Impact of privacy concerns on resistance to smart services: does the 'Big Brother effect' matter?

Zied Mani, Inès Chouk

► To cite this version:

Zied Mani, Inès Chouk. Impact of privacy concerns on resistance to smart services: does the 'Big Brother effect' matter?. Journal of Marketing Management, 2019, The role of smart technologies in decision making: developing, supporting and training smart consumers, 35 (15-16), pp.1460-1479. 10.1080/0267257X.2019.1667856 . hal-03217977

HAL Id: hal-03217977

<https://hal.science/hal-03217977>

Submitted on 5 May 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Impact of privacy concerns on resistance to smart services:

Does the “Big Brother effect” matter?

Zied MANI

LEMNA Research Center, Nantes University, IUT Saint Nazaire, France

58 rue Michel Ange 44606 Saint Nazaire cedex.

+33601232078

zied.mani@univ-nantes.fr

Inès CHOUK

THEMA Research Center, UMR CNRS 8184, Cergy-Pontoise University, France

33, boulevard du Port, 95011 Cergy-Pontoise cedex

Chair of “Digital Economy”, Paris-Dauphine University

ines.chouk@u-cergy.fr

Citation: 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, 35 (15-16), 1460-1479.
<https://doi.org/10.1080/0267257X.2019.1667856>

Abstract

The aim of this study is to provide a better understanding of the factors that explain consumer resistance to smart services from a privacy perspective. To this end, an exploratory qualitative study and a quantitative study were carried out. 653 French consumers answered an online questionnaire regarding smart services in the banking sector. Structural equation modeling was used to test the conceptual model. The findings show that information privacy, the unauthorized secondary use of personal information and perceived intrusion have an impact on consumer resistance to smart services. Moreover, our research highlights the major role of the “Big Brother effect” as an antecedent to these various privacy concerns.

Keywords: smart service; smart product; privacy concerns; resistance; Big Brother

Summary Statement of Contribution: The contribution of this paper is twofold. First, our study is, to our knowledge, the first to look at resistance to innovation from the standpoint of privacy. Second, our paper proposes a definition of the concept of the Big Brother effect and provides an empirical evidence of its impact on consumer privacy concerns: information privacy, the unauthorized secondary use of personal information and perceived intrusion.

INTRODUCTION

The Internet of Things (IoT) is defined as the next stage of the internet incorporating “billions of devices that are able to communicate with consumers and other systems, services, and devices through the Internet” (Novak & Hoffman, 2018, p. 216). These smart technologies are revolutionizing consumers’ lives: smart cities, smart homes, smart retailing, smart banking, smart grids, etc. For example, in the banking sector, smart devices provide new services for customers such as wearable contactless payment, real-time tracking of expenditure and instant management of bank accounts.

However, some questions legitimately deserve to be raised. Do smart technologies go hand in hand with “big progress”? Are the ever increasing numbers of smart devices always beneficial for and in the interests of the consumer? While the current trend is to respond affirmatively to these questions, some research is more equivocal and highlights consumer resistance to these new smart products and services (Mani & Chouk, 2018). Understanding consumer resistance seems crucial to ensure the success of smart products and services (Wunderlich et al., 2015). Indeed, resistance to innovation is often considered as one of the main reasons for the failure of new services and products (Heidenreich and Spieth, 2013). In this respect, a number of recent studies have proposed examining consumer resistance to smart services and products (e.g. Balta-Ozkan et al. 2013; Juric & Lindenmeier, 2018). Such studies generally examine resistance to these innovations by identifying barriers related to use (perceived complexity), value (e.g. perceived price), risk (e.g. security risk), image (e.g. self-image congruence), tradition (the need for human interaction), technological vulnerability (e.g. technology anxiety), inertia, and so on. The findings shed light on the functional and psychological barriers that make consumers reluctant to adopt IoT based services/products. However, these studies suffer from two main limitations.

First, despite the expanding literature on resistance to smart technologies, no research, to our knowledge, has proposed studying resistance to smart services from a privacy perspective. The few existing studies have mobilized certain specific variables that directly or indirectly impact consumer resistance (e.g. privacy concerns [Mani & Chouk, 2017]). However, given its multifaceted and contextual nature, privacy needs be studied from an overall perspective that takes into account its specificities with regard to the IoT (Hsu & Lin, 2016). Consequently, recent studies have analyzed the impact of privacy concerns on adoption (Marakhimov & Joo, 2017) and continued use intention (Hsu & Lin, 2016) of smart services/devices. These studies generally use the adoption paradigm (Davis, 1989; Venkatesh et al., 2012) to explain the process of consumer acceptance of a new smart service or product. While the adoption approach provides an understanding of the mechanisms for the diffusion of an innovation in the market, it does not explain why consumers may not accept the innovation (Ram and Sheth, 1989). In this context, analyzing consumer reactions through the resistance paradigm allows us to understand the barriers that create uncertainty and the rejection of innovations (Hazée et al., 2017). It is therefore legitimate to consider privacy concerns as barriers that generate a negative consumer reaction.

Secondly, the IoT is viewed as the third digital revolution, after the mobile internet and internet web pages (Novak & Hoffman, 2018). These technologies (1) favor the development of ubiquitous, autonomous and intelligent services and products, and (2) create major issues related to the management and protection of large amounts of information (big data). In this context, the “vision of a pervasive and omnipresent technology has spurred considerable controversy due to privacy concerns and fears of an Orwellian surveillance society” Sletteameås (2009, p. 219). “Big Data is watching YOU” (Lichy et al., 2017), “Big Brother imagery” (Xu et al., 2009), “Big Brother Syndrome” (Minerva, 2016), “Big other” (Zuboff, 2015)... all of which are expressions currently used to refer to an Orwellian world in which

people are under surveillance and subject to control. Various press articles and surveys (e.g. KPMG, 2015) highlight the growing presence of this concern in the minds of consumers. However, to our knowledge, there have been no empirical studies examining the impact of this variable in the context of negative consumer reactions to innovations. Accordingly, we propose studying the “Big Brother effect” (BBE) as one of the components of consumers’ privacy concerns to explain consumer resistance to smart services.

To fill these theoretical gaps, we address the following research questions: what is the impact of privacy concerns on consumer resistance to smart services? To what extent does the BBE have an impact on these concerns and on consumer resistance to smart services?

The objectives of our research here are as follows: (1) to identify consumers’ privacy concerns within the framework of the IoT, (2) to test the impact of these privacy concerns on consumers’ resistance to innovation, and (3) to investigate to what extent the BBE improves our understanding of negative consumer reactions to new smart services. To this end, we conducted an empirical study in the banking sector. Indeed, this sector presents real development opportunities for the IoT (MarketandMarket, 2017). At the same time, banks face significant privacy challenges due to sensitive data and the risk of cyber-attacks.

The remainder of the paper is divided into three sections. The first provides a literature overview and presents the research hypotheses. The second elaborates the methodology and presents the results. The final section discusses the findings and looks at their managerial and theoretical implications.

Literature review

What are smart services?

In the service literature, the concept of “smart” refers to two ideas. First, it refers to the use of a technology that is termed “smart” in that it concerns “an electronic device or system that can be connected to the Internet and used interactively” (Foroudi et al., 2018, p. 271). Secondly,

the term “smart” describes the new characteristics and capabilities of services in terms of the nature of consumer interaction, the nature of the service experience and the provision of services (Roy et al., 2017).

The term “smart services” is used in the present study to designate services that include IoT devices (e.g. wearables) in support of service delivery. Smart services lie within a new context in which the idea of smartness implies new partnerships between the company and its customers and new methods of collecting, exchanging and analyzing data and information (Pantano et al., 2018). According to many (Porter & Heppelmann, 2014; Wunderlich et al. 2015; Lim & Maglio, 2018), smart services integrate new characteristics, allowing them to be autonomous (i.e. carrying out automatic actions without the user’s intervention), intelligent (i.e. analyzing and understanding data related to users and their environment), connected (i.e. collecting and exchanging data with the user and with other devices) and ubiquitous (i.e. providing services anytime, anywhere, and from any device).

While some research has highlighted the benefits and drivers of adoption of smart services, other studies have focused consumer concerns leading to resistance to these services.

Smart services: a consumer resistance to innovation perspective

In the marketing and innovation literature, the conceptualization of consumer resistance varies considerably from study to study (Heidenreich and Spieth, 2013). Among the perspectives for studying resistance, some authors identify two levels: a micro level (individual resistance) and a macro level (collective resistance) (Peñaloza and Price, 1993). Individual resistance generally refers to individuals’ oppositional reactions to novelty and attempts to impose the innovation, while collective resistance refers to organized and group actions (e.g. boycotts, protests) aimed at more radically opposing marketing practices (Roux, 2007).

Since our research objective is to analyze the impact of privacy concerns on individual resistance to smart services, we adopt the micro level perspective. More specifically, our

study lies within research that has studied consumer resistance as individual resistance to innovation. Consequently, in line with Heidenreich and Spieth (2013), consumer resistance in our research can be defined as an individual negative reaction toward a new product/service.

In the service marketing literature, resistance to innovation is generally studied within the theoretical model of resistance to innovation proposed by Ram and Sheth (1989) as the outcome of five barriers (Laukkanen 2016; Hazée et al. 2017). Thus, the consumer may be hesitant to use a new service due to its complexity (i.e. usage barrier), economic performance (i.e. value barrier) and the risk involved (i.e. risk barrier). In addition, other barriers arise when the new service or product upsets the consumer's entrenched beliefs (i.e. image barrier and tradition barrier).

In line with this resistance paradigm, an emerging research perspective focuses on consumers' negative reactions to smart services (e.g. Balta-Ozkan et al. 2013; Hong et al. 2017; Park & Koh, 2017). These studies generally examine the barriers that drive consumers to express resistance to smart services (see Table 1). In these cases the authors argue that smart services as an innovation lead to changes in consumer habits, beliefs, and a satisfactory status quo (Mani & Chouk 2018).

Table 1. Review of the main studies on resistance barriers in the context of the IoT

References	IoT context	Nature of study	Relevant findings
Balta-Ozkan et al. 2013	Smart home	Qualitative	The authors identify several social barriers inhibiting the acceptance of smart homes, such as control, security, and cost.
Mani and Chouk (2017)	Smart product (smart watches)	Qualitative and quantitative	The findings show that innovation characteristics (perceived usefulness, perceived novelty, perceived price, perceived intrusiveness) and consumer characteristics (privacy concerns, self-efficacy) are variables that explain consumer resistance to smart products.
Park and Koh (2017)	Smart products (e.g. smart watches, smart glasses)	Quantitative	Situational factor (i.e. perceived pace of technology change) and perceived expectation are variables that explain resistance to new products.
Mani and Chouk (2018)	Smart service	Quantitative	The authors extend and update Ram and Sheth's (1989) theoretical framework on the barriers leading to consumer resistance to innovation. They introduce new barriers (technological vulnerability barriers, ideological barriers and dispositional barriers) to explain consumer resistance to smart services.
Hong et al. (2017)	Smart home	Quantitative	The empirical results show that four types of risk (i.e. performance risk, financial risk, privacy risk and psychological risk) are affected by technological uncertainty and service intangibility on the one hand, and have positive effects on resistance to the smart home on the other.
Juric and Lindenmeier (2018)	Smart products (smart-lighting products)	Quantitative	The empirical results identify performance expectancy, social pressure and compatibility and health concerns as major determinants of individuals' inclination to adopt or reject smart-lighting products.

Despite the contributions of these studies in understanding the factors of resistance to smart services, no research has focused on various privacy concerns or has empirically examined the impact of Big Brother concerns. However, several authors stress the importance of these

concerns in view of the proliferation of new technologies (e.g. Sletteameås, 2009), including the IoT.

Privacy concerns in a smart services context

Privacy concerns

Privacy is generally defined as the individual's ability to control his/her personal information (Bélanger and Crossler, 2011; Lancelot-Miltgen et al., 2016). For Margulis (1977, p. 10) "privacy, as a whole or in part, represents the control of transactions between person(s) and other(s), the ultimate aim of which is to enhance autonomy and/or to minimize vulnerability". In the context of the proliferation of new technologies in everyday life (home, leisure...) and in the economic sphere (work, shopping...), privacy has become a central topic in the literature, including the marketing literature (Lancelot-Miltgen et al., 2016). Indeed, the use of new technologies in the fields of retailing and services generates significant amounts of information and data. This explosion of sensitive and personal information has been accompanied by consumers' growing concerns about the misuse of such information by companies or external entities. Thus, concern for privacy has today become one of the major inhibitors to the adoption and acceptance of new technologies in retailing and services (Miyazaki & Fernandez, 2001; Aloysius et al., 2016), including smart services.

The characteristics of smart services as potential privacy concerns

In the case of services based on IoT devices, the user does not always have control over the information and data provided (Hsu & Lin, 2016). Rather it is the products themselves (e.g. smart watches, smart wristbands) that communicate with each other instantaneously and carry out actions without the intervention of the user (e.g. automatically arranging payment of a bill based on the data collected). These services are also characterized by the proliferation of communicating devices such as the products used on a day-to-day basis by the consumer (e.g. car, refrigerator, weighing machine, home security system) and the products made available

by the company (e.g. payment terminal, shopping assistant systems) (Roy et al., 2017). In this way the company is made aware continuously and instantaneously of customers' needs through data supplied by smart devices. These devices enable the company to acquire information about customers' activities (e.g. through monitoring their day-to-day activities, knowledge of their habits, recording personal data, etc.) and to offer appropriate services (e.g. informing customers' of its banking activities, paying bills, authenticating purchases with personal data). In this context, the integration of smart technologies may facilitate companies' access to real-time data on consumer behavior, thereby generating big data (Pantano et al., 2018).

Big data, the proliferation of digital media, the presence of smart products in everyday life... all of these may increase consumers' privacy concerns in an IoT context (Hsu & Lin, 2016). In this respect, various experts have identified vulnerability issues and privacy-related risks associated with a number of smart products (and their associated services) on the market. For example, every year the Mozilla Foundation publishes a list of connected objects in its "Privacy not included¹" program, criticizing connected objects that do not respect their users' privacy. In the same vein, Ching and Singh (2016) analyzed three connected objects (Google glass, Fitbit devices, and Samsung smart watches) and identified technical vulnerabilities (e.g. photos and videos can be recorded without user's consent) that expose users to the risk of their private information being appropriated (through, for example, phishing, eavesdropping, and spyware).

On the academic level, research on privacy issues related to the IoT is still at an embryonic stage. Some recent research has highlighted privacy risks regarding the use of smart devices/services (Hsu & Lin, 2016; Wiegard & Breitner, 2017; Marakhimov & Joo, 2017). Thus, in line with our research objective, we decided to carry out a preliminary small-scale

¹ <https://foundation.mozilla.org/en/privacynotincluded/>

qualitative study to identify the different facets of privacy concerns in a smart services context. In the next section, we explain our methodology and present our findings.

Preliminary qualitative study on consumer privacy concerns about the IoT

To explore consumer privacy concerns about the IoT (smart products and/or smart services) we conducted nineteen semi-structured interviews. The participants were selected by means a convenience sampling strategy (Hufnagel & Conca, 1994). The nineteen participants have varied characteristics: 10 women, 9 men, average age 30.4; and various professions (administrative assistant, students, sales manager, trainee, etc.). All participants are located in the Ile-de-France region of France. The number of participants was determined through the principle of theoretical saturation. That is, we conducted interviews until we arrived at the point of theoretical saturation, when no new themes were emerging from the data (Strauss & Corbin, 1990).

We used an interview guide that included questions about respondents' perceptions, concerns and expectations related to the IoT. This was structured in three parts. The first part began with general questions about the respondents' expertise and use of new technologies and their knowledge of the IoT (e.g. "Please tell me about your use of new technologies). In the second part, we showed respondents a video produced by a specialized agency that shows an example of a smart service. Given the recent emergence of smart services and their relatively low diffusion rate in France, the video was intended to help respondents understand how a smart service works. The video shows banking and financial transactions being carried out through various smart devices (for example, making an appointment with a bank advisor from a connected watch, payment by means of a connected bracelet, consulting bank accounts on domestic devices, the remote signing of a contract). After they had viewed the video, respondents were asked open-ended questions (e.g. What do you think about this smart service?, Do you have any concerns regarding smart services? If so, what are they?).

Based on this initial qualitative study – a thematic analytic approach was used to analyze the data (Braun and Clarke 2006) –, we identified several concerns² expressed by consumers about smart services. In line with our research objective, we focused primarily on privacy,³ identifying four such concerns expressed by the informants: a concern for individual privacy, perceived intrusion, secondary use of personal information, and the Big Brother effect (Table 2).

²Examples of concerns expressed by consumers but not addressed in this research: economic cost, loss of control, etc.

³ Note that two participants did not clearly express any privacy concerns.

Table 2. Findings of the preliminary study

The concern for privacy construct.	Description of concern	Examples of verbatim comments
Information privacy	An individual variable that characterizes: - the individual's desire for better protection of his or her privacy. - a high concern for privacy	"What bothers me is the fact of tracking consumers, the fact of collecting all this data (...) I'm not reassured by so much personal information collection and I'm afraid it's going to get worse. Today we're being geolocated and tomorrow what?" (R5)
Perceived intrusion	Concern related to the fear: - of the ability of connected objects to penetrate consumers' private lives without permission - that the company may access information related to personal activities - of smart products being used to send spam	"The intrusive side is like pop-ups, cookies, it's really, purely intrusive, you leave a trace of everything you do, it's studied to be able to orient you on precise choices (...) I'm for advertising, but I say no to all the subliminal advertising messages bombarding you" (R3)
Unauthorized secondary use	Concern that information collected by smart products may be used: - by unauthorized entities - for other, non-consensual purposes - to select consumers according to their profiles (good vs. bad)	"I still have this concern about the security and confidentiality of my accounts. If I ever get my smart watch stolen, which allows me to be identified when I enter the agency, the thief could pretend to be me" (R12) "I need to be sure that the data is not lost anywhere, and that it is not used for bad purposes. And that's complicated to handle" (R16)
Big Brother effect	An individual tendency to perceive that: - the world is under generalized surveillance - individuals have lost control over their choices - there is a system where unknown entities spy on and manipulate citizens - digital multinationals use data to observe individuals.	"You're completely geolocated, followed everywhere, it's the Big Brother thing [about the connected bank service shown on the video]. It's horrible! It's horrible!" (R6) "I feel like I'm being watched and manipulated because of all the information they have about me" (R11)

We integrated these four privacy concerns into our theoretical model (Figure 1). In the following section we formulate our hypotheses.

Framework and hypotheses

In line with previous research (Smith et al., 1996; Miyazaki & Fernandez, 2001; Malhotra et al., 2004; Xu et al., 2012), we propose to study perceived intrusion, the importance of information privacy, the unauthorized secondary use of personal information, and the fear of a Big Brother effect as privacy concerns. Drawing on the theory of resistance to innovation (Ram and Sheth, 1989), we consider these concerns as barriers that positively impact consumer resistance to smart services. We now explain the different variables of our model.

Information privacy

Information privacy refers to an individual variable that depicts a high concern for privacy and a desire to exercise control over personal data (Bélanger and Crossler, 2011). The proliferation of new technologies has accentuated consumers' privacy concerns (Inman and Nikolova, 2017). Several studies have highlighted the importance of this individual variable in explaining consumers' behaviors, attitudes and intentions in a virtual transaction context. Lancelot-Miltgen et al. (2016) have pointed out that privacy concerns have a positive impact on risk perception and a negative impact on trust in IT innovations, while Eastlick et al. (2006) found that privacy concerns negatively impact purchase intentions.

Because of their ubiquitous nature, smart products are expected to be present in the daily lives of consumers and likely to exacerbate their feeling of invasion of privacy (Mani & Chouk, 2017). Individuals who attach great importance to protecting their privacy will naturally tend to reject services that use these smart technologies. For example, in the context of smart homes, previous studies have found that privacy risk limits the perceived value (Kim et al.,

2017) and increases consumer resistance to such a service (Hong et al., 2017). We therefore put forward the following hypothesis.

H1. Information privacy concern has a positive impact on consumer resistance to smart services.

Perceived intrusion

According to several authors, intrusion is closely linked to the idea of the violation of personal space (Xu et al., 2012). In this sense, Morimoto and Macias (2009, p. 139) emphasize that intrusion is a facet of privacy concern and refer to the “individual’s right to be left alone and/or freedom from ‘unwanted intrusions of others’”. In other words, intrusion involves a perception of a harmful incursion into the space of personal information and is a fundamental component of privacy concern (Xu et al., 2012).

Previous research shows that the more companies’ marketing practices are perceived as irritating, intrusive or annoying, the lower the probability that consumers will give permission for interactive marketing activities (Krafft et al., 2017). In their study of smart services in healthcare, Wiegard and Breitner (2017) identify perceived intrusion as a construct of mobile user information privacy concerns that has a positive impact on the perception of privacy risks. These privacy risk factors override the perceived value of using the smart health service. Similarly, Mani and Chouk (2017) point out that perceived intrusiveness, defined as the preoccupation with the entry of smart products into the consumer’s private life without permission, positively impacts resistance to these products. We thus put forward the following hypothesis.

H2. Perceived intrusion has a positive impact on consumer resistance to smart services.

Unauthorized secondary use of personal information

Secondary use generally refers to “the practice of using data for purposes other than those for which they were originally collected” (Bélanger and Crossler, 2011, p. 1018). Indeed, to interact with a company, the consumer increasingly has to use virtual channels (e.g. internet banking, mobile shopping) that collect, use and store private information of various kinds (e.g. names, addresses, lifestyle characteristics and purchasing habits) (Lwin and Williams 2003). This requirement increases the risk of unauthorized secondary use, where “information is collected from individuals for one purpose but is used for another, secondary purpose without authorization from the individuals” (Smith et al. 1996, p. 171). For example, when purchasing on the internet, the buyer provides the company with his/her postal address for delivery, which is then used by the company to send targeted advertisements to the consumer’s home. Similarly, smart services may present privacy threats with regard to the re-use of consumers’ data (Hsu & Lin 2016). IoT devices have the capacity to continuously collect and store sensitive information (e.g. geographical location, financial data). This information may be automatically transmitted to supply databases belonging to the company or to external parties without the consumer’s consent. In the IoT context, Hsu and Lin (2016) identify a negative link between privacy concerns about IoT services, including unauthorized secondary use of personal information, and the continued intention to use such services. It can therefore be assumed that unauthorized secondary use constitutes a barrier that increases consumer resistance. Thus:

H.3. Unauthorized secondary use of personal information has a positive impact on consumer resistance to smart services.

The Big Brother effect

The term ‘Big Brother’, which has entered everyday language, originates from George Orwell’s novel *Nineteen Eighty-Four*. Big Brother is a fictitious character, a figure of the totalitarian state and extreme control of freedom and privacy, whose motto “Big Brother is

watching you” reminds every citizen of his omnipresence and power. This Orwellian vision is increasingly in evidence today and the term ‘Big Brother’ is considered by Sarpong and Rees (2014, p. 217) to be the most commonly used contemporary metaphor for describing surveillance and “any activity that seeks to curtail the freedom of individuals or society as a whole”. In the 1980s and 1990s, with the proliferation of computer use at work, several authors had already used the term “Big Brother Syndrome”, in reference to “a growing fear of computer monitoring and controlling people’s lives” (Rosenfeld et al., 1996, p. 266). More recently Zuboff (2015) has warned of the danger of a new world of “surveillance capitalism” and a “Big Other” which “is a ubiquitous networked institutional regime that records, modifies, and commodifies everyday experience from toasters to bodies, communication to thought, all with a view to establishing new pathways to monetization and profit. Big Other is the sovereign power of a near future that annihilates the freedom achieved by the rule of law” (Zuboff, 2015, p. 81).

In line with this Orwellian perspective, we propose the concept of the ‘Big Brother effect’, defined as the perception by the individual of a world subject to monitoring and control by known or unknown, visible or invisible entities that possess specific and above-average technical powers. The concept refers to the idea that the individual constantly lives with the thought that everything he or she does will be recorded somewhere in a digital file by powerful entities. In the minds of consumers, such entities may be private or public organizations (e.g. multinational computer companies, state surveillance organizations).

The growing number of scandals related to the leaking of personal data and the surveillance of citizens by state or private organizations (e.g. the PRISM internet surveillance set up by the NSA [Kuner et al., 2013], the Sesame Credit Consumer scoring Program in China [Kostka, 2019]) contributes to the suspicion and fear of an Orwellian world. Various new technologies, including smart products, may be perceived by consumers as a threat to their individual

freedoms and the right to privacy. Indeed, with connected objects and mobile applications, organizations can now access, store and analyze consumer information in real time, allowing them to refine their knowledge of consumer habits (Wunderlich et al., 2015). Through their ubiquity, autonomy and intelligence, smart products “raise privacy issues since they can put consumers under constant surveillance” (Mani & Chouk, 2017, p. 80). In this context, Xu et al. (2009, p.137) note that “the Big Brother imagery looms in the popular press”, in which the impact of new technologies on privacy is often discussed. We can therefore assume that the BBE increases concerns for privacy. We propose the following hypotheses.

H4. The Big Brother effect has a positive impact on concern about information privacy

H5. The Big Brother effect has a positive impact on concern about unauthorized secondary use of personal information

H6. The Big Brother effect has a positive impact on perceived intrusion

Moreover, the information systems literature suggests that the perception of Big Brother surveillance is leading to stress, fatigue and decreased job performance (Rosenfeld et al., 1996). In line with this research, we assume that the BBE can lead to a negative consumer reaction towards smart services and thus promote resistance to them. Thus:

H7. The Big Brother effect has a positive impact on consumer resistance to smart services.

Figure 1. Theoretical framework and hypotheses

Methodology

Procedure and sample

Panel members of a French research company, representative for the French population in terms of gender and age, were asked to fill out an online questionnaire regarding smart services in the banking sector. Indeed, smart banking service is an area with a high potential for development (MarketandMarket, 2017). For the data analysis, 653 completed questionnaires were used.

The participants were shown a video presenting real examples of smart services (this is the same video used for the qualitative study). We introduced filter questions to check the correct functioning of sound and image on the equipment used by the respondents. After watching the video, participants were asked to answer several sets of questions on several themes: their perception of the smart bank service, their perception of IoT devices in general, their personality, and their socio-demographic characteristics.

Respondents were located in different regions in France. 54% of respondents are women. The average age is 42 years. Various socio-professional categories were represented: farmers,

business owners, unemployed, students, retired, etc. (for more details regarding methodology, refer to Mani and Chouk (2018).

Measures

Participants responded to a series of multi-item 7-point Likert measures ranging from ‘completely disagree’ (1) to ‘completely agree’ (7). Unauthorized secondary use of personal information was measured with the scale of Smith et al. (1996). To measure perceived intrusion, we adapted the Xu et al. (2008) scale. To measure information privacy concerns, we were inspired by the scales of Malhotra et al. (2004) and Smith et al. (1996). Regarding the BBE, no research has explicitly measured this. The measures were therefore grounded on the Orwellian view of Big Brother, including elements related to a powerful figure. Specifically, two items (BBE1 and BBE2) were written by the researchers on the basis of the exploratory study previously presented, and two items (BBE3 and BBE4) were adapted from the conceptual and qualitative work of Galič et al., (2016), Sarpong and Rees (2014), and Zuboff (2015). In line with our definition of BBE, this construct is operationalized in terms of the capacity of new technologies to monitor and spy on consumers in a visible or invisible manner. Despite our using new measures for the BBE construct, the indicators of reliability and validity are satisfactory ($\alpha = 0.92$, CR = 0.92, AVE = 0.75). Consumer resistance to smart services was measured through the Heidenreich and Spieth (2013) scale. These various scales are detailed in Table 3. Table 4 shows satisfactory reliability coefficients for all the scales of the model.

Table 3. Scale measurement

Scale	Code	Item	Mean	SD
Information privacy	INP1	I'm concerned about threats to my personal privacy	5.5	1.53
	INP2	I'm concerned about data collected by the smart banking service without my permission		
	INP3	I'm concerned about the use of my personal data without my consent.		
Perceived intrusion	PIN1	I feel that as a result of my using smart banking service, others know about me more than I am comfortable with	5.1	1.58
	PIN2	I believe that as a result of my using smart banking service, information about me that I consider private is now more readily available to others than I would want		
	PIN3	I feel that as a result of my using smart banking service, information about me is out there that, if used, will invade my privacy		
	PIN4	I think the smart banking service can be intrusive (new)		
Unauthorized secondary use	USU1	I am concerned that the smart banking service may use my personal information for other purposes without notifying me or getting my authorization	5.39	1.56
	USU2	When I give personal information to use the smart banking service, I am concerned that apps may use my information for other purposes.		
	USU3	I am concerned that the smart banking service may share my personal information with other entities without getting my authorization		
Big Bother effect	BBE1	I think that with new technologies, citizens are increasingly being spied on	5.31	1.50
	BBE2	I think that new technologies reinforce the power to monitor citizens without their knowledge		
	BBE3	I think the world is under general surveillance		
	BBE4	I think unknown entities use new technologies to observe citizen		
Resistance	RES1	I have a negative opinion about the smart banking service	3.85	1.93
	RES2	I'm not in favor of the smart banking service		
	RES3	I have a bad judgment on the smart banking service		

Psychometric quality of constructs

Convergent and discriminant validity

A confirmatory factor analysis using AMOS software was carried out. This analysis showed that all items for the independent variables and the dependent variable loaded highly on the respective constructs. Furthermore, convergent validity and discriminant validity of the constructs were checked according to the procedure suggested by Fornell and Larcker (1981). To assess the convergent validity of our concepts, we verified two conditions: the link between the latent variable and each of its indicators must be significant and the average variance extracted must be greater than 0.5 (table 4).

Table 4. Reliability and convergent validity

Latent variables	Cronbach's alpha (α)	Construct Reliability	AVE	Items Code	Loadings	p-value
Information Privacy	.97	.96	.90	INP1	.97	
				INF2	.95	.000
				INF3	.93	.000
Perceived intrusion	.94	.94	.80	PIN1	.91	
				PIN2	.93	.000
				PIN3	.91	.000
				PIN4	.82	.000
Unauthorized secondary use	.95	.96	.88	USU1	.95	
				USU2	.93	.000
				USU3	.94	.000
Big Brother Effect	.92	.92	.75	BBE1	.93	
				BBE2	.91	.000
				BBE3	.84	.000
				BBE4	.77	.000
Resistance	.96	.96	.88	RES1	.95	
				RES2	.90	.000
				RES3	.97	.000

AVE: Average Variance Extracted

The discriminant validity of the latent variables was tested by demonstrating that the variance that each construct shares with its items is greater than the variance it shares with the other constructs (table 5).

Table 5. Discriminant validity

Construct	1	2	3	4	5	Square root of AVE
1. Information privacy	1					.95
2. Perceived intrusion	.43	1				.92
3. Unauthorized Secondary use	.69	.54	1			.94
4. Big Brother effect	.51	.45	.67	1		.86
5. Resistance	.35	.39	.42	.33	1	.94

Common method bias

We tested the common method variance (CMV) with the unmeasured latent method factor technique (Podsakoff et al. 2003). A comparison of the fit of two models (one with and the other without the unmeasured latent factor) using a chi-square difference test ($\Delta\chi^2 = 280.97$; $p < 0.001$) indicated that the model without the unmeasured latent factor had a better fit. This suggests that the common method variance does not pose a threat of bias to the relationships in our model.

Multicollinearity

To assess multicollinearity, we examined the variance inflation factor (VIF). Results show the highest value of VIF is 2.8 (< 10). Hence, we can conclude that multicollinearity is not an issue for our model (Hair et al., 1995). Moreover, the examination of the correlation matrix does not show very high correlations for the independent variables.

Test of the research model

To test our theoretical model, a structural equation modelling (AMOS) was used (Figure 2). The fit indices for the model suggest a good overall model fit (Hair et al., 2006): $\chi^2 = 483.39$, $df = 112$, comparative fit index (CFI) = 0.97, Tucker-Lewis index (TLI) = 0.96, incremental fit index (IFI) = 0.97 and root mean square area of approximation (RMSEA) = 0.07. The

results indicate that information privacy has a significant positive impact on consumer resistance to smart services ($\beta = 0.13$, $CR = 2.19$, $p = 0.03$). Hypothesis H1 is therefore confirmed. Hypothesis H2 is supported since the effect of perceived intrusion on consumer resistance to smart services is significant ($\beta = 0.28$, $CR = 5.32$, $p < .001$). Moreover, unauthorized secondary use of personnel information has a positive significant effect on consumer resistance to smart services ($\beta = 0.30$, $CR = 4.19$, $p < .001$). This result supports H3. Hypothesis H4 is supported since the effect of the BBE on information privacy is statistically significant ($\beta = 0.61$, $CR = 16.95$, $p < .001$). The BBE has a significant positive impact on perceived intrusion ($\beta = 0.55$, $CR = 13.50$, $p < .001$) and on unauthorized secondary use of personnel information ($\beta = 0.81$, $CR = 23.98$, $p < .001$). Our results confirm hence H5 and H6. Finally, the impact of the BBE on consumer resistance is not significant, H7 is then not supported ($p > .05$).

Figure 2. Results

Discussion

The aim of our research is to study consumers' reactions to smart services from a privacy perspective. To this end, we have proposed a model identifying privacy concerns as antecedents to resistance to smart services. More specifically, in line with previous research (e.g. Hsu and Lin, 2016), our research confirms the positive link between perceived intrusion

and negative consumer's reaction to innovation. In other words, the fear of companies violating consumers' privacy is an obstacle to the acceptance of smart services. In addition, our research contributes to past work by examining the impact on consumer resistance of the unauthorized secondary use of personal information. This variable was found to be the antecedent with the greatest impact on resistance to smart services ($\beta=.30$). Indeed, consumers are concerned about the communication of their data to other entities without their consent. Regarding the concern for privacy of information, our results highlight the positive effect of this variable on resistance to innovation. While Mani and Chouk (2017) identified an indirect effect of this variable on resistance to innovation (through perceived intrusion), our model empirically confirms a direct positive relationship. This result is in line with the work of Eastlick et al. (2006), who identified a direct effect of privacy information concern on purchase intent regarding a services e-tailer.

In addition, our results highlight a significant positive impact of the BBE on the three privacy concerns. Our research contributes to the technology innovation literature by providing an empirical evidence of the impact of the BBE on privacy information concern, the unauthorized secondary use of personal information and perceived intrusion. In other words, our research identifies BBE as a central variable to understand the growing concerns of consumers about the proliferation of new technologies in their lives. This completes the work of the authors who evoked the importance of taking into account the fear of an Orwellian schema to understand the decision process of individuals (e.g. Rosenfeld et al., 1996; Sarpong & Rees, 2014).

Unexpectedly, the direct impact of the BBE on consumer resistance to smart services was not significant. This impact seems to be only indirect (via the other three privacy concerns), a finding that may be accounted for by the fact that the BBE is based on consumers' impression of being spied on and rarely on tangible proofs. Consequently, consumers do not base their

decision to resist or not to resist on this variable. This result confirms the complex role of BBE as a psychological variable in explaining consumer resistance to innovation. Indeed, previous research has failed to identify the direct impact of certain psychological variables such as perceived risk on consumer resistance to innovation (Laukkanen, 2016).

Implications for research

From a theoretical standpoint, our research has two implications. First, to the best of our knowledge, it is the first to study resistance to innovation from a privacy perspective. Most previous research has examined resistance to innovation on the basis of models integrating a variety of barriers (e.g. Laukkanen, 2016), whereas our study focuses primarily on barriers related to various consumer privacy concerns. This perspective is interesting particularly when the innovation is in its first stage of development. Indeed, faced with an innovation that they have never (or not yet) used, consumers base their perception on their own predispositions to resist change. According to the status quo bias theory (Samuelson & Zeckhauser, 1988; Kim & Kankanhalli, 2009), resistance to innovation can be explained by an individual predisposition to reject any novelty, because it generates more risks than benefits. Thus, in a context where consumers perceive significant privacy risks, they prefer the status quo in order to minimize losses. This perspective of studying resistance through the lens of privacy therefore enriches the emerging research on resistance to innovation in services (Hazée et al., 2017; Laukkanen, 2016).

The second theoretical contribution of this study is to define the BBE and to provide an empirical evidence of its impact on the information privacy, the unauthorized secondary use of personal information and the perceived intrusion. This original variable enriches existing research on privacy concerns. Drawing on Orwell's dystopian vision and Zuboff's (2015) theoretical framework, BBE offers a theoretical perspective adapted to a new context of the proliferation of smart technologies and the growing use of big data. While in existing

research, the idea of big brother is often conceptually mentioned in an organizational context (Rosenfeld et al., 1996; Sarpong & Rees, 2014), our research is the first to our knowledge to provide an empirical evidence of the importance of this concept in a consumer context.

Implications for practice

Privacy concerns are one of the major issues facing companies today. Our results show that these concerns can become inhibitors to the acceptance of smart services. Based on our results, we suggest managerial practices that can address these concerns. First, we propose a strategy based on promoting the company's ethical values, which may involve greater transparency in the management of consumers' personal data. Consumers must be able to understand clearly how their data is managed, stored and protected. Companies could therefore adopt a personal data privacy charter. For example, an insurance company in France (MAIF) has adopted a charter "for a humane and ethical digital world"⁴ that contains a number of principles, including respect (the company undertakes not to sell personal data), transparency (the company undertakes to inform each customer of the origin, content and use of personal data), security (the company undertakes to host personal data in France or within the European Union), and forgetting (customers may ask for that their personal data to be deleted at any time). In the same vein, companies could acquire "privacy protection" labels in partnership with independent organizations. In France, for example, the CNIL (French National Commission for Information Technology and Civil Liberties), an independent public organization, offers certification in accordance with GDPR legislation⁵ (General Data Protection Regulation). Furthermore, engineering schools, universities and business schools have a role to play for better privacy protection. It would be interesting, for example, to run more courses related to ethics in students' educational programs.

⁴ <https://entreprise.maif.fr/entreprise/pour-une-societe-collaborative/decouvrir-nos-actions/maitriser-les-enjeux-numeriques/chartenumerique>

⁵ <https://www.cnil.fr/fr/les-labels-cnil>

Secondly, companies need to develop a relational strategy to address concerns related to the Big Brother effect. The aim here is to provide answers to the various consumer questions related to the data collected by the IoT, artificial intelligence, mobile apps, and so on. In this respect, companies should strengthen their online presence management so as to interact with customers on social networks, for example. The role of online presence management would be to respond to accusations, prejudices and fake news about the management of personal data. Finally, in terms of public policy, governments should strengthen privacy laws and provide better protection for whistleblowers who expose consumer mass surveillance.

Conclusion

Previous work on the adoption of innovations has been criticized for neglecting factors that lead to the rejection of innovation (Kleijnen et al., 2009), notably in the area of services (Hazée et al. 2017;). The present study contributes to a better understanding of the factors that explain consumer resistance to smart services from a privacy perspective. The findings show that resistance to smart services is directly influenced by various privacy concerns: information privacy, the unauthorized secondary use of personal information and perceived intrusion. In addition, our research highlights the major role of BBE as an antecedent to these consumers' various privacy concerns.

Despite the interest of studying the role of these different consumer concerns, it is important to consider them in combination with the perceived benefits of smart services. For example, Roy et al. (2018) highlight the role of the benefits of innovation in determining customer acceptance of smart retail technology. More specifically, these authors emphasize that the characteristics of innovation (i.e. perceived usefulness, perceived ease of use, and perceived adaptiveness) are perceived as advantages leading to favorable attitudes and behavioral intentions. For their part, Wiegard and Breitner (2017) hypothesize that consumers' decisions to adopt a smart service in healthcare are determined by their trade-offs between perceived

benefits and perceived privacy risks (privacy calculus). In other words, the use of wearable health devices has benefits in terms of improving health management (i.e. perceived usefulness), enhancing experience (i.e. perceived enjoyment) and reducing effort (i.e. effort expectancy). A favorable trade-off between these benefits and privacy risks increases the perceived value and promotes the adoption of smart services.

Accordingly, the privacy concerns identified in our research should be put in perspective together with the potential benefits. We can assume that, despite privacy concerns regarding smart banking, consumers can perceive benefits to this service, such as convenience, just-in-time promotions, and personalization. Thus, in accordance with privacy calculus theory (Culnan & Armstrong, 1999), consumers would accept making concessions with regard to their privacy if, in return, they perceive/receive significant benefits. To strengthen their customers' choice and reinforce its brand reputation, it is important for banks to be more transparent, diligent, and secure in the management of private data. Indeed, the offers proposed by companies perceived as "secure" or "trustworthy" with regards to consumers' information privacy are more likely to be accepted by buyers (Inman & Nikolova, 2017).

Furthermore, while this study contributes to the literature on resistance to innovation, some limitations has to be addressed by future research. First, the specific application context of our research is the banking sector, which limits the generalizability of our findings to other smart service sectors (e.g. smart homes, smart cities, insurance). Although this context has been chosen in several previous studies for studying consumer resistance to a new service (e.g. Laukkanen, 2016), some of the issues described are not necessarily found in other sectors. Second, our research focuses on four main privacy concerns as antecedents to resistance. Other factors such as improper access and errors (Smith et al., 1996) could also explain consumer resistance as well as the perception of a "privacy calculus" (potential benefits versus potential risks of data disclosure). Similarly, the model could be

enriched by considering, for example, the moderating role of individual variables: perception of the global impact of the technology, self-efficacy and technology anxiety, among other considerations. Finally, the conceptualization of BBE can be enriched by taking into account contextual variables. Consumers may have different perceptions of BBE depending on the cultural context, media coverage of certain scandals and the role of the mass media.

References

- Balta-Ozkan, N., Davidson, R., Bicket, M., & Whitmarsh, L. (2013). Social barriers to the adoption of smart homes. *Energy Policy*, 63, 363–374. doi:10.1016/j.enpol.2013.08.043
- Bélanger, F. & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly*, 35(4), 1017-1041. doi:10.2307/41409971
- Braun, V. & Clarke V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77-101. doi:10.1191/1478088706qp063oa
- Ching, K. W. & Singh, M. M. (2016). Wearable technology devices security and privacy vulnerability analysis. *International Journal of Network Security & Its Applications*, 8(3), 19–30. doi:10.5121/ijnsa.2016.8302
- Corbin, J.M. & Strauss, A., 1990. Grounded theory research: Procedures, canons, and evaluative criteria. *Qualitative Sociology*, 13(1), 3–21. doi:10.1007/bf00988593
- Culnan, M. J. & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, 10(1), 104–115. doi:10.1287/orsc.10.1.104
- Davis, F. D. 1989. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3): 319-339. doi:10.2307/249008
- Eastlick, M. A., Lotz, S. L., & Warrington, P. (2006). Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment. *Journal of Business Research*, 59(8), 877–886. doi:10.1016/j.jbusres.2006.02.006
- Fornell, C. & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, 18(1), 39-50. doi:10.1177/002224378101800104

- Foroudi, P., Gupta, S., Sivarajah, U., & Broderick, A. (2018). Investigating the effects of smart technology on customer dynamics and customer experience. *Computers in Human Behavior*, 80, 271–282. doi:10.1016/j.chb.2017.11.014
- Galič, M., Timan, T., & Koops, B.-J. (2016). Bentham, Deleuze and Beyond: An overview of surveillance theories from the Panopticon to participation. *Philosophy & Technology*, 30(1), 9–37. doi:10.1007/s13347-016-0219-1
- Hair, J.F.Jr., Anderson, R.E., Tatham, R. L. & Black, W.C. (1995). *Multivariate data analysis* (3rd ed). New York: Macmillan.
- Hair, J.F.Jr., Black, W.C., Babin, B.J., Anderson, R.E. & Tatham, R.L. (2006). *Multivariate data analysis*, Pearson Prentice Hall, NJ: Upper Saddle River.
- Hazée, S., Delcourt, C., & Van Vaerenbergh Y. (2017), Burdens of access: Understanding customer barriers and barrier-attenuating practices in access-based services, *Journal of Service Research*, 20(4), 441–456. doi:10.1177/1094670517712877
- Heidenreich, S. & Spieth, P. (2013). Why innovations fail — The case of passive and active innovation resistance. *International Journal of Innovation Management* 17(5), 1-42. doi:10.1142/s1363919613500217
- Hong, A., Changi, N., & Seongcheol, K. (2017). Analysis of the barriers that consumers encounter when smart home service is introduced in South Korea. *14th International Telecommunications Society (ITS) Asia-Pacific Regional Conference: "Mapping ICT into Transformation for the Next Information Society*, Kyoto, Japan, 24-27 June.
- Hsu, C-L. & Lin J.C-C. (2016), Exploring factors affecting the adoption of internet of things services, *Journal of Computer Information Systems*, 58(1), 49-57.
- Hufnagel, E. M., & Conca, C. (1994). User response data: The potential for errors and biases. *Information Systems Research*, 5(1), 48–73. doi:10.1080/08874417.2016.1186524
- Inman, J.J. & Nikolova, H. (2017). Shopper-facing retail technology: A retailer adoption decision framework incorporating shopper attitudes and privacy concerns. *Journal of Retailing*, 93(1), 7-28. doi:10.1016/j.jretai.2016.12.006
- Juric, J., & Lindenmeier, J. (2018). An empirical analysis of consumer resistance to smart-lighting products. *Lighting Research & Technology*, 51(4), 489–512. doi:10.1177/1477153518774080
- Kim, H.W. & Kankanhalli, A. (2009). Investigating user resistance to information systems implementation: A status quo bias perspective. *MIS Quarterly* 33, 567-582. doi:10.2307/20650309

- Kim, Y., Park, Y., & Choi, J. (2017). A study on the adoption of IoT smart home service: using Value-based Adoption Model. *Total Quality Management & Business Excellence*, 28(9-10), 1149–1165. doi:10.1080/14783363.2017.1310708
- Kleijnen, M., Lee, N.J. and Wetzels, M. (2009). An exploration of consumer resistance to innovation and its antecedents. *Journal of Economic Psychology*, 30(3), 344-357. doi:10.1016/j.joep.2009.02.004
- Kostka, G. (2019). China's social credit systems and public opinion: Explaining high levels of approval. *New Media & Society*, 21(7), 1565–1593. doi:10.1177/1461444819826402
- KPMG (2015). *The internet of things should we embrace its full potential?* Retrieved from <https://assets.kpmg/content/dam/kpmg/pdf/2016/05/Cyber-Insights-Magazine-The-Internet-of-Things.pdf>
- Krafft, M., Arden, C. M., & Verhoef, P. C. (2017). Permission marketing and privacy concerns — Why do customers (not) grant permissions? *Journal of Interactive Marketing*, 39, 39–54. doi:10.1016/j.intmar.2017.03.001
- Kuner, C., Cate, F. H., Millard, C., & Svantesson, D. J. B. (2013). PRISM and privacy: will this change everything? *International Data Privacy Law*, 3(4), 217–219. doi:10.1093/idpl/ipt020
- Lancelot-Miltgen, C., Henseler, J., Gelhard, C., & Popovič, A. (2016). Introducing new products that affect consumer privacy: A mediation model. *Journal of Business Research*, 69(10), 4659–4666. doi:10.1016/j.jbusres.2016.04.015
- Laukkanen, T. (2016). Consumer adoption versus rejection decisions in seemingly similar service innovations: The case of the Internet and mobile banking. *Journal of Business Research*, 69, 2432-2439. doi:10.1016/j.jbusres.2016.01.013
- Lichy, J., Kachour, M., & Khvatova, T. (2017). Big Data is watching YOU: opportunities and challenges from the perspective of young adult consumers in Russia. *Journal of Marketing Management*, 33(9-10), 719–741. doi:10.1080/0267257x.2017.1313301
- Lim, C. & Maglio, P. P. (2018). Data-driven understanding of smart service systems through text mining. *Service Science*, 10(2), 154–180. doi:10.1287/serv.2018.0208
- Lwin, M. O., & Williams, J. D. (2003). A model integrating the multidimensional developmental theory of privacy and theory of planned behavior to examine fabrication of information online. *Marketing Letters*, 14(4), 257-272. doi:10.1023/b:mark.0000012471.31858.e5

- Malhotra, N. K., Kim, S. S. & Agarwal J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, 15(4), 336-355. doi:10.1080/0267257x.2017.1313301
- Mani, Z. & Chouk, I. (2017). Drivers of consumers' resistance to smart products. *Journal of Marketing Management*, 33(1/2), 76–97. doi:10.1080/0267257x.2016.1245212
- Mani, Z. & Chouk, I. (2018). Consumer resistance to innovation in services: Challenges and barriers in the Internet of Things era. *Journal of Product Innovation Management*, 35(5), 780-807. doi:10.1111/jpim.12463
- Marakhimov, A., and Joo, J. (2017). Consumer adaptation and infusion of wearable devices for healthcare. *Computers in Human Behavior*, 76, 135–148. doi:10.1016/j.chb.2017.07.016
- Margulis, S.T. (1977). Conceptions of privacy: Current status and next steps. *Journal of Social Issues*, 33(3), 5-21. doi:10.1111/j.1540-4560.1977.tb01879.x
- MarketandMarket, (2017). IoT in banking and financial services market by solution. Retrieved from <https://www.marketsandmarkets.com/Market-Reports/iot-banking-financial-services-market-172304505.html>
- Minerva, R. (2016). Toward a definition of Internet of Things, Retrieved from http://www.tlc.dii.univpm.it/blog/wp-content/uploads/2016/06/Course-DAY-3_b.pdf
- Miyazaki, A.D. & Fernandez, A. (2001). Consumer perceptions of privacy and security risks for online shopping. *Journal of Consumer Affairs*, 35(1), 27-44. doi:10.1111/j.1745-6606.2001.tb00101.x
- Morimoto, M., & Macias, W. (2009). A Conceptual framework for unsolicited commercial e-mail: Perceived intrusiveness and privacy concerns. *Journal of Internet Commerce*, 8(3-4), 137–160. doi:10.1080/15332860903467342
- Novak, T.P. and Hoffman, D.L. (2018). Relationship journeys in the Internet of Things: a new framework for understanding interactions between consumers and smart objects. *Journal of the Academy of Marketing Science*, 47(2), 216–237. doi:10.1007/s11747-018-0608-3
- Pantano, E., Priporas, C. V., & Dennis, C. (2018). A new approach to retailing for successful competition in the new smart scenario. *International Journal of Retail & Distribution Management*, 46(3), 264–282. doi:10.1108/ijrdm-04-2017-0080
- Park, K. & Koh, J. (2017). Exploring the relationship between perceived pace of technology change and adoption resistance to convergence products. *Computers in Human Behavior*, 69, 142–150. doi:10.1016/j.chb.2016.12.017

- Peñaloza L. and Price L. (1993). Consumer resistance: a conceptual overview, in L. McAlister et M. Rothschild (coord.), *Advances in Consumer Research*, 20, Provo, Utah, Association for Consumer Research, 123-128.
- Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, 88(5), 879–903. doi:10.1037/0021-9010.88.5.879
- Porter, M. E., & Heppelmann, J. E., (2014). How smart, connected products are transforming competition. *Harvard Business Review*, 92(11), 64-88.
- Ram, S. and Sheth, J.N. (1989). Consumer resistance to innovations: the marketing problem and its solutions. *Journal of Consumer Marketing*, 6(2), 5-15. doi:10.1108/eum0000000002542
- Rosenfeld, P., Booth-Kewley, S., Edwards, J. E., & Thomas, M. D. (1996). Responses on computer surveys: Impression management, social desirability, and the Big Brother syndrome. *Computers in Human Behavior*, 12(2), 263–274. doi:10.1016/0747-5632(96)00006-4
- Roux, D. (2007). Consumer resistance: Proposal for an integrative framework. *Recherche et Applications En Marketing* (English Edition). 22(4), 59–79. doi:10.1177/205157070702200403
- Roy, S.K., Balaji, M.S., Quazi, A., & Quaddus, M. (2018). Predictors of customer acceptance of and resistance to smart technologies in the retail sector. *Journal of Retailing and Consumer Services*, 42, 147–160. doi:10.1016/j.jretconser.2018.02.005
- Roy, S.K., Balaji, M.S., Sadeque, S., Nguyen, B., & Melewar, T. C. (2017). Constituents and consequences of smart customer experience in retailing. *Technological Forecasting and Social Change*, 124, 257–270. doi:10.1016/j.techfore.2016.09.022
- Samuelson, W. & Zeckhauser, R. (1988). Status quo bias in decision making. *Journal of Risk and Uncertainty*, 1, 7-59. doi:10.1007/bf00055564
- Sarpong, S., & Rees, D. (2014). Assessing the effects of “Big Brother” in a workplace: The case of WAST. *European Management Journal*, 32(2), 216–222. doi:10.1016/j.emj.2013.06.008
- Slettevåg, D. (2009). RFID-the “Next Step” in consumer-product relations or Orwellian nightmare? Challenges for research and policy. *Journal of Consumer Policy*, 32, 219-244. doi:10.1007/s10603-009-9103-z
- Smith, H.J., Milberg, J.S., & Burke, J.S. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*, 20(2), 167-196.

- Venkatesh V., Thong, J. & Xu, X. (2012). Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. *MIS Quarterly* 36(1): 157–178. doi:10.2307/41410412
- Wiegard, R-B., & Breitner M. H. (2017). Smart Services in Healthcare: A Risk-Benefit-Analysis of Pay-as-You-Live Services from Customer Perspective in Germany. *Electronic Markets*, 29(1), 107–123. doi:10.1007/s12525-017-0274-1
- Wunderlich, N.V., Heinonen, K., Ostrom, A.L., Patricio, L., Sousa, R., Voss, C., & Lemmink, J.G.A.M. (2015). ‘Futurizing’ smart service: implications for service researchers and managers. *Journal of Services Marketing*, 29(6/7), 442–447. doi:10.1108/jsm-01-2015-0040
- Xu, H., Dinev, T., Smith, H.J., & Hart, P. (2008). Examining the formation of individual's information privacy concerns: Toward an integrative view. *Proceedings of 29th Annual International Conference on Information Systems (ICIS 2008)*, Paris, France.
- Xu, H., Gupta, S., Rosson, M. B., & Carroll, J. M. (2012). Measuring mobile users’ concerns for information privacy. *Thirty Third International Conference on Information Systems: Association for Information Systems*, Orlando, USA.
- Xu, H., Teo, H.-H., Tan, B. C. Y., & 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), 135–174. doi:10.2753/mis0742-1222260305
- Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, 30(1), 75–89. doi:10.1057/jit.2015.5