The adoption of smart services: do privacy concerns, trust in benevolence and usage experience matter?

Catherine Viot, Charlotte Lecuyer, Caroline Bayart, Agnès Lancini

Viot, C., Lecuyer, C., Bayard, C & Lancini, A. (2024).The adoption of smart services: do privacy concerns, trust in benevolence and usage experience matter? *Journal of Consumer Marketing*, © Emerald Publishing Limited [ISSN 0736-3761], [DOI 10.1108/JCM-04-2022-5299], Accepted 16 July 2024.

Access to the online published version : https://www.emerald.com/insight/content/doi/10.1108/JCM-04-2022-5299/full/html

The adoption of smart services: do privacy concerns, trust in benevolence and usage experience matter?

Introduction

The emergence of smart connected products (SCP) and smart services (SS) is a key characteristic of the third stage in the evolution of the Internet: "the Internet of Things (IoT) phase" (Hoffman and Novak, 2018). SCP open up new business opportunities and enable organisations to offer SS to consumers. SS rely on many SCP, such as smartphones, wearables or smart speakers to support service delivery (Allmendinger and Lombreglia, 2005; Mani and Chouk, 2019). They exploit the functionalities of these intelligent devices to offer consumers a new service experience. These functionalities are autonomy (performing automatic actions), intelligence (analysing and understanding data) and connectivity (collecting and exchanging data with the user and with other devices) (Mani and Chouk, 2019: 1462). For example, using smart technologies such as on-board diagnostic sensors, insurance companies can deliver new services such as "pay as you drive" and "pay how you drive" insurance. SS have developed significantly in recent years (Dreyer *et al*., 2021). They can be found in a variety of sectors, such as smart tourism, smart retail, smart cities, smart healthcare, and smart insurance (Roy *et al*., 2019) and have an impact on consumer behavior. Despite growing interest from both practitioners and researchers, the determinants of SS adoption in the long term remain unclear (Kim and Wang, 2021). Consumers perceive them as risky (Keh and Pang, 2010) and tend to show resistance (Mani and Chouk, 2016, 2019).

Given their ability to collect and share data, SS raise privacy issues (Wang *et al*., 2020). Despite privacy concerns, SS are used by customers who, at least tacitly, give the service provider permission to access their personal data. The privacy paradox, defined as the contradiction between users' concerns about the risk of disclosing their personal information and their information disclosure behaviors (Norberg *et al*., 2007; Norberg and Horne, 2007), is used as a theoretical framework in this research.

In order to address resistance, the nature of the relationship between service providers and their customers must change (Pantano *et al*., 2018). Consumers' concerns about information privacy affect their perception of risk and trust in the service provider (van Slyke *et al*., 2006). Trust has been defined as confidence in an exchange partner, resulting from perceived expertise, integrity, or intentionality (Morgan and Hunt, 1999). Many studies have shown the central role of trust in consumer-brand relationships (Hess and Story, 2005). Ganesan and Hess (1997) proposed a two-dimensional conceptualization of trust by referring to credibility trust and benevolence trust. "Benevolence trust is based on the qualities, intentions, and characteristics attributed to the focal partner that demonstrate a genuine concern and care for the partner through sacrifices that exceed a purely egocentric profit motive" (Ganesan and Hess, 1997: p. 440). Benevolence refers to a higher level of trust than credibility, since cooperative behavior is not based on rational calculation, but on goodwill (Borys and Jemison, 1989). This argument is particularly relevant in the context of the Internet and Information Technologies (IT), when people have to disclose personal data in

order to access online services (Gefen *et al*., 2003; McKnight *et al*., 2002). Wu *et al*. (2014) found that, among the dimensions of trust, benevolence trust has the greatest impact on IT use. Therefore, due to the complex nature of SS, benevolence trust attributed to the service provider is essential to balance the perceived risks of consumers in terms of information privacy.
The research questions this paper attempts to address are: (1) What are the drivers of SS adoption? and (2) Do the drivers of SS adoption differ depending on whether the consumer is already using SCP or not? As the literature emphasizes the key role of trust and privacy concerns in IT adoption, this research specifically questions the influence of these two factors on the adoption of SS. To date, research on consumer behavior has mainly focused on the early adoption of SCP (Koohang *et al*., 2022). However, some consumers have already adopted basic SCP (wearables, smart speakers, etc.). The resulting experience may influence future adoption of SS. Beliefs and attitude about the intention to adopt SS may change depending on the particular stage of IoT adoption (Karahanna, *et al*., 1999; Attié and Meyer-Waarden, 2022) and the user experience (Chatterjee *et al*., 2021; Lee, 2019; McKnight *et al*., 2020). Over time, "experience becomes more predictive than initial impressions" (McKnight *et al.*, 2020: p.1016) in explaining adoption. Therefore, it is crucial to question the influence of benevolence trust in the service provider and privacy concerns on the intention to adopt SS, depending on whether the individual already uses SCP or not.
To address these research questions, we first discussed the factors that facilitate SS adoption using the privacy paradox framework (Norberg *et al*., 2007). We then conducted an online survey to investigate the determinants of SS adoption. This survey focused more specifically on one type of SS: a connected car insurance based on the principles "pay as you drive" and/or "pay how you drive", a system later explained in the methodology section. Hypotheses were tested using structural equation modeling with multigroup analyses.
The expected contributions are twofold. From a theoretical point of view, this research aims to improve knowledge of the adoption of SS, by investigating two factors: benevolence trust in the service provider and privacy concerns. The results show that benevolence trust in the service provider directly and positively influences intention to adopt SS. They also confirm that privacy concerns are a significant barrier to this adoption. Moreover, this research complements the existing literature (Mani and Chouk, 2019) by proposing a distinction between users and non-users of SCP. The results confirm that privacy concerns are a barrier to the intention to adopt SS only for consumers who already use physical smart devices. From a managerial perspective, the main objective is to provide practical guidelines for SS providers.

1. Literature review

The privacy paradox

Previous studies have identified an inconsistency between consumers' attitude towards privacy and their subsequent behaviors. This mismatch is commonly referred to as the privacy paradox (Norberg *et al.*, 2007) and is explained by the calculus theory which states that consumers weigh the potential risks of disclosing their personal information against the potential benefits of using a product or service (Dinev and Hart, 2006). The privacy calculus theory suggests that individuals make decisions based on a balance between the expected loss and the potential gain of disclosing personal information (Dinev and Hart, 2006). People disclose information when the expected gain is greater than the cost resulting from the loss of privacy. "Although consumers frequently express great concern about the collection and utilization of their data, they frequently behave paradoxically, disclosing their information" (Massara *et al*., 2021: p. 1815). Dienlin and Trepte (2015) questioned whether the "privacy paradox" is a relic of the past, before concluding that it

was still relevant on social networking platforms. Users sometimes exhibit paradoxal privacy behaviors: on the one hand they agree to reveal their real name and mobile phone number, but on the other hand they are reluctant to disclose their address (Dienlin and Trepte, 2015). They might agree to share personal information, if they find it useful even if it contradicts their attitudes towards privacy. For example, they might share driving data with their insurer (e.g., geolocation, speed, etc.) in exchange for a lower insurance premium.

Privacy

In the digital age, consumers are increasingly concerned about privacy issues, and, as Jebarajakirthy *et al*. (2023: p. 153) pointed out, "Every new technology brings its own privacy concerns and risks". Privacy is "the ability to manage information about oneself" (Bélanger *et al*., 2002: p. 249) and the right of individuals to determine for themselves, when, how and to what extent information about them is shared with others (Westin, 1967). The literature refers to a number of different concepts: privacy, privacy knowledge or awareness, and privacy concerns. Although numerous, the "definitions of privacy typically include some form of control over the potential secondary uses of one's personal information" (Bélanger and Crossler, 2011, p. 1018). However, this concept is highly context sensitive (Margulis, 2003; Westin, 1967), as the costs and benefits are perceived differently across consumers and vary significantly from one situation to another. Dinev and Hart (2006) observed that consumers do not seek for absolute privacy, but are willing to sacrifice some of their personal data in order to obtain some benefits. SS, usually associated with physical smart devices that are able of making autonomous decisions, bring certain benefits to consumers, but inherently involve some loss of control over privacy information.

Trust in the benevolence of the partner

In the consumer behavior literature, trust is usually associated with qualities such as integrity, benevolence and competence (Gefen *et al*., 2003; McKnight *et al*., 2002). Based on their definition of trust as "a willingness to rely on a partner based on beliefs or expectations arising from that partner's experience, reliability, and benevolence", Ganesan and Hess (1997) proposed a two-dimensional conceptualization of trust that includes credibility trust and benevolence trust. Credibility trust refers to the intention to behave cooperatively, as a result of the costly or irrational nature of possible opportunistic behavior. "Benevolence trust is based on the qualities, intentions, and characteristics attributed to the focal partner that demonstrate a genuine concern and care for the partner through sacrifices that exceed a purely egocentric profit motive" (Ganesan and Hess, 1997: p. 440).

Trust in the benevolence of the partner, which results from the partner's willingness not to act opportunistically, even when the opportunity exists, is receiving renewed attention (Wu *et al.*, 2014). For some authors, benevolence refers to a more affective dimension of trust (Kantsperger and Kunz, 2010), and "trustee caring and motivation to act in the truster's interests" (McKnight *et al*., 2002: p. 337). Furthermore, benevolence is considered situation-specific, as it captures the underlying motivation for situation-specific behavior.

Despite the diversity of definitions, there is a consensus that trust plays an essential role in an uncertain and risky environment (Bhattacharya *et al*., 1998; Mayer *et al*., 1995). This concept therefore needs to be carefully considered in the context of SS adoption, as data collection and sharing with the service provider and third parties are key elements that differentiate SS from other traditional services.

2. Conceptual development

Trust in the benevolence of the smart-service provider

Marketing literature mainly highlights the positive influence of trust on consumer responses (Belanger and Crossler, 2011; Chaudhuri and Holbrook, 2001; McKnight *et al*. 2002, etc.). Gao and Bai (2014) suggest that trust in service providers plays a central role in IoT adoption intentions. In particular, recent research shows a significantly greater influence of benevolence than any other dimension of trust on consumer behavior, customer loyalty (Kantsperger and Kunz, 2010) and continued use of online social networks (Wu *et al*., 2014). Furthermore, the literature suggests that the role of trust in the benevolence is particularly important in situations that consumers perceive as risky, because cooperative behavior is not based on rational calculation, but on goodwill (Borys and Jemison, 1989). This argument is particularly relevant in the context of the IoT, where people are required to disclose personal information in order to access associated services. McKnight *et al.* (2002) argue that in situations where users choose to disclose their personal information to the online service provider, they are more concerned with the benevolence of the service provider than with its competence.

Due to the specificity of trust in the benevolence of the service provider (affective, context-specific), we choose to focus on this particular dimension. Inspired by previous definitions (Mayer *et al*., 1995; Wu *et al*., 2014), in the current study, trust in the benevolence of the service provider (TBSP) is defined as the belief that an SS provider is positively oriented toward its customers beyond the profit motive, and that it will consider the customer's well-being rather than purely its own benefit and act in the user's interest. Furthermore, the literature tends to support a positive relationship between TBSP and the intention to adopt a new technology (Wu et *al.*, 2014; McKnight *et al*., 2002).

Privacy concerns and smart services

While SS offers many benefits to users, they can also lead to the misuse of private information. The main forms of private information misuse, in relation to SS, are similar to those identified for online social networks: the collection of personal information without the user's knowledge or consent, and the sharing of user information with third party organizations (Mollick and Mykytyn, 2009). Studies that examine the impact of privacy concerns on intention to adopt new technologies are scarce. Instead, they focus on the relationship between privacy and the intention to disclose share personal information (Li *et al*., 2023). In the context of IoT, privacy concerns positively influence consumer's resistance to SCP (Mani and Chouk, 2016) as well as to SS (Mani and Chouk, 2019).

Usage experience in IoT physical devices

Previous research shows that the drivers of new technology adoption may change over time, due to better knowledge once the technology in question is actually adopted (Karahanna, *et al.*, 1999; McKnight *et al*., 2020; Venkatesh *et al*., 2003). According to consumer behavior research (Howard and Sheth, 1969) and cognitive dissonance theory (Festinger, 1957), using a product can change one's perceptions, attitudes and needs regarding the product. In the IT domain, Triandis (1980) explains that adoption beliefs change as the IT innovation is adopted and used. According to McKnight *et al*. (2020), experience with IT leads to the formation of an attitude, which in turn leads to stronger behavior. It is therefore expected that the intention to adopt SS will be stronger for SCP users than for non-SCP users. For example, someone who already owns a connected watch should be more inclined to adopt SS than a non-SCP user. Consequently, the factors influencing the intention to adopt SS should depend on the experience of using SCP.

Previous studies have explored the relationship between technology adoption and trust. The concept of initial trust in technology emerged from this extensive body of literature (Jarvenpaa and Leidner, 1998; Meyerson *et al*, 1996) and was recently described by McKnight *et al.* (2020) as "trust during the period before one has significant personal experience with the technology". According to Zanna and Rempel (1988), there are three general classes of information that explain IT adoption: information about past behaviour, affective information and cognitive information. Then, pre-adoption beliefs are formed primarily on the basis of indirect experiences with IT (affect or cognition - McKnight *et al*., 2020). Lee (2019) also shows that individuals who use less SS at home place more emphasis on trust in the service provider. Indeed, TBSP should be a lever for SS adoption for consumers with no prior experience in SCP. Therefore, we expect that TBSP will influence the intention to use SS only for consumers with limited experience in using SCP (SCP non-users).

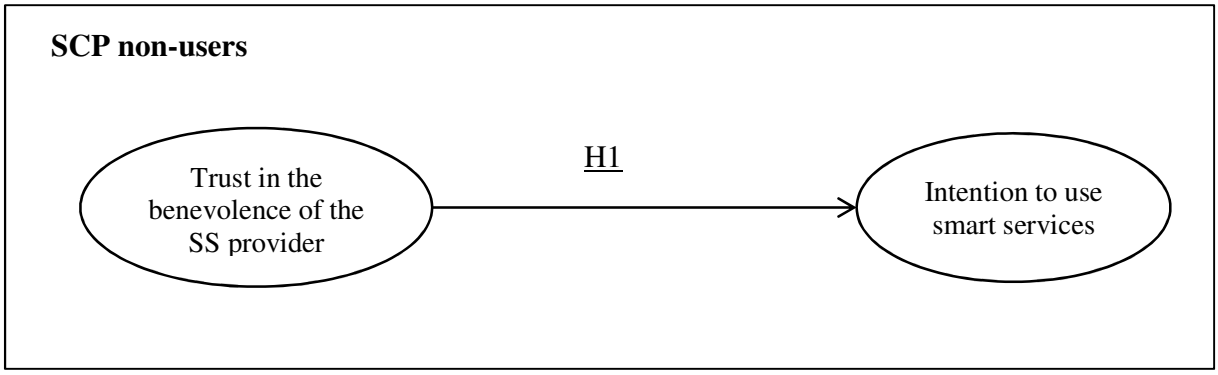
H1: TBSP positively influences the intention to adopt SS only for consumers who do not yet use SCP.

When consumers are already using a new technology, their experience of using it increases, as does their knowledge of and concerns about the risks involved. Once consumers start using SCP, they become more aware of the privacy issues they may raise (Koohang *et al*., 2022). In fact, privacy issues negatively influence intention to use IoT services (Lee, 2019), because some users may perceive privacy concerns to be greater than the expected benefits of IoT (Lee, 2019). McKnight *et al.* (2020) also suggest that post-adoption usage beliefs are formed based on past experiences. In this sense, users with experience of SCP are also more aware of privacy issues and privacy concerns should slow down their adoption of SS. As a result, we expect privacy concerns to act as a barrier, but only for consumers who already have experience with SCP (SCP users).

H2: Privacy concerns negatively influence the intention to adopt SS only for consumers who already use SCP.

Figure 1 shows the set of hypotheses describing the conceptual model for SCP $_{users}$ and SCP $_{non\text{-}users}$.

Figure 1. Models for quasi-experimental groups



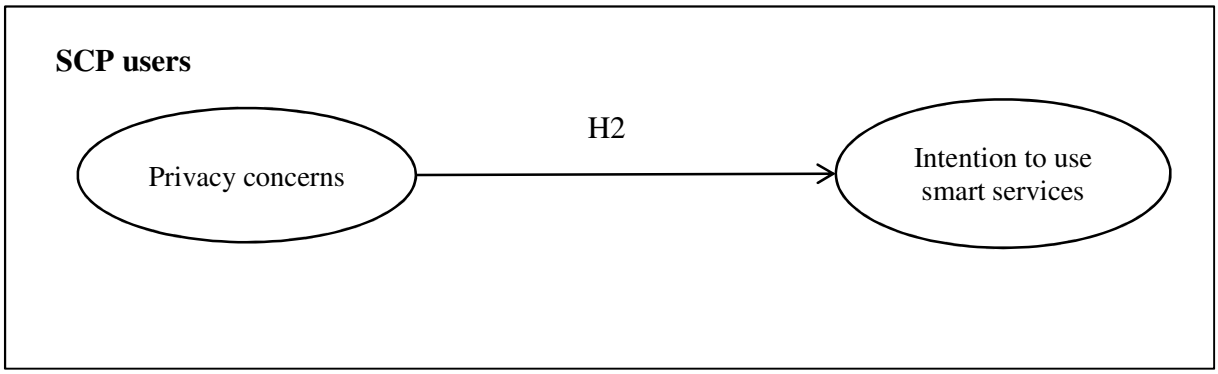


Figure 1 is the property is the property of the author(s).

3. Methodology

Focusing on "pay-as-you-drive" and/or "pay-how-you-drive" car insurance, this study investigates the intention to adopt a smart service in the insurance sector. Some insurers offer to their customers an on-board diagnostic sensor that can collect data on driving style and driven mileage. The insurer then uses the shared data to evaluate driving behavior and determine the rate of the insurance policy. Good drivers and/or those who drive less can thus benefit from reduced rates. The benefits are twofold: reducing the price to be paid and promoting more responsible driving behavior.

Sample and survey

French consumers were invited to complete an online survey (N = 380). To control for *ex-ante* common method bias, the study used two versions of the questionnaire, each with a different order of items measuring a given construct. Respondents were randomly assigned to one of the two versions. The questionnaire started with screening questions, as the survey was only aimed at people with a self-insured car. Then, specific items related to the respondents' SCP ownership, intention to adopt SS, TBSP and privacy concerns were asked. An open-ended question allowed respondents to list the SCP they owned, except widespread smartphones, tablets or laptops, in order to determine whether or not the individual is a user of SCP. The final questions concerned control variables such as attitude towards SCP, subjective knowledge regarding SCP, and respondents profile (gender, age, income and education level). 18 questionnaires were not included in the analysis because respondents had not subscribed to a car insurance policy in their own name. The number of completed questionnaires came to 362 (54% female; M_{age}=43.2 years old [18 to 79 years]; σ_{Age}=12.6). For 45% of respondents, the monthly net income is between €1,500 and €2,500. More than 30% of respondents own a SCP in addition to their smartphone, tablet or laptop. This percentage is close to the average percentage observed in France (Opinion Way, 2018). The average number of SCP per respondent is less than two (M_{SCPs} = 1.8).

Measurement

We used and/or adapted existing scales: TBSP (McKnight *et al.*, 2002), privacy concerns (Dinev and Hart, 2006). We also created two *ad hoc* items, reflecting the "pay as you drive" and the "pay how you drive" principles, for the behavioral intention to subscribe to a smart connected car insurance (Appendix 3).

Respondents indicated their agreement on a seven-point Likert scale, ranging from 1 (strongly disagree) to 7 (strongly agree). The mean values and standard deviation for each construct

(Appendix 1) show that the intention to subscribe to a smart connected car insurance is relatively low (1.99), compared to the mean of the other constructs: privacy concerns (4.70) and TBSP (3.89).

Quasi experimental group building

To differentiate between SCP users and non-users, we created a dummy variable: "own/don't own an SCP". This variable serves as a proxy to capture the experience of using SCP. We then utilized subjective knowledge and attitude toward SCP to further refine the construction of the quasi-experimental groups, as both variables reflect experience in using SCP. Prior to testing our hypotheses, we assessed and compared the levels of subjective knowledge and attitude toward SCP within the quasi-experimental groups. Attitude toward SCP, measured by a 3-item scale (Singh and Fang, 2004), and subjective knowledge, measured by a 4-item scale (Flynn and Goldsmith, 1999), are expected to be higher among SCP users due to their experience with IoT technology. As anticipated, the average subjective knowledge of SCP users is higher than that of non-users ($SK_{SCP\ non\text{-}users}$=3.22; S.D.=1.1; $SK_{SCP\ users}$=4.01; S.D.=1.02; t=6.94; p<.001). Similarly, the average attitude of SCP users is higher than that of non-users ($Att_{SCP\ non\text{-}users}$=4.26; S.D.=1.16; $Att_{SCP\ users}$=4.55; S.D.=0.98; t=4.55; p<.001). These findings confirm the validity of the proxy used to form the two experimental groups. Consequently, we will consider SCP users and SCP non-users as two distinct quasi-experimental groups in our analyses. This classification resulted in two sub-samples (or quasi-experimental groups): the first consisting of 256 SCP non-users and the second consisting of 106 SCP users.

4. Findings

Firstly, to control for common method variance bias (CMV), we performed Harman's one-factor test (Fuller *et al.*, 2016). The first principal component accounted for 37% of the variance, a percentage well below the recommended cut-off of 50%, suggesting that CMV is not an issue in this research (Podsakoff and Organ, 1986). A series of principal component analysis confirmed the reliability of the scales (Appendix 1).

Assessing the structural model and multigroup analysis

Next, in order to test our hypotheses, we performed structural equation modeling (SEM), using the AMOS 25.0 software. We followed the two-step approach, which recommends building a measurement model to assess the psychometric properties of the scales in a first step, before testing the hypotheses through a structural model, in a second step. A three-factor model (including TBSP, Privacy concerns, and Behavioral intention) provides a satisfactory fit (CFI=.983; RMSEA=.061; SRMR=.0321; χ^2=77.5; *df*=33; *p*<.001). Means, standard deviations, composite reliability and average variance extracted were within the optimal norms (Appendix 2). The average variance extracted (Fornell and Larcker, 1981) ranged from .63 (TBSP) to .81 (privacy concerns). The measurement model provides satisfactory discriminant validity (Appendix 2).

We then built a structural model using a bootstrap procedure based on 5,000 bootstrap samples, in order to performe a multigroup analysis, with the dummy variable « own/ don't own SCP », as recommended by Sauer and Dick (1993).

We first tested the differences between an unconstrained model (χ^2=157.15; *df*=68) and a constrained model (χ^2=196; *df*=86). The results confirm that the two groups (SCP non-user/user) differ at the model level ($\Delta\chi^2$=39; *p*<.01). The goodness of fit statistics for the multigroup unconstrained model were acceptable: CFI=.966; RMSEA=.06; SRMR=.072.

Then, we ran invariance tests. In two separate models, we forced the considered parameters to be equal and compared the constrained and unconstrained models. According to Hypothesis H1, we

expected a significant influence of TBSP in the group of SCP non-users. Although the results are consistent with expectations ($\lambda_{SCP\ non\text{-}users}$ =.225**; p=.008; $\lambda_{SCP\ users}$=-.092; p=.972), the invariance test failed to demonstrate the superiority of the unconstrained model (Table I). Consequently, Hypothesis H1 is rejected. The influence of TBSP is similar in both groups.

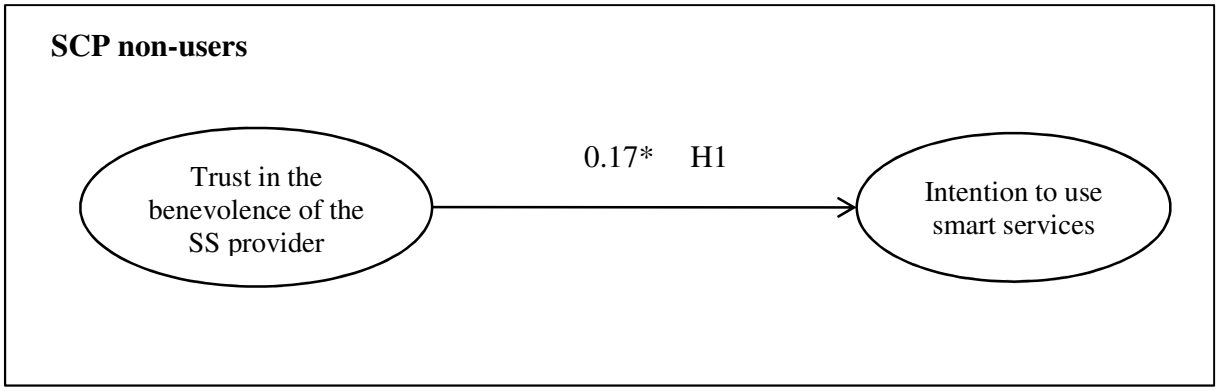
Table I. Results of multi-group analyses

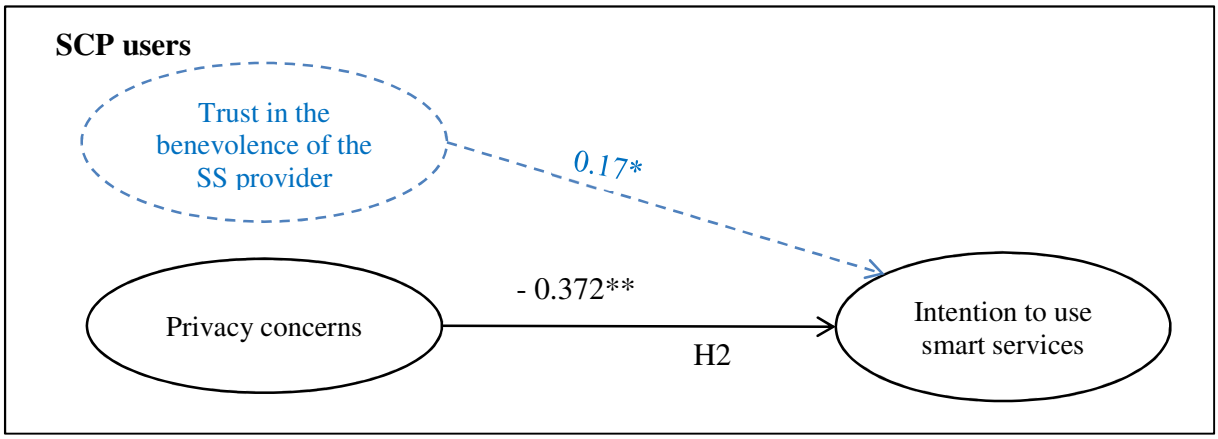
Models	Constrained parameters	DF	Δ DF	χ^2	Δ χ^2	p-value
Unconstrained model	-	68	-	157.15	-	<.001
Constrained model 1	Privacy-concerns - behavioral intention	69	1	165.64	8.51	.004
Constrained model 2	TBSP - behavioral intention	69	1	158.77	1.62	.203

Notes: DF=degrees of freedom; TBSP = Trust in the benevolence of the service provider. Table I is the property of the author(s).

In contrast, the second invariance test showed that the unconstrained model outperformed the constrained model for the "privacy concerns–intention" parameter (Table I). In support of Hypothesis H2, the results confirm a negative influence of privacy concerns on the intention to adopt SS in the group of SCP users ($\lambda_{SCP\ users}$=-.378*; p=.014; $\lambda_{SCP\ non\text{-}users}$=-.092; p=.170). Table II summarizes the results of the study.

Figure 2. Results for quasi-experimental groups





Notes: 1) The relationship between TBSP and the intention to use a smart service was not hypothesized for the quasi-experimental group of SCP users. However, the multigroup analysis shows that this relationship is significant in both groups.; 2) * p<.05; **p< .01. Figure 2 is the property of the Authors.

Table II. Summary of results

	Relationship	*Results*	*Estimate*
H1	TBSP-BI (SCP non-users)	Rejected	Similar influence of TBSP in users and non-users groups
H2	PC-BI (SCP users)	Supported	Negative influence of PC in the SCP users group ($\lambda_{SCP\ users}$=-.372**, p<.05) (no significant effect in the SCP non-users group).

Note: BI=behavioral intention; TBSP= Trust in the Benevolence of the Service Provider; PC=privacy concerns; * p<.05; ** p<.01; n.s.=non-significant. Table II is the property of the author(s).

5. Discussion and conclusion

Recent research focuses on the adoption of new SCP products (Mani and Chouk, 2017; Authors, 2023), but services and their intangible nature are a priority for future research (Ostrom *et al.*, 2015). While the number of SS in the marketplace continues to grow, to date there has been little empirical research focusing on the factors that explain SS adoption. In order to analyse the determinants that impact the intention to adopt SS, this research attends to combine consumer-specific factors, such as privacy concerns, with factors related to his/her relationship with the organisation, such as benevolence trust.

Theoretical contributions and implications

Three theoretical contributions, based on the privacy-paradox theory (Norberg *et al.*, 2007), are provided.

Firstly, our research shows that the relationship that customers have with the organisation seems to be of interest in explaining their intention to adopt SS. In particular, our research investigating the role of TBSP, complements Gao and Bai's (2014) findings. These authors have retained the

credibility and reliability dimensions of the trust concept, but not that of benevolence, and failed to confirm the influence of trust on the intention to adopt IoT. Consumers should therefore be more likely to adopt SS if they trust the SS provider's benevolence. From a theoretical point of view, this choice highlights the legitimacy of the organisation in the adoption of SS.

Secondly, this research supports the existing literature on the privacy paradox (Norbert *et al*., 2007; Aguirre *et al*., 2016). While the influence of concerns about personal data on the adoption of SCP is well known (Attié and Meyers-Waarden, 2022; Jaspers and Pearson, 2022), their impact on the adoption of SS is not yet well documented in the literature. The only exception is Mani and Chouk's study (2019). By demonstrating a direct relationship between privacy concerns and the intention to adopt SS, our study confirms the results of Mani and Chouk (2019) and stands out from those on SCP, which found a moderating effect of privacy concerns (Attié and Meyers-Waarden, 2022; Jaspers and Pearson, 2022). These findings suggest a differentiated effect of privacy concerns, depending on whether SCP or SS adoption is being explained. The effect of privacy concerns could be explained by the greater perceived sensitivity of the private data needed for SS to work effitiently, compared with SCP. Our work complements previous research by including a contingency factor – SCP usage experience – as a variable explaining the intention to adopt SS. Our results highlight a strong negative correlation between privacy concerns and intention to adopt SS, among consumers who already use SCP ($\lambda_{\text{SCP users}}$=-.37**, p<.01). This result can be explained because SCP users become more aware of the privacy issues they may raise (Koohang *et al*., 2022). As stated in the privacy paradox, some users may perceive privacy concerns to be greater than the expected benefits of IoT (Lee, 2019). Indeed, SCP users have a higher level of interest and engagement with IT, which is often related to a heightened sensitivity to privacy issues. By using SCP, consumers have been informed about how data is collected, stored and used. Conversely, SCP non-users may have limited knowledge of data collection and management practices, different expectations and a lower level of awareness of personal data protection issues. These findings show that the privacy paradox is not a 'relic of the past', and support the findings of Dienlin and Trepte (2015).

Lastly and counterintuitively, our results highlight that TBSP continue to exert a strong influence on behavioral intention independently of familiarity with the use of SCP. The predominant role of TBSP on the intention to adopt SS, regardless of SCP usage experience may seem counter-intuitive. The first reason lies in the nature of the data being transmitted. Milne *et al*. (2017) suggest an inverse relationship between the sensitivity of personal data and the willingness to provide it. Referring to Milne *et al*.'s (2017) typology, which classifies personal data according to its sensitivity, the data transferred in our study is sensitive. In-vehicules sensors record location and speed provide a wide range of information about driving behavior (e.g., driving style, compliance with traffic regulations rules). Consumers may fear that their insurer will impose economic penalties in the event of an accident or inappropriate behavior (e.g. exceeding the speed limit, dangerous overtaking), or even share sensitive data with the police (although under current French law, no fines can be impose in such circumstances). Whether or not consumers interested in subscribing to SS are SCP users, it seems difficult to commit to disclosing such sensitive data to an insurer without a certain level of TBSP. A second explanation relates to concerns about data security and potential misuse by third parties. A benevolent SS provider is more likely to have proven mechanisms to address data security concerns and may be committed to respecting the privacy of its users. In addition, a benevolent SS provider is likely to be perceived as transparent

about data collection, use and protection practices and provides clear information about how data is handled

Implications for practice

One of the main concerns of firms is to accelerate the diffusion of innovations to the market. As pointed out by Jahanmir and Cavadas (2018: p. 342), "Exploring and comprehending the determinants of late adoption will allow firms to accelerate the rate of adoption for their technologies". The difficulty facing managers today is the uncertainty surrounding the adoption of new value propositions by consumers. This is particularly true for SS, which requires costly development, and for the insurance sector, a market that by its nature involves personal data. In this context, decision-making is complex. While the privacy paradox may explain the acceptance of providing sensitive data in order to benefit from advantageous services (a lower premium for smart connected car insurance), it takes time for consumers to understand and assess the nature of the associated risks.

The challenge for SS providers is therefore to convince both consumers who are confortable using new technologies and those who are not. They should reassure these customers by informing them what data is being collected and for what purpose. Data security is all the more critical given the sensitivity of the personal information collected and security breaches can have serious consequences for the privacy of consumers. One of the priorities for marketers of SS should be to build a relationship with their customers based on benevolence trust. To achieve this, communication needs to be strengthened to highlight elements that are likely to build trust and reassure consumers, rather than focusing solely on the innovative nature of the service. This mays also involve investment in R&D to secure infrastructures or implementation of data security protocols within the organisation. The use of a third party, such as a secure platform for data transmission and storage, would reassure consumers and ultimately increase their willingness to adopt SS. Customer Relationship Management (CRM) also plays a key role. Reactivity and a proactive approach to problems, (i.e. the ability to anticipate and resolve them before they become critical) demonstrate an immediate concern for customers and help to reinforce perception of benevolence.

Our findings also provide empirical evidence that service providers should promote SS differently when targeting current SCP users. The first objective would be to target SCP users and more broadly those who are familiar with the IoT, with attractive commercial offers. According to the two-step communication flow model defined by Katz and Lazerfeld (2006), experienced users could then influence and persuade more reluctant customers, through positive word of mouth. With the change in scale and especially the speed of information dissemination made possible by social networks, this strategy seems promising. The idea would be to identify expert consumers, whom the serice provider could highlight on its website and social networks to reassure people who are less comfortable with new technologies. In addition, insurers could adopt an incremental approach, starting with offering services that are less divisive, in terms of personal data disclosure, and therefore less likely to raise consumer concerns. This service could take the form of a mobile application where users can voluntarily report information about their driving behavior. This intermediate step would allow customers to become familiar with IoT technology through a more familiar device and facilitate the adoption of more personal data-intensive SS in the future.

Privacy concerns are more complex in the case of smart connected car insurance. Devices such as on-board sensors in vehicles collect large amounts of data in real time. This data provides information about the location and travel patterns of individuals, the analisis of wich can lead to

detailed profiling of consumers, which raises concerns about its impact on premium levels. The need to obtain informed consent for data collection can also be difficult to manage. It is crucial that consumers fully understand what data is being collected, how it will be used and how it will affect their insurance. Ensuring informed consent can be complex due to the specific nature of the information involved and the complex regulatory framework of the insurance sector. An interesting approach would be to make the organisation's commitment not to disclose personal information on driving behaviour to third parties, especially those who could harm the insured. For example, regular information on the use of the data collected, or a link to legal articles reminding people that it is impossible to prove an offence using GPS data are low-cost measures likely to make it easier for consumers to accept smart connected car insurance. As long as customers perceive that their insurer is benevolent and trustworthy, they are likely to adopt innovative SS.

Limitations and future directions

This research presents some limitations. Firstly, it was conducted within a specific context, smart connected car insurance. The results must therefore be interpreted with caution when attempting to generalise to other contexts. Our results do not support hypothesis H1, which states that TBSP positively influences the intention to adopt smart services only among SCP non-users. Future research could therefore consider the replicability of the results when considering different types of data (sleep quality, physical condition, mobility patterns…) and test the impact of the perceived sensitivity of the information transmitted, which could moderate the relationship between TBSP and intention to adopt SS. Given the evolutionary nature of the technology, future research should also include additional measures of IoT knowledge in the model, to better understand its impact on SS adoption, as well as the concepts of perceived security, security risk or ease of use. Finally, the gap between behavioral intention and behavior is sometimes large. In order to confirm these results, it would therefore be useful to replicate the study by collecting data from different service providers, in order to measure the impact of the identified determinants on actual behavior.

REFERENCES

Aguirre, E., Roggeveen, A.-L., Grewal, D. and Wetzels, M. (2016), "The personalization–privacy paradox: implications for new media", *Journal of Consumer Marketing*, Vol. 33 No. 2, pp. 98-110.

Allmendinger, G. and Lombreglia, R. (2005), "Four strategies for the age of smart services", *Harvard Business Review*, Vol. 83 No. 10, pp. 131.

Attié, E. and Meyer-Waarden, L. (2022), "The acceptance and usage of smart connected objects according to adoption stages: an enhanced technology acceptance model integrating the diffusion of innovation, uses and gratification and privacy calculus theories", *Technological Forecasting and Social Change*, Vol. 176.

Authors

Bhattacharya, R., Devinney, T.M. and Pillutla, M.M. (1998), "A formal model of trust based on outcomes", *Academy of Management Review*, Vol. 23 No. 3, pp. 459-72.

Bélanger, F. and Crossler, R.E. (2011), "Privacy in the digital age: A review of information privacy research in information systems". *MIS Quarterly*, Vol. 35 No. 4, pp. 1017-1041.

Bélanger, F., Hiller, J. and Smith, W.J. (2002), "Trustworthiness in electronic commerce: the role of privacy, security, and site attributes", *Journal of Strategic Information Systems,* Vol. 11 No. 3/4, pp. 245-270.

Borys, B. and Jemison, D. (1989), "Hybrid arrangements as strategic alliances: theoretical issues in organizational combinations", *Academy Management Review*, Vol. 14 No. 2, pp. 234–249.

Chatterjee, S., Chaudhuri, R., Vrontis, D. and Hussain, Z. (2021), "Usage of smartphone for financial transactions: from the consumer privacy perspective", *Journal of Consumer Marketing*, Vol. 40 No. 2, pp. 193-208.

Chaudhuri, A. and Holbrook, M.B. (2001), “The chain of effect from brand trust and brand affect to brand performance: The role of brand loyalty”, *Journal of Marketing*, Vol. 65 No. 2, pp. 81-93.

Dinev, T. and Hart, P. (2006), “An extended privacy calculus model for e-commerce transactions”, *Information Systems Research,* Vol. 17 No. 1, pp. 61-80.

Dienlin, T. and Trepte, S. (2015), “Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors”, *European Journal of Social Psychology*, Vol. 45 No. 3, pp. 285-297.

Dreyer, S., Werth, O., Olivotti, D., Guhr, N. and Breitner, M.H. (2021), “Knowledge management systems for smart services: A synthesis of design principles”, *e-Service Journal.*, Vol. 13 No. 2, pp. 27-67.

Festinger, L. (1957), « *A theory of cognitive dissonance* », Stanford University Press.

Flynn, L. and Goldsmith, R. (1999), “A short, reliable measure of subjective knowledge”. *Journal of Business Research,* Vol. 46 No. 1, pp. 57-66.

Fornell, C. and Larcker, D.F. (1981), “Evaluating structural equation models with unobservable variables and measurement error”, *Journal of Marketing Research,* Vol. 18 No. 1, pp. 39-50.

Fuller, C.M., Simmering M.J., Atinc G., Atinc,Y. and Babin, B.J. (2016), “Common methods variance detection in business research”, *Journal of Business Research*, Vol. 69 No. 8, pp. 3192-3198.

Ganesan, S. and Hess, R. (1997), “Dimensions and levels of trust: implications for commitment to a relationship”, *Marketing Letters,* Vol. 8 No. 4, pp. 439–448.

Gao, L. and Bai, X. (2014), “A unified perspective on the factors influencing consumer acceptance of internet of things technology”, *Asia Pacific Journal of Marketing and Logistics*, Vol. 26 No. 2, pp. 211-231.

Gefen, D., Karahanna, E. and Straub, D.W. (2003), “Trust and TAM in online shopping: an integrated model”, *MIS Quarterly*, Vol. 27 No.1, pp. 51-90.

Heidenreich, S. and Kraemer, T. (2016), “Innovations—Doomed to Fail? Investigating Strategies to Overcome Passive Innovation Resistance », *Journal of Product Innovation Management*, Vol. 33 No. 3, pp. 277-297.

Hess, J. and Story, J. (2005), "Trust-based commitment: multidimensional consumer-brand relationships", *Journal of Consumer Marketing*, Vol. 22 No. 6, pp. 313-322.

Hoffman, D.L. and Novak, T.P. (2018), “Consumer and object experience in the internet of things: An assemblage theory approach,. *Journal of Consumer Research,* Vol. 44, pp. 1178-1204.

Howard, J.A. and Sheth, J.N. (1969), “*The Theory of Buyer Behavior*”, New York: John Wiley, pp. 12-15.

Jahanmir, S.F. and Cavadas, J. (2018), “Factors affecting late adoption of digital innovations”, *Journal of Business Research*, Vol. 88, pp. 337-343.

Jarvenpaa, S.L. and Leidner, D.E. (1998), “Communication and trust in global virtual teams, *Journal of Computer-Mediated Communication*, Vol. 3 No. 4, pp. 971-815.

Jaspers E.D.T. and Pearson E. (2022), “Consumers' acceptance of domestic Internet-of-Things: The role of trust and privacy concerns”, *Journal of Business Research*, Vol. 142, pp. 255-265.

Jebarajakirthy, C., Weaven, S., Arli, D. and Iqbal Maseeh, H. (2023), “Consumer privacy in the technological era”, *Journal of Consumer Marketing*, Vol. 40 No. 2, pp. .153-154

Kantsperger, R. and Kunz, W.H. (2010), “Consumer trust in service companies: a multiple mediating analysis”, *Managing Service Quality: An International Journal*, Vol. 20 No. 1, pp. 4-25.

Karahanna, H., Straub, D.W. and Chervany, N.L. (1999), “Information technology adoption across time: a cross-sectional comparison of pre-adoption and post-adoption beliefs”, *MIS Quarterly*, Vol. 23 No. 2, pp. 183-213.

Katz, E., Lazarsfeld, P.F., and Roper, E. (2006), “*Personal Influence: The Part Played by People in the Flow of Mass Communications”*, 1st ed., Routledge.

Keh, H.T. and Pang, J. (2010), “Customer reactions to service separation”, *Journal of Marketing*, Vol. 74 No. 2, pp. 55-70.

Kim, K.J. and Wang, S. (2021), "Understanding the acceptance of the Internet of Things: an integrative theoretical approach", *Aslib Journal of Information Management*, Vol. 73 No. 5, pp. 754-771.

Koohang, A., Sargent, C.S., Nord, J.H. and Paliszkiewicz , J. (2022), "Internet of Things (IoT): From awareness to continued use International", *Journal of Information Management*, Vol. 62.

Lee, M. (2019), "An empirical study of home IoT services in South Korea: The moderating effect of the usage experience", *International Journal of Human–Computer Interaction*, Vol. 35 No. 7, pp. 535-547.

Li, J., Zhang ,Y. and Mou, J. (2023), "Understanding information disclosures and privacy sensitivity on short-form video platforms: An empirical investigation", *Journal of Retailing and Consumer Services*, Vol. 72.

Mani, Z. and Chouk, I. (2016), "Drivers of consumers' resistance to smart products", *Journal of Marketing Management*, Vol. 33 No. 1-2, pp. 76-97.

Mani, Z. and Chouk, I. (2019), "Impact of privacy concerns on resistance to smart services: does the 'Big Brother effect' matter?", *Journal of Marketing Management*, Vol. 35 No. 15-16, pp. 1460-1479.

Margulis, S.T. (2003), "Privacy as a Social Issue and Behavioral Concept", *Journal of Social Issues*, Vol. 59 No. 2, pp. 243-261.

Massara, F., Raggiotto, F. and Voss, W.G. (2021), "Unpacking the privacy paradox of consumers: A psychological perspective", *Psychology & Marketing,* Vol. 38 No. 10, pp. 1814-1825.

Mayer, R.C., Davis, J.H. and Schoorman, D. (1995), "An integrative model of organizational trust", *Academy of Management Review*, Vol. 20 No. 2, pp. 709-34.

McKnight, D.H., Choudhury, V. and Kacmar, C. J. (2002), "Developing and validating trust measures for e-commerce: an integrative typology", *Information Systems Research*, Vol. 13 No. 3, pp. 334-359.

McKnight, D.H., Liu, P. and Pentland, B.T (2020), "Trust change in information technology products", *Journal of Management Information Systems*, Vol. 37 No. 4, pp.1015-1046.

Meyerson, D.; Weick, K.E. and Kramer, R.M. (1996), "Swift trust and temporary groups", In Kramer R.M. and Tyler T.R. (ed.), *Trust in Organizations: Frontiers of Theory and Research*. Thousand Oaks, CA: Sage, pp. 166-195.

Milne, G.R., Pettinico, G., Hajjat, F.M. and Markos, E. (2017), "Information sensitivity typology: mapping the degree and type of risk consumers perceive in personal data sharinog", *The Journal of Consumer Affairs*, Vol. 51 No. 1, pp. 133-161.

Mollick, J.S. and Mykytyn, P.P. (2009), "An empirical investigation on the effects of privacy policies on perceived fairness of online vendor", *Journal of Internet Commerce*, Vol. 8, pp. 88-112.

Morgan, R.M. and Hunt, S. (1999), "*Relationship-based competitive advantage: the role of relationship marketing in marketing strategy*", *Journal of Business Research*, Vol. 46, pp. 281-90.

Norberg, P.A, Horne, D.R. and Horne, D.A. (2007), "The privacy paradox: personal information disclosure intentions versus behaviors", *Journal of Consumer Affairs*, Vol. 41 No. 1, pp. 100-126.

Norberg P.A. and Horne D.R. (2007), "Privacy attitudes and privacy related behavior", *Psychology & Marketing*, Vol. 24 No. 10, pp. 829–847.

Opinion Way (2018), *Les Français et les objets connectés,* for Internet Society, France, June 2018. Ostrom, A. L., Parasuraman, A., Bowen, D. E., Patrício, L., and Voss, C. A. (2015), "Service Research Priorities in a Rapidly Changing Context", *Journal of Service Research*, Vol. 18 No. 2, pp. 127-159.

Pantano, E., Priporas, C.V. and Dennis, C. (2018), "A new approach to retailing for successful competition in the new smart scenario", *International Journal of Retail & Distribution Management*, Vol. 46 No. 3, pp. 264-282.

Podsakoff, P.M. and Organ, D.W. (1986), "Self-reports in organizational research: Problems and prospects", *Journal of Management*, Vol. 12, pp. 69-82.

Roy, S.K., Singh, G., Hope, M., Nguyen, B., and Harrigana, P. (2019), "The rise of smart consumers: role of smart servicescape and smart consumer experience co-creation", *Journal of Marketing Management*, Vol. 35, No. 15-16, pp. 1480-1513.

Sauer, P. L. and Dick, A. (1993), "Using moderator variables in structural equation models", in NA - Advances in Consumer Research, 20, eds. Leigh McAlister and Michael L. Rothschild, Provo, UT: Association for Consumer Research, pp. 636-640.

Singh, Y.Y. and Fang, K. (2004), "The use of a decomposed theory of planned behavior to study Internet banking in Taiwan", *Internet Research,* Vol. 14 No. 3, pp. 213-23.

Storey, C. Cankurtaran, P., Papastathopoulou, P. and Jan Hultink, E. (2015), "Success Factors for Service Innovation: A Meta-Analysis", *Journal of Product Innovation Management*, Vol. 33 No. 5, pp. 527-548.

Triandis, H.C. (1980), «"Values, Attitudes, and Interpersonal Behavior", Nebraska Symposium on Motivation, University of Nebraska Press, Lincoln.

Urban, G.L., Sultan, F. and Qualls, W. (1999), "Design and evaluation of a trust based advisor on the Internet". Working paper MIT. https://www.researchgate.net/profile/Glen-

van Slyke, C., Shim, J.T., Johnson, R. and Jiang, J. (2006), "Concern for information privacy and online consumer purchasing", *Journal of the Association for Information Systems*, Vol. 7 No. 6, pp. 415-444.

Venkatesh, V., Morris, M.G., Davis, G.B. and Davis, F.D. (2003), "User acceptance of information technology: toward a unified view", *MIS Quarterly*, Vol. 27 No. 3, pp. 425-478.

Wang, Y., Yan, Z., Feng, W. and Liu, S. (2020), "Privacy protection in mobile crowd sensing: a survey", *World Wide Web*, Vol. 23 No. 1, pp. 421-452.

Westin, A.F. (1967), "*Privacy and freedom"*, New York: Atheneum.

Wu, C.-C., Huang, Y. and Hsu, C.-L. (2014), "Benevolence trust: a key determinant of user continuance use of online social networks", *Information Systems and e-Business Management*, Vol. 12, pp. 189-211.

Zanna, M. P. and Rempel, J. K. (1988), « *Attitudes: A new look at an old concept* », in D. Bar-Tal & A. W. Kruglanski eds. *The social psychology of knowledge*, pp. 315–334, Cambridge University Press; Editions de la Maison des Sciences de l'Homme.

Appendix 1. Results of principal components analyses

	KMO	Bartlett's tests	Cronbach's alpha	Variance explained	Item	Loading	Communality
Privacy concerns (PC) (Dinev and Hart, 2006)	.852	χ^2 = 1455; df = 6; p< .001	.945	85.95	PC1	.980	.774
					PC2	.946	.894
					PC3	.944	.891
					PC4	.937	.878
Trust in the Benevolence of the Service Provider (TBSP) (McKnight *et al*., 2002)	812	χ^2 = 713; df = 6; p< .001	.851	72.09	TBSP1	.852	.726
					TBSP2	.840	.706
					TBSP3	.884	.781
					TBSP4	.819	.671

Note: df = degrees of freedom ; The table in Appendix 1 is the property of the author(s).

Appendix 2. Correlation matrix, composite reliability and square root of average variance extracted (AVE)

	Means (standard deviation)	Composite reliability	AVE	BI	TBSP	PC
Behavioral intention (BI)	1.99(1.24)	.89	.80	**.894**(a)		
TBSP	3.88(1.02)	.87	.63	.144**(b)	**.794**	
Privacy concern (PC)	4.70(1.35)	.95	.81	-.160**	.138**	**.900**

Notes: (a) Diagonal elements in bold are square root of AVE, (b) Off-diagonal elements are correlations, (c) ** p <0.01; TBSP = Trust in the benevolence of the service provider. The table in Appendix 2 is the property of the author(s).

Appendix 3. Measures

Privacy concerns

1. I am concerned that the information I submit to my insurer, about my driving behavior, could be misused.
2. I am concerned that a person can find private information about my driving behavior.
3. I am concerned about providing personal information about my driving behavior to my insurer, because of what others might do with it.
4. I am concerned about providing personal information about my driving behavior to my insurer because of what others might do with it.

Trust in the benevolence of the service provider

1. I believe that my insurance company would act in my best interest.
2. If I required help, my insurance company would do its best to help me.
3. My insurance company is interested in my well-being, not just its own.
4. I believe that my insurance company is continually seeking to improve the responses provided to customers' needs.

Intention to adopt smart services

1. In the mid-term, I am likely to sign up for a connected car-insurance (through a device placed in my car), which will allow my insurer to obtain information on the distance driven.
2. In the mid-term, I am likely to sign up for a connected car-insurance (through a device placed in my car), which will allow my insurer to obtain information on my driving style.