Summer 7-19-2017

Explaining Adoption of Pervasive Retail Systems with a Model based on UTAUT2 and the Extended Privacy Calculus

Alexander Weinhard
University of Würzburg, alexander.weinhard@uni-wuerzburg.de

Matthias Hauser
University of Würzburg, matthias.hauser@uni-wuerzburg.de

Frédéric Thiesse
University of Würzburg, frederic.thiesse@uni-wuerzburg.de

Explaining Adoption of Pervasive Retail Systems with a Model based on UTAUT2 and the Extended Privacy Calculus

Completed Research Paper

Alexander Weinhard
University of Würzburg
Josef-Stangl-Platz 2
97070 Würzburg, Germany
alexander.weinhard@uni-wuerzburg.de

Matthias Hauser
University of Würzburg
Josef-Stangl-Platz 2
97070 Würzburg, Germany
matthias.hauser@uni-wuerzburg.de

Frédéric Thiesse
University of Würzburg
Josef-Stangl-Platz 2
97070 Würzburg, Germany
frederic.thiesse@uni-wuerzburg.de

Abstract

The advent of e-commerce puts traditional retail companies under a lot of pressure. A way retailers try to attract more customers to their physical stores is by offering online services on the retail sales floor. Such services are enabled through pervasive retail systems. These systems, however, do not only offer new opportunities but also bear risks for retailers because they heavily depend on privacy-related data, which customers could perceive as a potential privacy threat. In the present paper, we thus investigate the antecedents of customers' usage intention towards such systems and the trade-off between the perceived benefits and the perceived privacy costs that are associated with their use. To this end, we propose a model based on the most recent version of the Unified Theory of Acceptance and Use of Technology (UTAUT2) and the Extended Privacy Calculus Theory. We validate our model considering a smart fitting room application and show that the model is able to explain 67.1% of the variance in the behavioral intention to use the system and 43.1% of the variance in a person's willingness to disclose private information. Our results can be leveraged to design pervasive systems that are perceived as valuable instead of privacy threatening.

Keywords: Internet of Things, Technology Acceptance, Privacy Calculus, Pervasive Retail System, Radio Frequency Identification

Introduction

The advent of e-commerce has changed the retail landscape dramatically and puts traditional retail companies under a lot of pressure. Although customers still visit retail stores to see, touch and feel products, they often end up purchasing products online (MacKenzie et al. 2013; PwC 2015). According to a recent customer survey (PwC 2015), most customers prefer shopping online because of lower prices and the possibility to shop 24 hours a day, 7 days a week without the need to go to a physical store. The survey, however, also reveals that many customers decide against offline retail because their online counterparts provide better services (e.g., product reviews and product recommendations). In consequence, Vend (2016) expects so-called offline pure plays (i.e., retailers that only sell their products offline) to disappear. This, however, does not imply that retail stores will disappear completely in the near future. In contrast, recent studies suggest that companies with an online shop and physical retail stores have competitive advantage against pure online and offline players as long as they integrate their online and offline businesses (Herhausen et al. 2015).

Pervasive computing systems (also referred to as ubiquitous computing systems) offer great opportunities for the integration of online and offline businesses (Gregory 2015). Mark Weiser (1991), former chief technology officer of Xerox, describes the vision of such systems with the following words: “The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it.” Pervasive computing systems describe environments saturated with computing and communication capability that support human users (Satyanarayanan 2001). The objective thus is to make the lives of their users “simpler through digital environments that are sensitive, adaptive, and responsive to human needs” (Saha and Mukherjee 2003). In the present paper, we focus on pervasive computing systems in retail environments which we in accordance with Kourouthanassis et al. (2007) in the following refer to as *pervasive retail systems*. Examples of such systems are shopping carts that navigate customers through shopping isles (Kourouthanassis and Roussos 2003), shelves that provide additional information on items (Parada et al. 2015), and fitting rooms that offer for example product recommendations based on the garments brought into them (Hauser et al. 2017). Such systems allow retailers to provide services from their online shops on the retail sales floor, which promises enhanced customer experience. In addition, the systems generate valuable customer data such as customer walking paths through the store which a retailer could, for example, use to improve store layouts (Gregory 2015).

The collection of customer data, however, does not only offer new opportunities for retailers but also bears the risk of being perceived as a privacy threat by customers. Introductions of new technology in retail environments in the past have shown that not sufficiently considering privacy concerns can have severe consequences for retailers. When retailers in North America and Europe started to roll out radio frequency identification (RFID) technology in the early 2000s a public debate started on the potential misuse of the data that could be collected with that technology (Thiesse 2007). The Metro Group, for example, had to face a demonstration in front of its *Metro Future Store* and was given the infamous *Big Brother Award* after introducing an RFID-based loyalty card (Albrecht and McIntyre 2005). As a consequence, legislative bodies had to cope with the fears of the public and introduced new legislation to mitigate potential privacy threats through pervasive technology (Lockton and Rosenberg 2005). In the present paper, we therefore investigate the trade-off between customers’ perceived benefits and their perceived privacy concerns towards pervasive retail systems. To this end, we propose a model that integrates Venkatesh et al.’s (2012) Unified Theory of Acceptance and Use of Technology 2 (UTAUT2) with Dinev and Hart’s (2006) Extended Privacy Calculus Theory. The purpose of our study is to gain a better understanding of retail customers’ usage intentions towards pervasive retail systems and their underlying privacy disclosure behavior. To achieve this, we first determine the antecedents of people’s usage intentions towards pervasive retail systems. Here, we particularly focus on people’s willingness to provide personal information, which reflects the trade-off between the costs of disclosing private information and the perceived benefits of using a pervasive retail system. In a second step, we determine the antecedents of people’s information disclosure behavior. We validate the applicability of our research model considering an RFID-based *smart* fitting room. This application detects garments within cabins and uses privacy-related data (e.g., customer identity, purchase history) to offer additional personalized services such as product recommendations.

Related Work

Research on the adoption of pervasive systems that incorporates privacy aspects can be roughly categorized into (i) studies that investigate people’s information disclosure behavior and its influence on the adoption of pervasive systems and (ii) studies that use technology acceptance models in combination with privacy constructs.

The first group of studies uses privacy calculus models to identify privacy related determinants of people’s adoption behaviors towards pervasive systems. Xu et al. (2009) investigate people’s privacy concerns towards location-based services. Their model explains 40.2% of the variance of people’s intentions to disclose personal information but does not investigate the intention to use the service. Similarly, Zhao et al. (2012) build a privacy calculus model in order to investigate factors that lead users of location-based social networks to disclose location-related information. The authors are able to determine several privacy related factors that explain 41.7% of the variance in peoples’ information disclosure intention. In contrast, Li et al. (2016) focus on the intention to use pervasive systems. The authors investigate the adoption of wearable healthcare devices and develop a model that explains 15% of the variance in the intention to use them. Because of the low explanatory power of their model, Li et al. (2016) propose to use additional constructs from technology acceptance models in further research.

The second group of studies uses different technology acceptance models and extends them with privacy constructs. Cazier et al. (2008), Müller-Seitz et al. (2009), and Kowatsch and Maass (2012) extend the Technology Acceptance Model (TAM) from (Davis 1989). The first two studies investigate the adoption intention towards the auto-id technology RFID. The first study introduces the constructs *privacy risk likelihood* and *privacy risk harm;* the second study the construct *security concerns*. The results of both studies indicate that the privacy constructs have an influence on people's adoption intentions towards RFID technology. To the best of our knowledge, Kowatsch and Maass (2012) are the only group of authors that not only add additional constructs but combine the TAM model with the Extended Privacy Calculus Theory. They consider people's usage intentions towards four IoT-based services (e.g., healthcare monitoring services). Although the idea of the study is very interesting, the results are questionable because they test each of their hypothesis with only 23 completed questionnaires.

Similarly to the studies that extend the TAM, Gao et al. (2015), Nysveen and Pedersen (2016), and Zhou (2012) extend the more recent technology acceptance models UTAUT and UTAUT2. In contrast to the studies that extend the TAM, none of the studies fully integrates the privacy calculus theory. Instead, they all consider additional privacy constructs from different sources. Gao et al. (2015) refer to the privacy calculus theory but only consider the construct *privacy risk*. Nysveen and Pedersen (2016) use the construct *privacy risk harm*, and finally Zhou (2012) the constructs *privacy concerns*, *trust* and *perceived risk*. Gao et al. (2015) investigate users' adoption behaviors towards wearable healthcare devices and show that the construct privacy risk is one of the most important predictors of the model. Nysveen and Pedersen (2016) consider people's adoption behavior towards RFID-enabled services. In contrast to Gao et al. (2015), they are not able to show any effect of their privacy construct on the intention to use. Zhou (2012) investigates the adoption of location-based services. Similar to Gao et al. (2015), the author finds an effect of privacy risk on the usage intention. In addition, she is able to show an effect of the construct trust, but no relationship between the construct privacy concerns and the usage intention.

Similarly to Kowatsch and Maass (2012), our study integrates the privacy calculus theory with technology acceptance models. We use the Extended Privacy Calculus from Dinev and Hart (2006) because it is a well-accepted theory and covers many important nuances of people's privacy disclosure behavior. In contrast to Kowatsch and Maass (2012), however, we consider the UTAUT2 instead of the TAM, because it was developed to explain the adoption of consumer applications. Venkatesh et al. (2012) show that the UTAUT2 explains up to 74% in the behavioral intention to use a technology and 54% of the variance in the actual use of a technology. As pervasive retail systems fall into the category of consumer applications (Kourouthanassis and Roussos 2003), we expect a better explanation of people's adoption intention towards these systems by integrating the UTAUT2 with the Extended Privacy Calculus.

Research Model

Figure 1 depicts our proposed research model. As mentioned in the last section, we combine the UTAUT2 from Venkatesh et al. (2012) with the Extended Privacy Calculus introduced by Dinev and Hart (2006). We propose to substitute the UTUAT2 construct *price value* with the Extended Privacy Calculus. Whereas the price value captures the trade-off between the perceived monetary costs and the perceived benefits of using a technology, the Extended Privacy Calculus captures the trade-off between the perceived costs of disclosing private information and the perceived benefits of using a technology.

UTAUT2 Constructs

We use five of the UTUAT2's nine constructs in our model, namely *performance expectancy (PE), effort expectancy (EE), social influence (SI), hedonic motivation (HM)* and *behavioral intention (BI).*

Besides the price value construct, which we substitute with the Extended Privacy Calculus, we exclude three more of the UTAUT2's original constructs. We first do not consider the actual use of pervasive retail systems as the implementation of such systems is still at the very beginning. Following Salinas Segura and Thiesse (2015), we furthermore exclude the construct *habit* because it would require customers to have experience with pervasive retail systems. In addition, we exclude the construct *facilitating conditions* because some of the underlying questions are not suited for pervasive retail systems. Customers do, for example, not need particular resources to use them because they are implemented in retail stores and can be used without purchasing them first (see question FC1 in Venkatesh et al. (2012)). In addition, the technology is new and it is thus not obvious for customers how it is compatible with other technologies they use (see question FC3 in Venkatesh et al. (2012)).

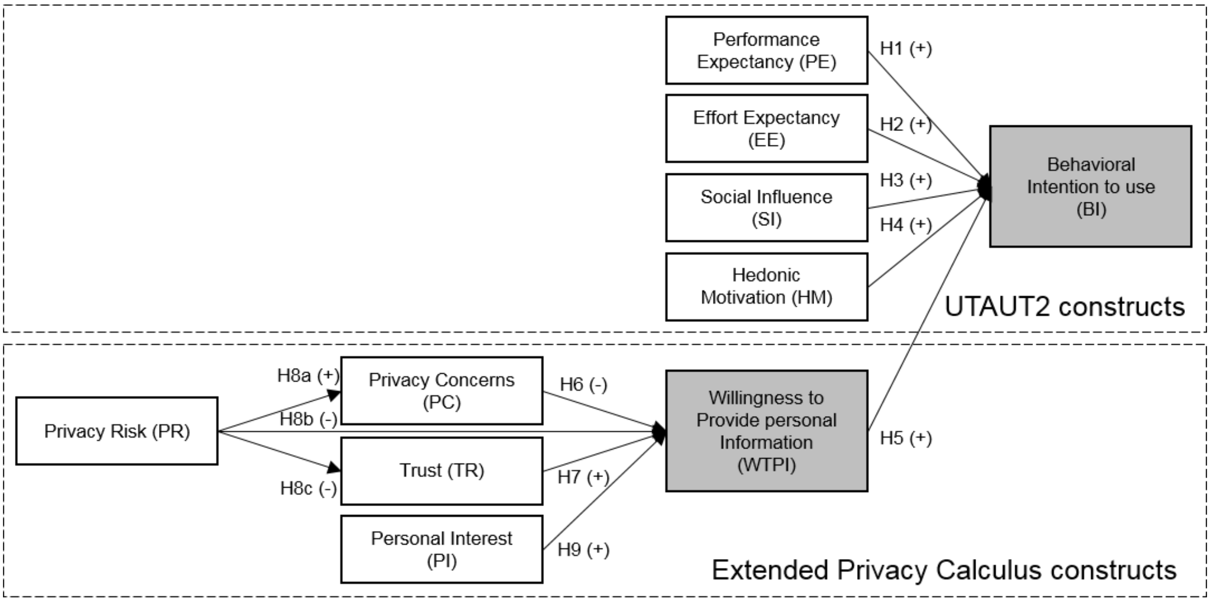

Figure 1 Research model and hypothesized relationships between the constructs

The first construct we incorporate is performance expectancy, which describes how much a technology user expects to improve the performance of a process through the use of a technology (Venkatesh et al. 2003). The idea of pervasive retail systems is to provide customers with features that aim at improving their shopping experience. In a smart fitting room, for example, users automatically receive personalized recommendations based on their current garment selection and their purchase history, which enables them to make better decisions in less time. We thus formulate the following hypothesis:

H1: PE has a positive effect on the behavioral intention to use a pervasive retail system.

Effort expectancy is “the degree of ease associated with consumers’ use of technology” (Venkatesh et al. 2012) and is thus positively related to BI. Obviously, if customers perceive the usage of pervasive technologies as intuitive they will be more likely to use them. Thus, we hypothesize:

H2: EE has a positive effect on the behavioral intention to use a pervasive retail system.

Social influence describes to what extent others influence one’s decision to use a technology (Venkatesh et al. 2003). *Others* are in our case people who are important to a retail customer (e.g., friends and family). Various studies examine the impact of the variable social influence on a person’s behavioral intention to use a technology. Studies validated this relationship empirically for the adoption of smart kiosks (Chiu et al. 2010), mobile payment solutions (Oliveira et al. 2016), and RFID-based applications in the healthcare sector (Chong et al. 2015). Consequently, we formulate the following hypothesis:

H3: SI has a positive effect on the behavioral intention to use a pervasive retail system.

Hedonic motivation denotes the pleasure of using a novel technology. According to Venkatesh et al. (2012), it is one of the most important factors in predicting a consumer’s intention to use a technology. Consequently, we assume that people who generally enjoy using novel technologies will be more likely to use a pervasive system and formulate the hypothesis as follows:

H4: HM has a positive effect on the behavioral intention to use a pervasive retail system.

Extended Privacy Calculus Constructs

As mentioned before, the use of pervasive retail systems is free of monetary charge. We thus exclude the price value construct from the UTAUT2. However, we argue that even though customers will not have to pay money for using the systems, they will be “charged” by having to disclose private information. Venkatesh et al. (2012) define the term price value as “consumers’ cognitive trade-off between the perceived benefits of the applications and the monetary cost for using them”. To capture the “costs of privacy”, i.e. the tradeoff between the perceived benefits and the perceived potential drawbacks of private information disclosure, we thus propose to replace the price value with the Extended Privacy Calculus Model. We therefore redefine the term price value as the cognitive tradeoff between the perceived benefits of using a pervasive retail system and the privacy related costs. To this end, we carefully adapted the proposed constructs of the Extended Privacy Calculus from Dinev and

Hart (2006) and also considered the study of Kowatsch and Maass (2012) who adapted Dinev and Hart's questions to the realm of IoT. The first construct we include in our model is the *willingness to provide personal information* (WTPI) which refers to a person's willingness to disclose private information to use all functionality of a pervasive application (Kowatsch and Maass 2012). As we assume that people would only be willing to disclose information if they intend to use the system, we hypothesize:

H5: WTPI has a positive effect on the behavioral intention to use that application.

The construct *privacy concerns against a pervasive retail system* (PC) reflects the concern of an opportunistic behavior related to the provided information by the user (Kowatsch and Maass 2012). According to Dinev and Hart (2006), privacy concerns are in accordance with the expectancy theory from Vroom (1964). Consequently, people should try to minimize negative consequences of their information disclosure behavior. We formulate the following hypothesis:

H6: PC has a negative effect on a person's willingness to provide personal information.

The construct *trust (TR) towards the party that provides a pervasive application* denotes people's belief that their private information will be handled secure, safe and in a competent way. Even though trust perception can be seen as the opposite of risk perception – which we also included in our model – this construct captures a different notion (Kowatsch and Maass 2012). For example, a customer can trust a retailer that provides a smart fitting room application and – at the same time – be aware that providing private information to use the application can bear some risks. Consequently, we hypothesize:

H7: TR has a positive effect on a person's willingness to provide personal information.

Perceived privacy risk (PR) describes the general perceived risk related to the disclosure of personal information (Kowatsch and Maass 2012). According to Dinev and Hart (2006) such risk includes the sale of private information to third parties or sharing of private information with third parties. This construct also reflects the misuse of personal information such as unauthorized access to the data or data theft. We consequently formulate the following three hypothesis:

H8a: PR has a positive effect on the perceived privacy concerns against using a pervasive shopping application.

H8b: PR has a negative effect on a person's willingness to provide personal information.

H8c: PR has a negative effect on the trust in the party providing the application.

The construct *personal interest in a pervasive retail application* (PI) reflects a person's degree of intrinsic motivation which overrides privacy concerns in order to use such an application (Kowatsch and Maass 2012). In contrast to the construct hedonic motivation from the UTAUT2, this construct measures the degree to which the cognitive attraction to a pervasive retail system overrides privacy concerns. Consequently, we formulate the following hypothesis:

H9: PI has a positive effect on a person's willingness to provide personal information.

Research Method

To validate our model we consider a smart fitting room application. The system recognizes the customers' garment selections based on RFID technology and provides suitable recommendations if customers identify themselves and allow the system to access their purchase history. In addition, the application offers the option of home delivery of chosen garments if the customer provides address and financial data to the system. The application that we consider in our study is based on a prototype that we are currently implementing on the retail sales floor at a leading German retailer.

Instrument Development and Data Collection

We conducted an online survey with students from a German university. We choose to target students because young people are the target group that the retailer in our study wants to attract to its stores with the pervasive retail system. As an incentive to participate, students had the chance to win one out of five book vouchers worth 20€ each. In the survey, we described the use case and its functionalities with pictures depicting the real world prototype (e.g., the user interface). We also informed the survey participants that they would have to identify themselves and share address as well as financial data in order to use the described fitting room functionalities. We carefully adapted the questions for the constructs we described above (see Appendix) and the answers using a seven point Likert scale. In total, 280 students participated in the survey. Our sample consists of 151 female and 129 male students with an average age of 23.2 years. The standard deviation is 3.5 years.

Data Preparation

As online surveys yield higher risks of careless responding due to unmotivated or inattentive respondents than pen and paper based versions (Huang et al. 2012), we conducted a structured data screening process.

We use the methods (i) screening for unusually short response times and (ii) screening for patterns to identify inattentive respondents. The first method assumes that participants who carelessly fill out a questionnaire are more likely to rush through it (Meade and Craig 2012). Based on preliminary tests, we assume that respondents who are familiar with pervasive systems and are fast readers would need at least four and a half minutes for completing the questionnaire.

The second method searches for unusual patterns in the data by using the long string method proposed by Johnson (2005). The author proposes to eliminate answers with an unusual number of consecutive repetitions of the same kind of answer (e.g., ten times the answer "very likely" in a row). We computed the long strings for each participant and removed completed questionnaires of participants with ten or more consecutive answers of the same type. Four of the participants that we identified with this method also fell under the previously defined response time cut-off. The times that it took the rest of the suspicious respondents to answer the questionnaires were also very close to this predefined cutoff.

Overall, the data cleaning process lead to a removal of 28 respondents, which were suspect to inattentive and unmotivated answering. These are exactly 10% of the respondents which is in correspondence with reports from other studies with student samples (see e.g. Kurtz and Parrish (2001)).

Results

Henseler et al. (2009) state that partial least squares (PLS) “path modeling is recommended in an early stage of theoretical development to test and validate exploratory models.” We aim at introducing a new theory and thus use PLS for the analysis of our theoretical model. Following Chin (2010), we present our results by first reporting the reliability and validity of the used item measures and then present the evaluation results of the structural model. We used SmartPLS Version 3.2.6. to conduct the analysis.

Model Reliability and Validity

Our latent variables show good reliability. Except from questionnaire item HM3, all items have outer loadings above the proposed value of 0.708 (Henseler et al. 2009). With an outer loading of 0.674, however, HM3 is only slightly below 0.708 and we thus did not exclude it from our analysis.

Table 1 reports the Cronbach’s Alpha, Composite Reliability and Average Variance Extracted (AVE) of each construct and shows the internal consistency of our model. All constructs have a Cronbach’s Alpha value higher than 0.7 and thus display convergent validity (Garson 2016). Furthermore, they all show a composite reliability greater than the cutoff of 0.8 which is considered good for confirmatory research (Daskalakis and Mantas 2008) and clearly above the proposed threshold of 0.7 that literature considers good for explanatory purposes (Hair et al. 2012). In addition, the AVE of all constructs is higher than the proposed threshold of 0.5 (Chin 1998) which means that the error variance does not exceed the explained variance (Garson 2016).

Table 1 Construct reliability and validity

	Cronbach's Alpha	Composite Reliability	AVE
BI	0.919	0.948	0.860
EE	0.882	0.915	0.731
HM	0.820	0.889	0.732
PC	0.916	0.941	0.800
PE	0.720	0.843	0.642
PI	0.807	0.886	0.721
PR	0.874	0.909	0.669
SI	0.878	0.925	0.803
TR	0.755	0.859	0.670
WTPI	0.859	0.914	0.781

We use the Heterotrait-Monotrait (HTMT) ratio for analyzing the discriminant validity of our model because Henseler et al. (2015) lately showed its superiority over the Fornell and Larcker criterion (Fornell and Larcker 1981). Table 2 shows that all HTMT ratios are below the strict cutoff value of 0.85 proposed by Kline (2015) which indicates good discriminant validity.

Table 2 Heterotrait-Monotrait ratios

	BI	**EE**	**HM**	**PC**	**PE**	**PI**	**PR**	**SI**	**TR**	**WTPI**
BI	1									
EE	0.286	1								
HM	0.774	0.302	1							
PC	0.301	0.127	0.154	1						
PE	0.796	0.382	0.845	0.104	1					
PI	0.722	0.242	0.633	0.209	0.570	1				
PR	0.332	0.115	0.199	0.828	0.133	0.220	1			
SI	0.570	0.204	0.557	0.072	0.691	0.406	0.126	1		
TR	0.558	0.184	0.437	0.279	0.387	0.559	0.376	0.400	1	
WTPI	0.711	0.180	0.507	0.358	0.502	0.692	0.309	0.367	0.614	1

The overall model fit is estimated with the Standardized Root Mean Square Residual (SRMR), which measures the difference between the observed correlation matrix and the model-implied correlation matrix. Our model shows an SRMR of 0.096 which indicates a good fit according to Garson (2016).

Structural Model

We determine the effect size f-squared of each variable with the following formula (Hair et al. 2014):

$$f^2 = \frac{R^2 included - R^2 excluded}{1 - R^2 included}$$

In order to calculate f^2 for each construct, we first calculate the R^2 of the full model (R^2_{included}). In a second step, we calculate R^2_{excluded} for each construct, which is the R^2 of the model without the construct currently under consideration. Effect sizes are considered small if they are above 0.02, medium if they are above 0.15 and large if they are above 0.35 (Cohen 1988). Furthermore, "if an exogenous construct strongly contributes to explaining an endogenous construct, the difference between R^2_{included} and R^2_{excluded} will be high, leading to a high f^2 value" (Hair et al. 2014). Table 3 shows the effect sizes of the variables. It reveals that WTPI and HM have the highest influence on BI and PI has the highest influence on WTPI. TR, PC and PR, on the other hand, have only small effects on WTPI. In addition, the table indicates a large influence of PR on PC.

Table 3 Effect sizes of the dependent variables

	Dependent Variable	**f²**	**Effect**
WTPI	BI	0.310	**medium**
HM	BI	0.202	**medium**
PE	BI	0.053	small
SI	BI	0.022	small
EE	BI	0.002	none
PR	PC	1.251	**large**
PR	TR	0.105	small
PI	WTPI	0.264	**medium**
TR	WTPI	0.102	small
PC	WTPI	0.039	small
PR	WTPI	0.003	small

The results of the structural model are presented in Table 4. We use bootstrapping with 5000 samples to determine whether the relations between the constructs are significant and support the stated hypotheses. The table shows that all hypotheses except H2 and H8b are supported. In addition, we calculate the indirect effects of PR on WTPI, considering again bootstrapping and 5000 samples. This results in a path coefficient of -0.251. We then added this value to the direct path coefficient of 0.067, which results in a total effect of -0.184 with a p-value of 0.001.

Table 4 Path coefficients for the structural model

Hypothesis		Path Coefficient	T Statistics	P Values	Supported
H1	**PE -> BI**	0.192	3.392	0.001	**Yes**
H2	**EE -> BI**	0.027	0.691	0.490	No
H3	**SI -> BI**	0.104	2.335	0.020	**Yes**
H4	**HM -> BI**	0.368	6.374	< 0.001	**Yes**
H5	**WTPI -> BI**	0.358	8.633	< 0.001	**Yes**
H6	**PC -> WTPI**	-0.223	3.222	0.001	**Yes**
H7	**TR -> WTPI**	0.275	4.626	< 0.001	**Yes**
H8a	**PR -> PC**	0.745	23.952	< 0.001	**Yes**
H8b	**PR -> WTPI**	0.067	0.837	0.402	No
H8c	**PR -> TR**	-0.309	4.748	< 0.001	**Yes**
H9	**PI -> WTPI**	0.430	7.647	< 0.001	**Yes**

Finally, we analyze the proportion of variance explained by our model. Table 5 shows that the constructs of BI explain 67.1% of its variance. As stated before, WTPI and therefore the result of the privacy calculus is the most important predictor for people's intention to use a pervasive retail system. 43.1% of the variance of WTPI is explained by its predictors, whereby the constructs personal interest and trust account for the biggest portion of people's intention to use a pervasive retail system.

Table 5 Explanatory power of structural model

	Adjusted- R^2	P Values
BI	0.671	< 0.001
WTPI	0.431	< 0.001
PC	0.554	< 0.001
TR	0.092	0.025

Discussion

Our research shows that the construct WTPI from the privacy calculus has a significant influence on the behavioral intention to use a pervasive retail system. The construct accounts for more variance in the behavioral intention than hedonic motivation from the UTAUT2 ($f^2 = 0.310$ against $f^2 = 0.202$). This indicates that people weigh the perceived benefits against the perceived drawbacks of providing personal information before they decide whether they want to use a pervasive retail system.

The most important variables for explaining the willingness to provide personal information are personal interest ($f^2 = 0.264$) and trust towards the institution that provides the application ($f^2 = 0.102$). This result is in accordance with Dinev and Hart's (2006) study, which also found that "the three factors most strongly related to the willingness to provide personal information were [...] privacy concerns, [...] trust, and personal [...] interest."

Our model, however, does not support the relationship between effort expectancy and the behavioral intention to use a pervasive retail system. One explanation could be that people perceive the smart fitting room as a fun application and do thus not perceive the process of learning to use the application as an effort. In consequence, effort does not play a role on their usage intention. Another explanation could be, that our sample comprises only students, which are digital natives and thus familiar with pervasive systems (e.g., smart phones and smart watches). The data revealed that most of them chose high values on the Likert scale for the questions of the construct effort expectancy regardless of their usage intention towards the smart fitting room. Nevertheless, we decided to keep the construct because we think that a survey with a different sample population (i.e., a sample not only comprising digital natives) could show a relationship between effort expectancy and the behavioral intention to use a pervasive retail system. We furthermore did not find support for the direct relationship between perceived privacy risk and the willingness to provide personal information. The model, however, revealed that privacy risk has a significant indirect effect on the willingness to provide personal information, which is in accordance with our expectations.

Conclusion

The present papers investigates customers' adoption intentions towards pervasive retail systems. In contrast to consumer products, customers do not have to purchase the systems to use them. The systems, however, heavily depend on privacy-related data, which customers could perceive as a potential privacy threat. To address this issue, we propose a model that combines the UTAUT2 and the Extended Privacy Calculus.

Our investigation shows that our model is able to explain 67.1% of the variance in people's intention to use a pervasive retail system. We show that people's willingness to provide personal information and the hedonic motivation from the UTAUT2 are the most important determinants of people's usage intention. We are thus able to demonstrate with our empirical investigation that the extended privacy calculus is a valid substitute for the construct price value of the UTAUT2 if the usage of a system does not come with monetary costs but requires disclosing privacy-related data. This implies that providers of such applications have to carefully consider people's privacy perceptions. If people are not willing to disclose necessary privacy-related data, they will not end up using the application even if it offers valuable benefits.

We did not only investigate the predictors of people's usage intention but also the predictors of people's willingness to provide personal information for using a pervasive retail system. Our investigation shows that our model is able to explain 43.1% of their willingness to provide such information. The most important antecedents are the constructs personal interest and trust. We show that the perceived benefits of pervasive retail systems must outweigh the perceived privacy costs so that people are willing to "forget" their privacy concerns (captured by the variable personal interest). If retailers are not able to achieve this, they might risk losing their customers and investing in an application that customers might not use at all. In addition, as trust towards the provider of pervasive retail systems is the second strongest predictor of the willingness to provide personal information, retailers should strive to preserve a good reputation for carefully handling customer data.

There are also some limitations to our research. First, although the student sample is appropriate for this study as young people are the target group of the retail company, the sample characteristics limit the generalizability of the study. Second, we conducted an online experiment and even though we carefully described the application and illustrated its use with meaningful pictures, there is still the possibility that a study with a real prototype would yield differing results. Third, with the smart fitting room application we only considered *one* pervasive retail system to validate our research model.

We see opportunities for further research in various directions. We encourage researchers to use our model for the investigation of people's adoption intention and disclosure behavior towards other privacy related pervasive retail applications. In addition, future research should not only consider usage intention but also actual usage behavior of pervasive applications. Not least, we believe that our proposed model could be used to explain adoption intention and privacy disclosure behavior of applications beyond pervasive retail systems.

Appendix

Questionnaire items translated from the German version that we used for our study.

Item	Statement	Adopted from
PE1	I would find the smart fitting room (SFR) useful when I would go shopping.	Venkatesh et al. (2012)
PE2	Using the SFR would help me to do my apparel shopping more quickly.	Venkatesh et al. (2012)
PE3	Using the SFR would help me to choose garments more easily.	Venkatesh et al. (2012)

EE1	Learning to use the SFR would be easy for me.	Venkatesh et al. (2012)
EE2	My interaction with the SFR would be clear and understandable.	Venkatesh et al. (2012)
EE3	I would find the SFR easy to use.	Venkatesh et al. (2012)
EE4	It is easy for me to become skillful at using the SFR.	Venkatesh et al. (2012)
SI1	People who are important to me would think that I should use the SFR.	Venkatesh et al. (2012)
SI2	People who influence my behavior would think that I should use the SFR.	Venkatesh et al. (2012)
SI3	People whose opinions that I value would prefer that I use the SFR.	Venkatesh et al. (2012)
HM1	Using the SFR would be fun.	Venkatesh et al. (2012)
HM2	Using the SFR would be enjoyable.	Venkatesh et al. (2012)
HM3	Using the SFR would be very entertaining.	Venkatesh et al. (2012)
BI1	I intend to use the SFR in the future.	Venkatesh et al. (2012)
BI2	I will always try to use the SFR when I go shopping.	Venkatesh et al. (2012)
BI3	I plan to use the SFR frequently.	Venkatesh et al. (2012)
PR1	What do you believe is the risk that personal information collected by the SFR could be sold to third parties?	Dinev and Hart (2006)
PR2	What do you believe is the risk that personal information collected by the SFR could be misused?	Dinev and Hart (2006)
PR3	What do you believe is the risk that personal information collected by the SFR could be made available to unknown individuals or companies without your knowledge?	Dinev and Hart (2006)
PR4	What do you believe is the risk that personal information collected by the SFR could be made available to government agencies?	Dinev and Hart (2006)
PR5	What do you believe is the risk that personal information collected by the SFR could be jeopardized by hacking activities?	Kowatsch and Maass (2012)
PC1	I am concerned that personal information collected by the SFR could be misused.	Dinev and Hart (2006)
PC2	I am concerned that a person or an agency can find private information about me when I would use the SFR.	Dinev and Hart (2006)
PC3	I am concerned about the information collected by the SFR because of what others might do with it.	Dinev and Hart (2006)
PC4	I am concerned about the information collected by the SFR because it could be used in a way I did not foresee.	Dinev and Hart (2006)
TR1	Retailers would provide the SFR in a safe way such that information can be exchanged electronically	Dinev and Hart (2006) / Kowatsch and Maass (2012)
TR2	Retailers would provide the SFR in a reliable way such that transactions can be conducted	Dinev and Hart (2006)
TR3	Retailers that provide the SFR, would handle personal information in a competent fashion.	Dinev and Hart (2006)
PI1	I find that my personal interest in the SFR would override my privacy concerns.	Dinev and Hart (2006)
PI2	The greater my interest in the SFR would be, the more I would tend to suppress my privacy concerns.	Dinev and Hart (2006)
PI3	In general, my need for the SFR would be greater than my concern about privacy.	Dinev and Hart (2006)
WTPI1	I would provide accurate and identifiable personal information for ordering products with the SFR.	Dinev and Hart (2006)
WTPI2	I would identify myself with a customer id card in order to receive personal product recommendations.	Dinev and Hart (2006) / Kowatsch and Maass (2012)
WTPI3	I would provide accurate information about myself in order to use all functionality of the SFR.	Dinev and Hart (2006) / Kowatsch and Maass (2012)

Acknowledgements

This research was carried out under the Research Project SERAMIS (Sensor-Enabled Real-World Awareness for Management Information Systems), funded by the EU under the VII Framework Research Program.

The authors would like to thank Anja Krautmacher and Andreas Ballauf.

References

Albrecht, K., and McIntyre, L. 2005. *Spychips: How major corporations and government plan to track your every move with RFID*, Nashville: Nelson Current.

Cazier, J. A., Jensen, A. S., and Dave, D. S. 2008. "The Impact of Consumer Perceptions of Information Privacy and Security Risks on the Adoption of Residual RFID Technologies," *Communications of the Association for Information Systems*, (23).

Chin, W. W. 1998. "The partial least squares approach to structural equation modeling," *Modern methods for business research*, (295:2), pp. 295–336.

Chin, W. W. 2010. "How to write up and report PLS analyses," in *Handbook of partial least squares*, Springer, pp. 655–690.

Cohen, J. 1988. "Statistical power analysis for the behavioral sciences Lawrence Earlbaum Associates," *Hillsdale, NJ*, pp. 20–26.

Daskalakis, S., and Mantas, J. 2008. "Evaluating the impact of a service-oriented framework for healthcare interoperability.," *Studies in health technology and informatics*, (136), p. 285.

Davis, F. D. 1989. "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," *MIS Quarterly*, (13:3), pp. 319–340.

Dinev, T., and Hart, P. 2006. "An Extended Privacy Calculus Model for E-Commerce Transactions," *Information Systems Research*, (17:1), pp. 61–80 (doi: 10.1287/isre.1060.0080).

Fornell, C., and Larcker, D. F. 1981. "Evaluating structural equation models with unobservable variables and measurement error," *Journal of marketing research*, pp. 39–50.

Gao, Y., Li, H., and Luo, Y. 2015. "An empirical study of wearable technology acceptance in healthcare," *Industrial Management & Data Systems*, (D. Xiaojun Wang, Professor Leroy White, ed.), (115:9), pp. 1704–1723 (doi: 10.1108/IMDS-03-2015-0087).

Garson, G. D. 2016. *Partial Least Squares: Regression and Structural Equation Models*, Asheboro, NC: Statistical Associates Publishers.

Gregory, J. 2015. *The Internet of Things: Revolutionizing the Retail Industry* (available at https://www.accenture.com/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_14/Accenture-The-Internet-Of-Things.pdf).

Hair, J. F., Ringle, C. M., and Sarstedt, M. 2012. "Partial Least Squares: The Better Approach to Structural Equation Modeling?," *Long Range Planning*, (45:5–6), pp. 312–319 (doi: 10.1016/j.lrp.2012.09.011).

Hair, J., Sarstedt, M., Hopkins, L., and G. Kuppelwieser, V. 2014. "Partial least squares structural equation modeling (PLS-SEM): An emerging tool in business research," *European Business Review*, (26:2), pp. 106–121 (doi: 10.1108/EBR-10-2013-0128).

Hauser, M., Griebel, M., Hanke, J., and Thiesse, F. 2017. "Empowering Smarter Fitting Rooms with RFID Data Analytics," in *Proceedings of the 13th International Conference on Wirtschaftsinformatik*.

Henseler, J., Ringle, C. M., and Sarstedt, M. 2015. "A new criterion for assessing discriminant validity in variance-based structural equation modeling," *Journal of the Academy of Marketing Science*, (43:1), pp. 115–135 (doi: 10.1007/s11747-014-0403-8).

Henseler, J., Ringle, C. M., and Sinkovics, R. R. 2009. "The use of partial least squares path modeling in international marketing," in *New challenges to international marketing*, Emerald Group Publishing Limited, pp. 277–319.

Herhausen, D., Binder, J., Schoegel, M., and Herrmann, A. 2015. "Integrating Bricks with Clicks: Retailer-Level and Channel-Level Outcomes of Online–Offline Channel Integration," *Journal of Retailing*, (91:2), pp. 309–325 (doi: 10.1016/j.jretai.2014.12.009).

Huang, J. L., Curran, P. G., Keeney, J., Poposki, E. M., and DeShon, R. P. 2012. "Detecting and Deterring Insufficient Effort Responding to Surveys," *Journal of Business and Psychology*, (27:1), pp. 99–114 (doi: 10.1007/s10869-011-9231-8).

Johnson, J. A. 2005. "Ascertaining the validity of individual protocols from Web-based personality inventories," *Journal of Research in Personality*, (39:1), pp. 103–129 (doi: 10.1016/j.jrp.2004.09.009).

Kline, R. B. 2015. *Principles and practice of structural equation modeling*, New York: Guilford publications.

Kourouthanassis, P. E., Giaglis, G. M., and Vrechopoulos, A. P. 2007. "Enhancing user experience through pervasive information systems: The case of pervasive retailing," *International Journal of Information Management*, (27:5), pp. 319–335 (doi: 10.1016/j.ijinfomgt.2007.04.005).

Kourouthanassis, P., and Roussos, G. 2003. "Developing consumer-friendly pervasive retail systems," *IEEE Pervasive Computing*, (2:2), pp. 32–39 (doi: 10.1109/MPRV.2003.1203751).

Kowatsch, T., and Maass, W. 2012. *IoT-I Deliverable - D2.4: Social Acceptance and Impact Evaluation* (available at https://www.alexandria.unisg.ch/211859/).

Kurtz, J. E., and Parrish, C. L. 2001. "Semantic Response Consistency and Protocol Validity in Structured Personality Assessment: The Case of the NEO-PI-R," *Journal of Personality Assessment*, (76:2), pp. 315–332 (doi: 10.1207/S15327752JPA7602_12).

Li, H., Wu, J., Gao, Y., and Shi, Y. 2016. "Examining individuals' adoption of healthcare wearable devices: An empirical study from privacy calculus perspective," *International journal of medical informatics*, (88), pp. 8–17 (doi: 10.1016/j.ijmedinf.2015.12.010).

Lockton, V., and Rosenberg, R. S. 2005. "RFID: The Next Serious Threat to Privacy," *Ethics and Information Technology*, (7:4), pp. 221–231 (doi: 10.1007/s10676-006-0014-2).

MacKenzie, I., Meyer, C., and Noble, S. 2013. *How retailers can keep up with consumers*, McKinsey & Company (available at http://www.mckinsey.com/industries/retail/our-insights/how-retailers-can-keep-up-with-consumers).

Meade, A. W., and Craig, S. B. 2012. "Identifying careless responses in survey data.," *Psychological Methods*, (17:3), pp. 437–455 (doi: 10.1037/a0028085).

Müller-Seitz, G., Dautzenberg, K., Creusen, U., and Stromereder, C. 2009. "Customer acceptance of RFID technology: Evidence from the German electronic retail sector," *Journal of Retailing and Consumer Services*, (16:1), pp. 31–39 (doi: 10.1016/j.jretconser.2008.08.002).

Nysveen, H., and Pedersen, P. E. 2016. "Consumer adoption of RFID-enabled services. Applying an extended UTAUT model," *Information Systems Frontiers*, (18:2), pp. 293–314 (doi: 10.1007/s10796-014-9531-4).

Parada, R., Melia-Segui, J., Morenza-Cinos, M., Carreras, A., and Pous, R. 2015. "Using RFID to Detect Interactions in Ambient Assisted Living Environments," *IEEE Intelligent Systems*, (30:4), pp. 16–22 (doi: 10.1109/MIS.2015.43).

PwC. 2015. *Total Retail 2015: Retailers and the Age of Disruption* (available at https://www.pwc.ie/media-centre/assets/publications/2015-pwc-ireland-total-retail-february.pdf).

Saha, D., and Mukherjee, A. 2003. "Pervasive computing: a paradigm for the 21st century," *IEEE Computer*, (36:3), pp. 25–31.

Salinas Segura, A., and Thiesse, F. 2015. "Extending UTAUT2 to Explore Pervasive Information Systems," in *ECIS 2015 Completed Research Papers*, Presented at the ECIS 2015 (doi: 10.18151/7217456).

Satyanarayanan, M. 2001. "Pervasive computing: Vision and challenges," *IEEE Personal communications*, (8:4), pp. 10–17.

Thiesse, F. 2007. "RFID, privacy and the perception of risk: A strategic framework," *The Journal of Strategic Information Systems*, (16:2), pp. 214–232 (doi: 10.1016/j.jsis.2007.05.006).

Vend. 2016. *Retail trends & predictions 2016: A collection of our top 12 forecasts for the retail industry*. (available at https://www.vendhq.com/university/retail-trends-and-predictions-2016).

Venkatesh, V., L. Thong, J. Y., and Xu, X. 2012. "Consumer Acceptance and Use of Information Technology extending the Unified Theory of Acceptance and Use of Technology," *MIS Quarterly*, (36:1), pp. 157–178.

Vroom, V. H. 1964. "Work and motivation. 1964," *NY: John Wiley & Sons*, (45).

Weiser, M. 1991. "The computer for the 21st century," *Scientific American*, (265:3), pp. 94–104.

Xu, H., Teo, H.-H., Tan, B. C. Y., and Agarwal, R. 2009. "The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services," *Journal of Management Information Systems*, (26:3), pp. 135–174 (doi: 10.2753/MIS0742-1222260305).

Zhao, L., Lu, Y., and Gupta, S. 2012. "Disclosure Intention of Location-Related Information in Location-Based Social Network Services," *International Journal of Electronic Commerce*, (16:4), pp. 53–90 (doi: 10.2753/JEC1086-4415160403).

Zhou, T. 2012. "Examining Location-Based Services Usage from the Perspectives of Unified Theory of Acceptance and Use of Technology and Privacy Risk," *Journal of Electronic Commerce Research*, (2012:13).