
| 52 | Somebody (e.g. hacker) will have information, where I am in this moment | |

## *9.3 Smart Energy Service*

| # | Concern | Recommendation, solution or comment |
|---|---|---|
| 1 | Cost | One time purchase |
| 2 | Privacy | Specific payment way (on the electricity operator bill maybe?) |
| 3 | Efficiency (proven) | I want to know BEFORE what I will gain ... proven statistics? |
| 4 | Interoperability | I don't want to buy another device if something changes (operator, new device) |
| 5 | Security, reliability. | Secure external (remote) access to the system settings. |
| 6 | Would prefer fees based on savings. | |
| 7 | That it wouldn't work as promised - that the service would in fact not select the best option | Be able to see all the time the criteria used for selection so I can verify them |
| 8 | That my data would be hacked | Don't use credit cards and the company should take responsibility if something went wrong |
| 9 | That my data would be sold to advertisers | Tough one... |
| 10 | I feel like I don't have privacy and my life has been watched by some machine (sensor) and recorded somewhere else. It's similar to put a video camera at my home. Someday, someone would reach this information without my permission. | The sensors are stupid, just like the sensor of the automatic door in the shopping mall or elevator. They are not intelligent enough to threaten my private life. |
| 11 | The system would know my habit and this information could be misused by someone. He could break into my house if he knows at which time I am not at home, like a burglar would do by watching my house. | No information should be saved or available by any one. The utility company should only know how much energy I have consumed in order to charge me, just like now how they do it. |
| 12 | This service could make my living condition better, but not necessary. I don't find my life so inconvenient that I have to pay in order to use this service. | Make it as a new feature of service provided by the utility company. Explain to me how this service can save energy so that I will gain both on the convenience of living and saving of heating or electricity. That would make me consider paying for this kind of service. |
| 13 | Could be too complex | Make it easy and clear in use |
| 14 | Loose of direct control | Provide usable control interface and give information about decisions and information the service took/used. e.g. switched of heating because of high prices and your personal information. let the user define the grade of automation and of information use. |
| 15 | Paying for nothing | Tell me a reason why I should need it. I´m just interested, it´s not my need to use it. |
| 16 | Accuracy of the service | |
| 17 | Reliability | |
| 18 | Efficiency | |
| 19 | Privacy | State legislation |
| 20 | Reliability of soft and hardware | Industry standards |
| 21 | Transparency of operations | Service support |
| 22 | High price | Promotional period for using the service |
| 23 | Abuse | High level of data protection |
| 24 | Costs | Low costs |
| 25 | Time | Barrier free |
| 26 | Control | No external control |
| 27 | Respectable | |
| 28 | Ecologically beneficial | |
| 29 | To pay too high prices | If other competitors exist, prices and company services compare with other |

| | | |
|---|---|---|
| 30 | To pass too much information for a third person | Compare working methods over a longer period |
| 31 | That the service is not working efficiently enough | Compare billings over a longer period |
| 32 | Misuse of personal information | Elaborated data protection laws and an independent commission controlling the use of information |
| 33 | Lack of transparency of the function of the Smart Energy Service (e.g. when does it change the provider and to which condition) | Full overview and control of the functions of this system |
| 34 | Promised efficiency and savings of the systems are not as big as expected | Full overview and control of the functions of this system |
| 35 | It does not show the real consumption | Visibility of the system. The user should see (see is more than simply know or trust) what is going on: what data are taken and how they are computed, feedback on user actions and tinkering with the system to find personalized optimal situations |
| 36 | It will start advertising home appliances that want to be pushed on me | I would like not to reply on a 'expert' if something goes wrong or need to be repaired or adjusted... if you need an expert, then a visible and transparent system would make it visible what the expert do to repair, fix or maintain it |
| 37 | That it would ended up costing more than what I have today | |
| 38 | An individual usage profile may be used for a robbery | Secure and encrypted communication channels |
| 39 | Security | More research and pilot projects |
| 40 | Practical implementation related issues | |
| 41 | It will work only in urban areas about 25 km from Torino (Fiat car town!) there is wideband interest | Legislation and rules for service providers |
| 42 | Most of the people in the country side rely on wood stove for heating and sometimes for warm water | Regulate the use of wood (highly polluting the environment |
| 43 | A lot of people in Italy are using photovoltaic power | There should be the option to sell its own photovoltaic generated power managed appropriately as a choice |
| 44 | It is a system that does not considers Life Cycle assessment how much will cost the system (also at the level of a single user) in environmental terms? Do we really spare the societal and environmental costs? | Government shall subsidize renewable provider exploiting renewable resources |

## *9.4 Healthcare Monitoring Service*

| # | Concern | Recommendation, solution or comment |
|---|---|---|
| 1 | False alerts (pos and neg) | Integration into existing Telecare systems |
| 2 | Misuse of data to reject service ("the doctor has told you to stay in bed and the emergency happened in the garden, so we are sorry we cannot pay for the medical treatment") | Transparency in data handling |
| 3 | Sensor data not reliable | Operation by neutral clearing house |
| 4 | Sensors are limiting my freedom of move | |
| 5 | Misuse by provider / third party | Strong incentive for provider to avoid misuse |
| 6 | False Positives / Negatives / Failure | Technological maturity |
| 7 | Lack of legal framework to handle privacy violations | Legal framework |
| 8 | Misuse of personal information | No cameras |
| 9 | Breakdown of service | Encrypted data exchange |
| 10 | Being part of a peep show | Small devices that are hard to identify as monitoring service by others |
| 11 | Data abuse | High privacy guidelines (e.g. German data protection laws); high fines in case of misuse |
| 12 | Two costly in relation to usage | Provide realistic payment plans |
| 13 | Too vulnerable to technical issues / high maintenance | Use simple devices which are made for extensive / outdoor usage |
| 14 | That my data is not safe and could be used against me | The system shall be provided by an independent and certified organization and I should be able to check my stored data at any time |
| 15 | That I feel controlled/monitored in my home | I want to know how my data is evaluated |
| 16 | Data security | |
| 17 | Misuse | |
| 18 | Privacy | |
| 19 | Privacy of the personal information. | Privacy of the personal information should be somehow guarantied. Maybe the access to this information should be limited to the small number of people and / or systems. |
| 20 | Concern that my private health data could be sold to the health marketing agencies. | Private health data should be separated from the information of the owner of that data. In that way health data could be used only for statistics. |
| 21 | Maybe if you trust this Healthcare Monitoring Service to much you want go the doctor even if you are not feeling well. And the situation could become more serious. | Users of this system should be trained and informed what this system could measure and when a person would be better to go to the doctor. |
| 22 | Misuse of my personal data | |
| 23 | General understanding in society that underestimates the dangers with regard to making such critical personal data available for such a system | |
| 24 | Data on vital parameter may not cover sufficiently all aspects on my personal health condition. | It should be possible to adapt parameter if applicable |
| 25 | Malfunction and misinterpreted emergency situations may occur | Re-confirm on the actual situation by redundant communication |
| 26 | HMS being a stand-alone service - need for additional devices to allow for other needs (orientation / medication-reminder, etc.) | All-in-one device |
| 27 | That it would make no actual difference to the outcome of a condition. | Ban data sharing |
| 28 | Data Privacy | Make Data a "property" whose ownership always belongs to the data subject. The taking of data become a "theft" with criminal not just regulatory consequences. The trade in data becomes a crime. |

| | | |
|---|---|---|
| 29 | Subjected to Automated decision-making. | Data can be used for one purpose only. The data physically destroyed after use. No long data retention policies. |
| 30 | Increased Cost family members who are genetically related. Due to data sharing and data analytics. | Decision-making is left as a function between humans not between devices and IT systems. |
| 31 | Decision-making is left as a function between humans not between devices and IT systems. | Loss of human monitoring, human intervention and human sympathy. |
| 32 | Privacy issues | Improve security measures |
| 33 | False positive alarm | To require some user interaction in case of alarm. E.g. "Are you okay?" -> if no response in 5 seconds, the alarm is triggered. |
| 34 | Stigma | The hardware should be unnoticeable in everyday situations. |
| 35 | Location tracking and logging | Location information should only be transmitted in case of emergency. |