LIBERA UNIVERSITÀ INTERNAZIONALE DEGLI STUDI SOCIALI

Department of Business and Management
Chair of Consumer Behavior

An exploration of barriers against IoT adoption across segments, and the influence of individual traits

Supervisor
Prof. Simona Romani

Co-Supervisor
Prof. Rumen Pozharliev

Candidate
Tina Marie Berg Toft

Student No.
700491

ACADEMIC YEAR
2017/2018

Acknowledgements

I would first like to thank my thesis supervisor Prof. Simona Romani at LUISS Guido Carli. I have received great support, help, and significant inputs throughout the entire thesis writing process. Her assistance cannot be appreciated enough.

I would also like to thank Ilaria Querci for her active interest and help. I have received great comments throughout the thesis writing process, which I am very grateful for.

Lastly, I am thankful for the managers who participated in my qualitative interviews, you provided great inputs from a practical perspective. I also want to thank everyone who participated in my research, especially people who conducted my first questionnaire as no rewards was given. Your participation provided the basis for this thesis' analyses which could not have been conducted without your participation.

Tina Marie Berg Toft
Roma, Italy
Thursday, June 14, 2018

Table of contents

Chapter 1: Introduction

Imagen a bicycle racer on a training ride for the world championship. On the way home, the bike's shifter mechanism for the rear gear gets a little unreliable, making it difficult to use the full range of gears. More energy than expected is required from the biker to cycle. Getting home is not an issue. However, the cyclist has two problems, repairing the shifter and getting a bit more nutritional fuel to maintain the desired quality of the ride. Using technology, the shifter may be repaired by using a bicycle internal diagnostic mechanism which identifies the problem with the shifter. After, the bicycle engages the internet and communicates the need for a shifter part to the rider's personal hub computer and database. The personal hub considers time to delivery, part cost, and other relevant factors and sends out an order or put out a bid request. The deal is made and the part is ordered. The second problem concerning nutritional fuel engages a different set of systems and processes. The biker is wearing clothing that keeps track of vital signs such as heart rate, hydration, body temperature, energy use, muscle strength, training zone, and foods processed. This information is processed in real time by insurance providers. A mapping system is monitoring current location and can find places to obtain food or beverages in addition to calculate the distance to a destination. The health system and mapping system coordinate in determining the additional energy needed by the rider and where to acquire nutrition to maintain the necessary energy level. A course to the retailer is mapped, as is the ensuing route back home (Weinberg, Milne, Andonova, & Hajjat, 2015). As you might notice, all the technical aspects of infrastructure and communications to seamlessly facilitate the scenario are currently not in place. However, many of the systems are actually available (Weinberg et al., 2015). In any matter this scenario is an illustration of what Internet of Things (IoT) is and what is possible with this technology.

IoT refers to the wireless connection of physical devices to the internet. Objects such as cars, kitchen appliances, and heart monitors can be connected through IoT. As the IoT grows in the next few years, more devices will be added to this list (Meola, 2016). Smart Objects are seen as the building blocks to IoT. Smart Objects are referred to as objects that can communicate with other Smart Objects, and can make decisions about themselves and their interactions with external entities (López, Ranasinghe, Harrison, & McFarlane, 2011). IoT is a revolutionary advance that brings the digital into the physical domain. Interactions is no longer just distributed virtually, but also everywhere in the real world, where people live, work, and play (D L. Hoffman & Novak, 2015). To further describe IoT's popularity, IoT has been identified as one of the emerging technologies in IT as noted in Gartner's IT Hype Cycle (Gubbi, Buyya, Marusic, & Palaniswami, 2013). The number of initiatives in the world taken by research organizations, industries, standardization bodies, and governments to bring IoT to a mass market, is significant (Borgia, 2014). Still, the growth of IoT has been much slower than expected. Glenn Stian Maeland (personal communication, March 13, 2018), product manager in Norway at Carlo Gavazzi which sells Smart House devices etc. said in an interview, that they have expected Smart Houses to emerge multiple times without it happening. However, the growth of IoT is expected to be huge in the future.

Problem

According to Hsu and Lin (2016), an increasing number of Smart Objects are connected to the internet. Many IoT services have been developed, and the global market for such services is growing rapidly. Despite the promising hype of IoT, adoption rates are low. Accenture's 2016 report, which studied 28 000 consumers in 28 countries, support this notion and stated that consumers demand is slow across a number of categories, and demand for devices enabled by IoT is not growing fast enough. During 2015 there was only a brief increase in purchase intention of IoT devices (Björnsjö, Viglino, & Lovati, 2016). According to D L. Hoffman and Novak (2015) only 16% of consumers own one device, and 4% own two or more devices (Gartner, 2014). Bradley, Barbier, and Handler (2013) also makes a similar conclusion, stating that 99.4% of physical objects are still unconnected, meaning that only 10 billion of the 1.5 trillion things globally are connected. Maeland (personal communication, March 13, 2018), stated that, in Norway it is built approximately 30 000 accommodations a year, and in 2011 only 11% of those accommodations had some kind of Smart Home installation. This shows the great potential of these installations. The slow pace of consumer adoption of new technologies is a major disappointment for the IoT industry (Mani & Chouk, 2016). It is stated that growth is stalling and IoT has not yet filled the gap (Björnsjö et al., 2016).

Assurant Inc's (2017) report state that US consumers are aware of nearly every category of connected technologies, however, adoption rates vary by category. Further, it would be difficult to reach a significant share of consumers, since 44% does not have any interest in owning Smart Devices. Sigbjorn Groven (personal communication, March 8, 2018), market and sales director at Future Home, a Norwegian Smart Home firm, similarly said in an interview that "adoption happens when consumer needs are clear ". He also pointed out that it is difficult for consumers to understand all the possibilities IoT have, and that this may be one reasons for why consumers to not adopt these devices. However, consumer expectations will grow due to IoT's presence in consumers' everyday lives. It is stated that consumers will insist on this technology through their purchases in the future (Acquity Group, 2014), which proves the importance of the research topic. It is forecasted that consumers will lag behind businesses and governments in IoT adoption, however, consumers will purchase a massive number of devices and invest a significant amount of money in IoT ecosystems in the future (Greenough, 2016). This is supported by Maeland (personal communication, March 13, 2018), which stated that the electro market is changing and that it will become normal to install alternative installations compared to today's conventional installations. Groven (personal communication, March 8, 2018), also gives an example of the huge growth they are expecting. Their goal is to sell 20 000 devices of smoke detectors in apartment blocks this year, until 08.03.18 the company had sold 1650 devices. Groven further states that people operating in in the market know that Smart Houses is going to be public domain, it is just a question of when the breakthrough is happening.

An increasing number of Smart Devices holds substantial promise for improving business processes and people's lives, but it will also lead to serious threats and technical challenges (Whitmore, Agarwal, & Da Xu, 2014). This is also discussed by Manyika et al. (2015), which emphasis that IoT offers considerable benefits as well as a new set of risks. It is expected that internet nodes may be located in everyday things, such as food packages, furniture and paper documents, by 2025. This highlights the future opportunities that will arise, and contribute to an economic development. The possible threats deriving from IoT are also stressed. Atzori, Iera, and Morabito (2010) emphasize that everyday objects will have security and privacy risk's, and that IoT could distribute those risk's far more widely than the internet to day does. Maeland (personal communication, March 13, 2018), assumes that consumers are not ready for this technology, because of the uncertainty surrounding it, and since IoT is expected to have a quick growth, in the future. A person does not want to invest a lot of money in a Smart House if the technology is outdated after five years, the consumers understand that there will be newer and better solutions in the future. Previous research found that US consumers have a significant amount of background anxiety about the connected world (Assurant Inc, 2017). Early adopters are tackling the challenges of data security, infrastructure, and skill sets necessary for the new data (O'Brien, 2017). While consumers in the early majority category to the laggard's category in the diffusion process are not (Rogers, 2010). This finding has also been reported in the Smart Home literature, where consumers concern are found to be one reason behind the slow adoption of the Smart Homes (Hong, Nam, & Kim, 2017). Many challenging issues, both technological and social still needs to be addressed before IoT will be widely accepted. This shows the importance of understanding and prohibiting barriers, as this thesis aims to do. This is in line with previous research which addresses the need to examine factors inhibiting the adoption process or causing rejection behavior (Laukkanen, 2016). This is important because many businesses face high production failure rates that stem from consumer resistance (Ram & Sheth, 1989).

Expected growth

Despite the slow growth of IoT, many are predicting that the economic impact of IoT will be huge. Estimates by many well respected organizations range widely. For instance, McKinsey Global Institute's 2013 report, identified twelve technologies that, by 2025, will have a massive economically impact. Of the Cyber-Physical Systems, IoT is expected to have the highest economic impact (Chui, Markus, & Roger, 2010). The same report's 2015 issue estimated that IoT has a total potential economic impact from 3.9 trillion dollars to 11.1 trillion dollars per year, by 2025 (Manyika et al., 2015). The Business Insider's report has forecasted that by 2020, 34 billion will be connected to the internet, whereas IoT devices will account for 24 billion. Additionally, 6 trillion dollars will be spent on IoT solutions each year from 2016 to 2021 (Greenough, 2016). A more optimistic prediction is made by IDC (2014), which states that the global IoT market will reach 7.1 trillion dollars in 2020. Further, Gartner (2014) has estimated that the number of IoT devices will grow from 900 million in 2009 to 26 billion in 2020. It is also found that wearables will contribute extensively to the expected growth, where number of smartphones, tablets and PCs is expected to reach 7.3 billion units by 2020 (Hsu & Lin, 2016). General Electric have predicted an even bigger growth of IoT devices and predicts that there will be 50 billion IoT devices in 2020, from 16 billion IoT devices in 2014. The same article further states that IoT can add as much as 15 trillion dollars to the global GDP by 2030 (Press, 2014; Weinberg et al., 2015). Borgia

(2014) states that each consumer will own 1000 devices by 2025. The amount invested in IoT technology and the rapid spread of connected devices highlight the great potential of the sector (Mani & Chouk, 2016; M. E. Porter & Heppelmann, 2014). IoT has been called the next industrial revolution, it will impact the way all business, governments and consumers interact with the physical world (Greenough, 2016). Several projects have been launched in the world since 2008, such as "Intelligent Earth" (US), "i2010" (EU), "i-Japan", and "To feel China". The latter has also identified IoT as one of five key emerging strategic industries (Hsu & Lin, 2016). The expected growth implies that it is important to understand the technologies, and acquire knowledge about why consumers adoption of IoT devices are slower than expected. It is first when companies know why consumers are not adopting IoT devices they can solve consumers issues, and ignite growth in this industry.

However, the growth of IoT will raise challenges and barriers. Despite the many forecasts of the great growth in the IoT industry, consumers do not adopt these devices in the extent to which is expected. For the IoT to reach these forecast's, barriers against IoT must be solved. Before companies can solve barriers against IoT adoption, there needs to be conducted research in this field. This thesis contributes to the literature by further exploring and mapping barriers against IoT adoption. Additionally, it is expected that individual traits may influence a consumer's decision to adopt or not. This will be analyzed through Parasurman's (2000) Technology Readiness Index. Based on this, the following research question is presented:

What are the barriers against IoT adoption? And do individual traits affect the adoption decision?

Scientific relevance

Internet of Things has been identified as one of the emerging technologies in IT, and several initiatives is initiated to bring IoT to market. IoT is evolving at a rapid pace, and the impact IoT will have is likely to be profound. As a result, there has been more research on IoT in the later years, with a boozed in 2014 (Russo, Marsigalia, Evangelista, Palmaccio, & Maggioni, 2015). Still, IoT is a fairly new field of study and there exists several gaps to fill. This thesis aims to fill some of these gaps, they are discussed in the following paragraph

Gap and contribution

The current literature regarding barriers against IoT adoption falls short in the following ways: First and foremost, this thesis contributes with a further exploration of barriers against IoT adoption. The selection of barriers is based on previous research mainly from the IoT and Smart Device literature (topic specific situational barriers). In addition, the innovation literature (non-topic specific situational barriers) has also been served as a basis for the selection of barriers where the IoT literature falls short. This thesis has an adoption view, were previous research also looks at consumer resistance (Mani & Chouk, 2016), purchase intention (Y. Chang, Dong, & Sun, 2014), and non-adoption resistance (Talke & Heidenreich, 2014). Since the research topic is relatively new, previous literature have mostly conducted qualitative research (Balta-Ozkan, Davidson, Bicket, & Whitmarsh, 2013; Brody & Pureswaran, 2015; Piwek, Ellis, Andrews, & Joinson, 2016), and few articles have a quantitative approach. Therefore, this thesis contributes to the literature with a recollection of barriers in a quantifying and organized way. In a few cases, previous literature regarding IoT have found evidence of barriers in a quantitative manner, then this thesis will serve as a replication of previous literature, and will contribute to the generalizability of previous results.

According to Laukkanen (2016), the mainstream research of technology adoption and acceptance involves technology implementation and use in the workplace. The consumer's view receives less attention. Additionally, few studies have focused on Smart Objects specifically, whereas the current literature have focused on one part of the domain, such as Smart Watches (Mani & Chouk, 2016), Smart Homes (Nakyung & Kim, 2015), or Smart Cars (Mallat, 2007). Several reports, such as Acquity Group (2014), Assurant Inc (2017), Accenture (Björnsjö et al., 2016), Cisco (Bradley et al., 2013), Business Insider (Greenough, 2016), and McKinsey Global Institute (Manyika et al., 2015) has discussed IoT and Smart Objects. These reports are not scientific research, but will still serve as a basis for the literature. To the best of my knowledge, there do not exist any previous scientific research that has tested the presence of barriers against IoT across segments. This is therefore a major contribution to the literature. The reasoning for doing this is the belief that some barriers will be present in every segment as an underling factor, and that some barriers will only be present in a few or one of the segments. Most research in the IoT field has mainly explored barriers, and hardy any research has tested for the individual trait's influence on barriers against IoT adoption. Both the innovation and technology literature have acknowledged that individual traits can influence adoption (Midgley & Dowling, 1978; Rogers, 2010).

Lastly, a more thorough investigation of the privacy and security barrier will be provided, where the aim is to solve the collection problem. The collection problem refers to the fact that some consumers allow companies to collect their personal information while other consumers do not. This additional investigation into one barrier will contribute to the literature as well, since little attempt have been made to solve the collection problem before. In this regard previous literature have also claimed that it is important to examine the shifting dimensions of privacy concerns as internet users are likely to differ from offline consumers in their concerns about personal information (Malhotra, Kim, & Agarwal, 2004). The gaps in the literature will serve as a basis for this paper, and hopefully this thesis will make some interesting contributions to previous literature.

Managerial relevance

Borgia (2014) points to the fact that IoT will bring tangible benefits to the environment, the society, individuals and business, because of IoT's new intelligent applications. Additionally, IoT have services and products in various domains, while it needs to ensure protection of personal information and content exchanged. IoT will lead to faster productivity growth and an increase in job creation. Additionally, it may facilitate delivering of services in a cheaper and better way than existing methods, and it will give the opportunity to innovate and offer new services and solutions to existing problems. IoT will also create the ability for companies to get closer to their customers and give an understanding of how the customers interact with their products. Previous research states that IoT will have a potential effect on the economic activity across industries, influencing their strategic decisions. Currently, about 80% of the GDP comes from physical industries, while only 20% of the GDP comes from digital industries. This is emphasized by Groven's (personal communication, March 8, 2018), which states that Future Home's biggest competition are normal houses. However, IoT will bring the physical industries closer to the cyber world and will change the physical industries' way of making businesses. Smart Objects will become active participants in business and social processes. Smart Objects will interact and communicate with themselves, with people, and the environment (Russo et al., 2015). Future businesses and marketing strategies of big companies such as Google, Facebook, Apple, and IBM are clearly defined, the future market is IoT (Borgia, 2014). Still, the emergence of IoT have some challenges, Maeland (personal communication, March 13, 2018), raises questions to how IoT will function with the existing technology, how IoT devices will work together, which language the devices should speak, how consumers should adjust to the new technology, and who should install the new solutions for the consumers. He further states that this will eventually demand extreme expertise.

Outline

The thesis is organized as follow: First, the theoretical framework will be presented, whereas IoT, Smart Devices and adoption will be defined. Thereafter, the literature review will be present where previous research will be discussed as a basis for which factors that are going to be tested as barriers against IoT adoption. The barriers are divided into situational barriers and individual traits. Situational barriers are again divided into topic specific barriers (security and privacy, dependence, intrusiveness, price, ease of use, value perception, self-efficiency, novelty) and non-topic specific barriers (risk, network effect, uncertainty, and knowledge). Individual traits will also be discussed in the literature review. Individual traits consist of optimism, innovativeness, discomfort, and insecurity. Next, this thesis will consist of two studies, first, Study 1 explores barriers against IoT adoption, second, Study 2 investigate one of the barriers found in Study 1 more thoroughly, being collection, one subcategory of the privacy and security barrier. The methodology, results and discussion related to Study 1 will be discussed before moving on to explaining the theory used in Study 2. The methodology and result section of Study 2 will be provided before a general discussion is presented. This discussion also addresses managerial and theoretical implications of the results. There will further be presented some limitations of the two studies conducted and avenues for future research. Lastly, a conclusion of the thesis will be provided.

Chapter 2: Theoretical Framework

Chapter 2, concerning the theoretical framework of this thesis will first present a definition of concepts, which include IoT, Smart Devices, and adoption. Secondly, the literature review will be presented, including a discussion of every barrier that could affect IoT adoption.

Definition of concepts

Internet of Things and Smart Devices

Smart Objects can be seen as the building blocks of Internet of Things. Smart Objects can collect information from the environment and interact with the physical world, additionally, they can exchange data and information. Smart Objects link people, machines, enterprises, houses, transportation, natural resources, production lines, and logistic networks, in a connected network (Russo et al., 2015). Rifkin (2014) also consider Smart Objects as building blocks of IoT. He further states that everyday objects are turned into Smart Objects by putting intelligence into them. Because of this, IoT is a new paradigm that can link everything with everyone within an integrated network. Hsu and Lin (2016) refers to IoT as a system that uses the internet to form a huge network of Smart Objects. While the conventional internet connects people in the exchange of information, the IoT integrates machines and objects with embedded sensors and allows them to communicate autonomously over the internet.

IoT

Different people are calling IoT different names, such as Internet of Objects, Embedded Intelligence, Machine-to-Machine interaction, Ambient intelligence, and Human-computer interaction, but the objective of IoT is still the same (Madakam, Ramaswamy, & Tripathi, 2015). Furthermore, a clear definition of Internet of Things does not seem to exist yet, as the term in itself is continuously evolving because the technologies and ideas that drive IoT are changing (Borgia, 2014; Madakam et al., 2015; Mishra et al., 2016; Whitmore et al., 2014). Still there has been many attempts at defining IoT. The European Research Cluster on the Internet of Things (IERC), defines IoT as a “dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual “things” have identities, physical attributes, and virtual personalities, use intelligent interfaces and are seamlessly integrated into the information network” (as cited in Vermesan et al., 2011, p. 10). While Madakam et al. (2015) defines IoT as “an open and comprehensive network of intelligent objects that have the capacity to auto-organize, share information, data and resources, reacting and acting in face of situations and changes in the environment”. Further, the same authors states that “IoT allows communication between human-to-human, human-to-things and things-to-things” (p.165). Whitmore et al. (2014) similarly state that the core concept is that objects can communicate with one another, and with other devices and services to achieve useful objectives. Lastly, Gubbi et al. (2013) defined IoT as the "interconnection of sensing and actuating devices providing the ability to share information across platforms through a unified framework, developing a common operating picture for enabling innovative applications. This is achieved by seamless ubiquitous sensing, data analytics and information representation with Cloud computing as the unifying framework" (p. 1647).

Previous research also discusses IoT as an interconnected network of heterogeneous entities (Atzori et al., 2010; Malina, Hajny, Fujdiak, & Hosek, 2016). It is also stated that IoT has a huge potential for developing new intelligent applications in many fields. This is mainly due to its ability to both collect information about natural phenomena, medical parameters, or user habits, and to offer consumers tailored services (Borgia, 2014). Some researchers have also explained IoT in two perspectives. First, the internet centric perceptive, were the internet services is the main focus, while data is contributed by the objects. Secondly, in the thing centric perceptive, the Smart Object is the focus (Gubbi et al., 2013). The "thing" can be read, recognized, located, addressed and controlled effortlessly by using the internet (Borgia, 2014).

IoT has been grouped in three major domains in previous research, these are: industrial domain, smart city domain, and health well-being domain (Borgia, 2014). Additionally, Mishra et al. (2016) have included personal and social as a fourth domain. Each domain is not isolated from the others, the domains is partially overlapped since some applications are shared (Borgia, 2014). Including this fourth domain can be justified by the expected growth of in-home devices, and wearables (Acquity Group, 2014). Still, the majority of connected things will be in the infrastructure (Borgia, 2014). Furthermore, IoT covers different aspects, such as personal, social, societal, medical, environmental, and logistics (Borgia, 2014). Additionally, IoT also includes patients remote monitoring, energy consumption control, traffic control, smart parking system, inventory management, production chain, customization of shopping at supermarkets, and civil protection (Sicari, Rizzardi, Grieco, & Coen-Porisini, 2015).

Smart Objects

Smart Objects are defined by Miorandi, Sicari, De Pellegrini, and Chlamtac (2012) as "a physical embodiment with communication functionality, possessing a unique identifier, some basic computing capabilities and a way to detect physical phenomena and to activate actions having an effect on physical reality" (p. 1498). Smart Objects can interact with other Smart Objects over the internet and with people (Hsu & Lin, 2016). Smart Objects may be perceived as a radical change (Ram, 1987), due to three main characteristics: intelligence, ubiquity, and autonomy (M. E. Porter & Heppelmann, 2014). Further, López et al. (2011) characterize Smart Objects as those objects that possess a unique identity, are able to sense and store measurements obtained, and devices that can make decisions about themselves and their interactions with external entities.

Adoption of IoT devices

Adoption is defined by Sathye (1999) as "the acceptance and continued use of a product, service or idea" (p.325). While new product adoption behavior is referred to as the degree to which consumers adopt a new product earlier than other consumers in their social system (Rogers & Shoemaker, 1971). Consumers go through a process of awareness, interest, evaluation, trial and then making the decision to adopt or reject a product (Rogers, 1976, 2010). However, Hall and Khan (2003) states that consumers do not have a choice between adoption and no adoption, rather the authors claim that consumers have the choice between adopting now or postpone the decision until later. Furthermore, attitude towards adopting a technology is generated by consumers primary beliefs about the consequences of adopting the technology, in addition to an evaluation of these consequences. Thus, attitude is made by the strength of the persons beliefs that adoption of a technology will lead to a certain consequence (Ajzen & Fishbein, 1980).

Literature review

Situational barriers

Situational barriers refer to obstacles directly and personally associated with the consumer. In this thesis, situational barriers consist of topic specific barriers, referring to barriers found in the IoT and Smart Device literature, as well as non-topic specific barriers referring to barriers found in the innovation and technology literature, these will be discussed in the following sections. First, table 1 is presented, which shows an overview of selected studies from previous research which will serve as a basis for the selection of situational barriers, these will also be discussed in the following.

Table 1

Previous research that has studied the barriers tested in this thesis

Topic specific situational barriers	Privacy and security	Malhotra et al. (2004) Gubbi et al. (2013) Björnsjö et al. (2016) Hsu and Lin (2016) Ziegeldorf, Morchon, and Wehrle (2014) Miorandi et al. (2012)
	Dependency	Mani and Chouk (2016) – Not supported Licoppe and Heurtin (2001)
	Intrusiveness	Boeck, Roy, Durif, and Grégoire (2011) Hérault and Belvaux (2014) Mani and Chouk (2016)
	Price	Björnsjö et al. (2016) Nakyung and Kim (2015) Kim, Chan, and Gupta (2007) Mani and Chouk (2016) Andersson and Heinonen (2002)
	Ease of use	Laukkanen and Lauronen (2005)

		I. T. Szmigin and Bourne (1999) Teo and Pok (2003) Jarvenpaa, Lang, Takeda, and Tuunainen (2003) Nysveen, Pedersen, and Thorbjørnsen (2005) Björnsjö et al. (2016)
	Self-efficiency	Davis, Bagozzi, and Warshaw (1989) Hill, Smith, and Mann (1986) Ellen, Bearden, and Sharma (1991) Park and Chen (2007) Mani and Chouk (2016)
	Value perception	Atzori et al. (2010) Wuenderlich et al. (2015) Björnsjö et al. (2016) D L. Hoffman and Novak (2015)
	Novelty	Mani and Chouk (2016) Wells, Campbell, Valacich, and Featherman (2010) Lazar, Koehler, Tanenbaum, and Nguyen (2015)
Non-topic specific situational barriers	Risk	Featherman and Pavlou (2003) J. Lu, Yao, and Yu (2005) Martins, Oliveira, and Popovič (2014) Yang, Liu, Li, and Yu (2015) Kang and Kim (2009) Sheth and Stellner (1979) Poo and Dalziel (2016) Laukkanen, Sinkkonen, Kivijärvi, and Laukkanen (2007) Laukkanen (2016) – Not supported Hirunyawipada and Paswan (2006)
	Network effect	Hall and Khan (2003) Risselada, Verhoef, and Bijmolt (2014) Hirunyawipada and Paswan (2006) Godes (2011)
	Uncertainty	Littler and Melanthiou (2006) Van Heerde, Mela, and Manchanda (2004) I. Szmigin and Foxall (1998) Arts, Frambach, and Bijmolt (2011) Castaño, Sujan, Kacker, and Sujan (2008) Hall and Khan (2003)
	Knowledge	D. C. Smith and Park (1992) Jansson, Marell, and Nordlund (2010) NTIA (2002) Rogers (2010)

Topic specific barriers

Topic specific barriers refers to barriers that are found in the IoT and Smart Device literature. In other words, barriers related to the topic of the thesis. One barrier discussed in this section is price and security, this barrier has received great attention in the literature. Over half of the literature that focused on challenges and barriers of IoT involve security and privacy. This focus reflects the potential impact of these issues on IoT adoption and diffusion (Whitmore et al., 2014). Privacy and security are also argued to be the most prominent issues, as they are the heart of trust, relationship building, and exchange (Weinberg et al., 2015). Other barriers discussed in previous research is dependency, intrusiveness, price, ease of use, self-efficacy, value perception, and novelty. Challenges and barriers vary depending on the IoT application. For instance, price is a major barrier in consumer application, while security, reliability and life time challenges has more focus in industrial IoT applications (Narayanan, 2017). In the following sections the topic specific barriers will be discussed.

Privacy and security

Ziegeldorf et al. (2014) defines privacy in IoT as "the guarantee to the subject for awareness of privacy risks, individual control of the collection and processing of personal information and awareness, as well as control of subsequent use and dissemination of personal information" (p. 2729). While security is referred to as the degree to which a consumer perceive the use of a device to be risk free (S. Xu, Fang, Chan, & Brzezinski, 2013). Previously, in non-electronic environments, individual privacy was easier to protect because of the relative inefficiency of communication channels (Hsu & Lin, 2016). This highlights the importance of addressing privacy and security issues, as it gets harder to protect consumers personal information. Furthermore, it is argued that consumers will assign greater emphasis and importance on data ownership and data flow-related issues (e.g. privacy) and less focus on traditional marketing factors. A brands reputation and perceptions will be based increasingly on privacy and respect for consumer data, which can signal respect for consumers. Weinberg et al. (2015) argues that privacy issues will have greater or equal importance as the marketing mix elements have in traditional marketing.

Consumers concerns for privacy are well justified. Data collection in IoT are completely different than previous methods, whereas IoT will raise many occasions for personal data to be collected. Therefore, it will be impossible for consumers to personally control the disclosure of their personal information (Atzori et al., 2010). This is supported by Weinberg et al. (2015), which state that IoT will lead to sharing and exposing of more information to both providers and other devices. A lot of IoT services can collect sensitive data, such as locations, personal, and medical data. Absence of privacy protection may therefore cause serious privacy leakage (Malina et al., 2016). It is predicted that the privacy and security barrier will be present in every segment constructed in the analyses part of this thesis, while other barriers such as price only will be present in one segment. Previous research has also pointed to the fact that the data collected and used in IoT will be remembered forever. This raises many privacy issues as the data can be used in both a positive and negative way (Gubbi et al., 2013). IoT applications is vulnerable to attacks, because it is physically easy to attack them, as they are often left unattended. However, respect for consumer's being and their privacy is important for the customer experience with IoT (Atzori et al., 2010). Consumers will consider and act on the tradeoffs associated with the conveniences offered by IoT and the cost and losses in privacy (Weinberg et al., 2015). Weber (2010) argue that privacy includes hiding personal information and have the ability to control what happens with this information.

Privacy and security issues also have a legal aspect, which needs to adequately take into account the globality, verticality, ubiquity and technicity of the IoT (Weber, 2010). In fact, EU has newly implemented a new legal regulation named the General Data Privacy Regulation (GDPR). This regulation aims to protect the data and privacy for all individuals in EU, by giving control to individuals (Salami, 2017). Furthermore, consumers also have varying individual perception and requirements to personal information (Ziegeldorf et al., 2014). For instance, consumers with higher concern for privacy will be more likely to read online privacy notices than people who are less concerned (Milne & Culnan, 2004).

As studies show that more than two-thirds of consumers are aware of the recent security breaches, it is expected that this thesis also will identify privacy and security as a barrier against IoT adoption. Furthermore, as much as 18% of consumers who were aware of recent hacker attacks and owning or planning to own IoT devices in the next few years decided to terminate their purchase, until they got safety guarantees. These consumers perceive the risk to outweigh the value of owning IoT devices. In the same study, the authors found that 24% of the participants decided to postpone purchase of an IoT device. Additionally, 47% of consumers mean that privacy risk and security concerns are a barrier to adoption of IoT devices (Björnsjö et al., 2016). This indicates that consumers do not trust the existing IoT technology. Similarly, the Acquity Group (2014), found that 57% of consumers were less likely to purchase wearable technology because of hacks and data breaches. Prior research states that use of IoT services may lead to risk for the users regarding unintentional publication of personal information (Hsu & Lin, 2016). The IoT environment is characterized by different devices which have to process and handle the data with user needs and rights in mind, therefore trust is a fundamental issue (Sicari et al., 2015). If there does not exist any public confidence in IoT, and that these devices will not cause serious threats to privacy, consumers will resist IoT (Atzori et al., 2010). Ignorance of people's privacy concerns can lead to nonacceptance and failure of new services damage to reputation, or lawsuits (Ziegeldorf et al., 2014). Hsu and Lin (2016) further argue that the greater the perceived control of personal information is for the consumer, the lower risk he or she feels. Many studies have stated that privacy concerns must be addressed to ensure that IoT becomes a reality (Chui et al., 2010; Hsu & Lin, 2016; Miorandi et al., 2012; Vermesan et al., 2011). This discussion has shown that there is strong evidence in previous literature for the existence of a privacy and security barrier against IoT adoption. However, it will still be interesting to test if my studies get the same results, and therefore contribute to the generalizability of privacy and security being a barrier against IoT adoption.

Dependence

Dependence refers to consumers degree of being dependent on a certain internet and computer-related technology. This has become the reality for several consumers in different contexts, including work, family and school (D L. Hoffman, Novak, & Venkatesh, 2004). Several technologies such as mobile phone (Licoppe & Heurtin, 2001), online video games (Lo, Wang, & Fang, 2005) and the internet (Hadlington, 2015) increases consumers dependency. It has been stated that dependency is linked to "technostress" (Shu, Tu, & Wang, 2011), meaning the negative impact of technology on consumers attitudes, thoughts, behavior and physiology (Weil & Rosen, 1997). Technological dependence may create isolation because communication with devices substitutes communications with humans. Additionally, technology dependency can also create addiction, due to abuse or overuse of a given technology (Charlton, 2002). Addiction can be seen as a more severe form of dependence as it can represent a pathological state (Dhir, Chen, & Nieminen, 2015). Mani and Chouk (2016) analyzed if dependence positively influenced consumer resistance to Smart Products and if dependence was a predictor of privacy concerns. The authors found evidence for dependence being a predictor of privacy concerns, a barrier which is discussed above. However, they did not find a significant effect of dependence on consumer resistance. However, this can be explained by their sample, consisting of digital natives, which may have difficulties in perceiving their dependence. Older consumers are on the other hand more likely to perceive dependence because they can compare their lives before and after the adoption of digital innovations. Additionally, it is difficult to evaluate dependence without owning the device that are being tested. It will therefore be interesting to see if this thesis finds evidence of dependency being a barrier against IoT adoption. Note that this thesis is testing wheatear dependency is a barrier for adoption, while Mani and Chouk (2016) tested wheatear dependency lead to consumer resistance.

Intrusiveness

Intrusiveness reference to someone entering the consumers life without permission. Smart Devices may be seen as intrusive because they have the ability to perform actions autonomously and without the permission of the consumer (Mani & Chouk, 2016). In marketing, intrusiveness is considered to have a negative impact on consumer behavior, as it triggers individual negative emotional reactions (Edwards, Li, & Lee, 2002). For instance, some consumers may find the act of capturing the flow of electricity into one's home, and the manner in which it is used over a period of time intrusive (Cavoukian, Polonetsky, & Wolf, 2010). Therefore, it is expected that some consumers find IoT devices to be intrusive. This is in line with previous research, which found that intrusiveness have a negative effect on consumers adoption of RFID (Boeck et al., 2011) and mobile location-based services (Hérault & Belvaux, 2014). Mani and Chouk (2016) found in their research that intrusiveness positively influences consumer resistance to Smart Products. Additionally, they found that privacy has a positive effect on intrusiveness, because, the more consumers feel sensitive about their privacy, the higher the level of perceived intrusiveness of the Smart Device will be.

Price

Price refers to consumer considerations of which monetary sacrifice is appropriate of the product in question (Mani & Chouk, 2016). It is stated that perceived sacrifices are both monetary and non-monetary. However, in this thesis price is operationalized to concern the monetary sacrifices. Monetary spending's includes the actual price of the product (Kim et al., 2007). However, Balta-Ozkan et al. (2013) suggests that consumers are concerned with cost of installation, repair, maintenance, learning, and savings, not just the purchasing cost. Accenture's 2016 report also state that price is one of the top barrier of IoT adoption (Björnsjö et al., 2016). This is supported by Nakyung and Kim (2015) which found that price is one of the most important factors when the consumers buy a Smart Home product or service. Interestingly, researchers also state that consumers are discouraged more by costs than they are attracted by benefits (Kim et al., 2007). Conflictingly, Acquity Group (2014) found in their 2014 report that consumers are comparatively less worried about price than other factors such as safety. Still they acknowledge that cost is an important consideration.

Previous research, studying 800 consumers in the US found that 56% of the respondents think Smart Devices are too expensive (Hong et al., 2017). Kim et al. (2007) further found that monetary costs serve as barriers to adoption of mobile-internet. It will therefore be interesting to test wheatear price is a barrier against adoption of IoT devices. The 2016 Accenture Digital Consumer Survey of 28.000 consumers in 28 countries also found that consumers price perception differs depending on where consumers are in the diffusion of innovation model. Early adopters of IoT and early majority are less concerned about price than late majority and late adopters. They are willing to spend on devices when they believe there is a compelling value proposition (Björnsjö et al., 2016). However, in general, 62% of consumers believe that IoT devices are too expensive, meaning that the majority of consumers actually perceive the price of IoT to be too high. It will therefore be interesting to test if price is a barrier against IoT adoption, or if consumers simply means that the price is too high, but they buy these devices anyway. A reason for why price may be perceived as a barrier against IoT adoption is the evidence for that monetary sacrifice reduces the perceived value of mobile services. The reasoning behind this is that high price, or having to pay a price at all keeps many new consumers from trying services they are not sure about (Andersson & Heinonen, 2002). This may be because consumers that do not have any experience with new technologies, cannot judge whether the price is high or low. According to the Adaption Level theory, instead of having perfect information about prices, consumers possess internal reference prices and make comparisons with these prices (Grewal, Monroe, & Krishnan, 1998). Lastly, Mani and Chouk (2016) found in their research that price has a significant positive impact on consumer resistance of Smart Products. They further state that perceived price seems to be one of the core reasons why consumers resist Smart Products, at the introduction stage of the product life cycle. However, if the perceived value of the devices is improved, consumers will be more likely to accept the financial risk. As stated, it will be interesting to test if this also apply to adoption.

Ease of use

Ease of use refers to consumers perception of how difficult IoT devices are to understand and use (Mallat, 2007). If consumers do not adopt an IoT device because they perceive the device to not be free of effort, they experience an ease of use barrier. Ease of use is also a component in the technology acceptance model (TAM) which is extensively researched (Gefen, Karahanna, & Straub, 2003). Ease of use in relation to the TAM model is defined by Davis (1989) as "the degree to which a person believes that using a particular system would be free of effort" (p. 320).

Complexity and ease of use have contributed to the low adoption of a variety of systems, such as Smart Cars and mobile banking (Laukkanen & Lauronen, 2005; I. T. Szmigin & Bourne, 1999). Similarly, ease of use and convenience have been found to affect consumer adoption of mobile technologies and services (Jarvenpaa et al., 2003; Nysveen et al., 2005; Teo & Pok, 2003). It will be interesting to test if this also is applicable to adoption of IoT devices. Furthermore, 64% of respondents in Accenture's study experienced a challenge when using a new IoT device in 2016. This is an improvement from the last year, whereas 83% of respondents experienced challenges with an IoT device (Björnsjö et al., 2016). Even if potential users believe that a given device is useful, they might, simultaneously believe that the system is too hard to use. In this case the effort of using the device outweigh the performance benefits of usage (Davis, 1989). Ease of use is proven to be similar to self-efficacy (Venkatesh & Davis, 1996), which is discussed next.

Self-efficiency

Self-efficiency is defined by Compeau and Higgins (1995) as "an individual's perception of his or her ability to use a technological innovative product" (p.193). It is suggested that self-efficacy can be obtained by (1) direct experience in a situation or a similar situation, or (2) observed performance of a similar task by other peoples (Venkatesh & Davis, 1996). Previous research have found a positive effect of self-efficacy on willingness to adopt technology (Davis et al., 1989; Hill et al., 1986). Further, self-efficiency is found to have a negative effect on consumer resistance to technological innovations (Ellen et al., 1991) and a positive effect on consumers adoption of innovations (Park & Chen, 2007). Note that these findings are from the innovation literature. Little research has tested self-efficacy as a barrier in the IoT literature, therefore it will be interesting to test if self-efficacy is a barrier against IoT adoption. Among the few researchers that have tested self-efficacy in the IoT literature is Mani and Chouk (2016), they found a negative impact of self-efficiency on consumer resistance to Smart Products. Indeed, when consumers feel confident about their ability to understand the use of Smart Products, they tend to show less oppositional reactions. This is in line with previous research in the innovation literature (Ellen et al., 1991).

Value perception

Value perception refers to the degree consumers perceive the usage of a given Smart Object as beneficial to them (D L. Hoffman & Novak, 2015). While Kim et al. (2007) defines value as "the trade-off between total benefits received and total sacrifices" (p. 112). It is further argued that most consumers do not have the need (D L. Hoffman & Novak, 2015, or interest (44%) in owning an IoT device (Assurant Inc, 2017). This makes it difficult for companies to reach many consumers. Marketers have also struggled to find the right value proposition to communicate to consumers (D L. Hoffman & Novak, 2015). For instance, increasing numbers of devices are being added to the IoT ecosystem, this raises questions about the utility and added value of these innovations (Mani & Chouk, 2016). This is important as Atzori et al. (2010) suggests that perceived benefits play a significant role in explaining why consumers use IoT services. Additionally, as Piwek et al. (2016) discuss in their research, many wearable devices do not add the functional value that is expected, and they require too much effort, which ruins the user experience. Similarly, Atzori et al. (2010) states that if consumers do not perceive the usage of devices as beneficial, they are unlikely to continue to use the devices. On the other hand, perceived benefits provided by IoT devices may be seen as improving the quality of users' lives in a wide range of domains.

While Björnsjö et al. (2016) state that an unsatisfactory value perception is reflected in concern over pricing, D L. Hoffman and Novak (2015) mean that it is not clear that lower price on its own can create more value for consumers. Furthermore, studies show that consumers care most about the primary functional values and user experience when evaluating IoT devices. It is also stated that designing offerings for user-centric experiences and value will be critical for adoption of IoT (Brody & Pureswaran, 2015). Interestingly, Wuenderlich et al. (2015) argue that the success of any new Smart Device depends on consumers perceived value. An example from the smartwatch market show that of 330 Apple Watch owners who were dissatisfied with the device, 86% of did not find any value in the product. In addition, 80% thought the device functionalities were too limited and 53% did not plan to purchase the next version (Desarnauts, 2015, November 30 ; Mani & Chouk, 2016). This serves as evidence for consumers perceived value matter in terms of IoT's success, it will therefore be interesting to test if value perception is a barrier against IoT adoption.

A problem existing today is that the IoT technology does not work optimal. For instance, smartwatches are connected to mobile phone, and text messages should appear on the watch, but this only happens sometimes and not in every situation it should. This means that consumers perceived value of this device may be unsatisfactory. This is discussed in Weinberg's (2015) research where they state that many IoT systems are available, however, all of the technical aspects of infrastructure and communications are not in place. Supported by Borgia (2014) which state that technical challenges need to be faced and solved for the IoT vision to successfully emerge, as a device that do not work, do not yield any value to the consumers. Previous research state that only 13% of business currently have all the technologies, platforms, or services required to support IoT initiatives (O'Brien, 2017).

Brody and Pureswaran (2015) anticipate IoT to emerging as a low-cost "democracy of devices" that will enable new digital economies and create new value, while they offer consumers better experiences. IoT devices should create value by applying connectivity and intelligence to improve the core value proposition to the devices. For instance, smart cooktops that automatically turn the heat down when a pot boils over.

Consumers will embrace solutions like this because they provide better cooking, less mess, increase safety and not because they are part of aa complex network. It is suggested that the most successful IoT solutions must be powerful in their value propositions, simplicity and reliability (Brody & Pureswaran, 2015).

Novelty

Consumers may perceive a device to be novel when there is a radical change in the device's concept, or simply changes in one attribute of the device (Ram, 1987). Novelty further refers to a device that is perceived to be unique, different, recent, or new (Venkatraman & Price, 1990). Novelty is a fundamental characteristic of any innovation. It is stated that the perceived newness of the idea for the consumer determines their reaction to it. Thus, perceptions of novelty differ across individuals and types of innovations (Rogers, 2010). Since a IoT device can be an innovation, it is expected that novelty also is a fundamental characteristic of IoT devices, but is shall be interesting to test if novelty influences IoT adoption. Mani and Chouk (2016) is one of few that has analyzed novelty in the IoT literature. They found a significant negative impact of novelty on consumer resistance to Smart Products. Since consumers perceive Smart Products as different and unique, they are less resistant to adopt these innovations. It will be interesting to test wheatear the same findings can be obtained for IoT adoption. Furthermore, Lazar et al. (2015) suggests that the novelty of a Smart Device is a compelling motivator for consumers to use Smart Devices. Further, they argue that there exists a drop off effect of use as novelty decreases and the cost of maintaining devices becomes irritating. This is supported by Wells et al. (2010) which found perceived novelty to decrease the perceived risk associated with technological innovation.

Non-topic specific barriers

Non-topic specific barriers refer to barriers that are not directly linked to IoT or Smart Objects. A lot of the literature in this section is collected from the innovation literature, but previous research discussed in this section also involves technology, new product developments etc. Two major research streams related to the non-topic specific literature is Rogers model of diffusion of innovation and the Technology Acceptance Model (TAM). While Rogers' (2010) model of diffusion of innovations, discusses characteristics that is expected to influence consumer acceptance of new products and services. The TAM model includes perceived ease of use and perceived usefulness in a model of technology acceptance (Davis, 1989). Worth mentioning, is the great failure rates of innovations, ranging between 50% and 90% (Castellion & Markham, 2013; Heidenreich, Kraemer, & Handrich, 2016). As Ram and Sheth's (1989) functional (value, risk, usage) and psychological (image, tradition) barriers are widely discussed in the innovation literature, these will also be discussed in this thesis serving as a basis for the non-topic related barriers. Furthermore, risk, network effect, uncertainty, and knowledge will be discussed. Additionally, compatibility is discussed in relation to network effect, relative advantage in relation to value and complexity in relation to the usage barrier.

Functional and psychological barriers

Ram and Sheth's (1989) functional and psychological barriers are widely used in prior research to explain active innovation resistance (Heidenreich et al., 2016; Laukkanen, 2016; Mani & Chouk, 2016; Talke & Heidenreich, 2014). Research in the field of innovation has identified these two categories of barriers as most meaningful in explaining consumers uncertainty to adopt technological innovations (Antioco & Kleijnen, 2010; Herbig & Day, 1992; Ram, 1989). Usage, value and risk barriers are functional, which occur when the consumer perceives a radical change during a new product adoption. While psychological barriers include tradition and image (Mani & Chouk, 2016). Psychological barriers mostly arise through conflicts with consumers prior beliefs (Antioco & Kleijnen, 2010). Laukkanen et al. (2007) found that the psychological barriers (image and tradition) was greater among mature consumers than younger consumers. The functional barriers are more likely to occur if consumers perceive significant changes from adopting an innovation. Psychological barriers are often created through conflicts with prior believes (Ram & Sheth, 1989). A brief explanation will be given of the psychological and functional barriers respectively.

The tradition barrier arises when an innovation is incompatible with individuals existing value, past experience and social norms (Ram & Sheth, 1989). Consumers have a favorable attitude toward the products they are currently using and they may be unwilling to replace their old products with new marketing offerings (Wang, Dou, & Zhou, 2008). The tradition barrier typically arises due to cultural changes which is enhanced when consumers meets an innovation adoption decision. The theory of reasoned action (Ajzen & Fishbein, 1980) illustrates how important social norms are in consumer decision making. Prior research in the innovation adoption field confirms that consumers rely heavily on their reference groups in their decision to use innovations (M. K. Chang & Cheung, 2001; Karahanna & Limayem, 2000). Conflicts with tradition have led to strong reactions from consumers, ranging from negative word of mouth, boycotts and sabotage (John & Klein, 2003; Poo & Dalziel, 2016), as well as rejection of internet banking (Laukkanen, 2016), and resistance to technology adoption (Poo & Dalziel, 2016). Conceptually, the tradition barrier relates to the concept of compatibility (Rogers, 2010), which will be discussed later.

According to Ram (1989) the *image barrier* relates to problems that arises from stereotyped thinking and lack of information. The image barrier is also explained as an extrinsic cue, which is used by consumers to assess new products (Bearden & Shimp, 1982). If consumers dislike the extrinsic cues, they develop a negative image of the innovation, creating an image barrier (Ram & Sheth, 1989). Previous research has found support for the image barrier, for instance Laukkanen (2016) found that the image barrier hinders adoption of mobile banking. Strebel, O'Donnell, and Myers (2004) found that an unfavorable image can affect consumers adoption intentions towards high technology durable goods.

Ram and Sheth (1989) propose that the *usage barrier* occurs when an innovation is conflicting with existing workflows, practices or habits. It relates to the device's usability and the necessary changes from the consumer perspective (Laukkanen et al., 2007). As resistance may be a consequence of habits (Kleijnen, Lee, & Wetzels, 2009), innovations that require changes in consumers routine demands a relatively long development process before gaining consumer acceptance (Herbig & Day, 1992). Also, if the perceived difficulties and challenges with a technology are perceived higher than the expected benefits, consumers are likely to reject the innovation (Poo & Dalziel, 2016). Prior research show that the cognitive effort required to adopt an innovation generates resistance (Ram, 1989). Also, Ram and Sheth (1989) found that the usage barrier have a significant influence on intention to adopt. On the other hand, Laukkanen (2016) found that the usage barrier did not explain non-adoption or postponement of internet and mobile banking services. Similarly, Poo and Dalziel (2016) only found a minor influence of consumer's perception of the usage barrier on acceptance of autonomous cars.

The usage barrier relates to the technology Acceptance Model (TAM) (Davis, 1989), where perceived ease of use and perceived usefulness is included in a model of technology acceptance. Perceived ease of use closely parallels to *complexity* (Hoeffler, 2003; Teo & Pok, 2003; Wood & Moreau, 2006), which refers to the extent to which an innovation is difficult to use and understand (Kleijnen et al., 2009). Complexity is found to be one of the most important antecedents of adoption behavior (Arts et al., 2011). The reasoning behind this is that the more an innovation is perceived as complex, the more learning cost to adopt new behaviors will be involved. (Hoeffler, 2003; Wood & Moreau, 2006).

The value barrier suggests that an innovation must be superior for consumers to replace an existing product (Ferreira, da Rocha, & da Silva, 2014), more specifically, it must have a superior performance to price ration (Ram & Sheth, 1989). Laukkanen (2016) found the value barrier to be a dominant barrier in terms of service innovation. This is also the case for barriers against technological innovation adoption (Kim et al., 2007). It is demonstrated that perceived lack of value lead to a significantly lower chance of consumers adopting a technology (Antioco & Kleijnen, 2010). The value barrier further relates to TAM's perceived usefulness (Davis, 1989) and Rogers (2010) relative advantage. *Relative advantage* is defined by Rogers (2010) as "the degree to which an innovation is perceived as better than the idea it supersedes" (p. 42). Relative advantage is a strong driver of behavior in consumers adoption of innovations (Arts et al., 2011; Kleijnen et al., 2009). Based on Construal Level Theory (Trope & Liberman, 2003), perceived relative advantage is expected to be weighed high by potential adopters as they are far from actual adoption behavior (i.e. intention stage) (Arts et al., 2011). Relative advantage is also a part of Rogers (2010) model of diffusion of innovations, including five characteristics postulated to influence consumer acceptance of new products and services.

The risk barrier is defined by Dowling and Staelin (1994) as "consumer's perceptions of the uncertainty and adverse consequences of buying a product (or service)" (p.119). Previous research perceive risk as a serious obstacle in the adoption process (Klerck & Sweeney, 2007). Nearly all innovations represent risks and offers potential side effects that cannot be anticipated (Antioco & Kleijnen, 2010). Further, consumers often experience doubts relating to innovation adoption in the form of different risk types, such as performance, physical, financial, psychological and social risk (Kaplan, Szybillo, & Jacoby, 1974). The risk barrier will further be discussed in depth below.

Risk

Risk will be one of the barriers that is predicted to influence adoption of IoT devices, and risk will therefore be included in the analyses conducted later. Perceived risk is a well-established concept in consumer behavior (Littler & Melanthiou, 2006), which refers to, consumers evaluation of the likelihood of negative outcomes when considering to adopt an innovation (Garcia & Atkin, 2006). Risk is one of the most frequently discussed extensions of traditional adoption and technology acceptance models (Herzenstein, Posavac, & Brakus, 2007). Previous research show that perceived risk has a negative influence on intention to use (Featherman & Pavlou, 2003; H.-P. Lu, Hsu, & Hsu, 2005; Martins et al., 2014; Yang et al., 2015), and an positive effect on resistance (Kang & Kim, 2009; Sheth & Stellner, 1979). Furthermore, Poo and Dalziel (2016) discusses the challenge of continual radical innovation, and suggests that the low adoption rate by consumers is caused by consumers resistance and perceived risk. Laukkanen et al. (2007) found that mature customers related significantly higher degrees of risk to the use of mobile banking compared to young consumers. Ram (1987) states that the level of perceived risk depends on the type of innovation. Minor innovations have lower risk than major innovations. He further discusses trialability, which also effects the perceived risk associated with an innovation. Trialability refers to how easily the innovation can be tried by consumers prior to adoption.

On the other hand, Laukkanen (2016) found that risk did not explain non-adoption or postponement of internet and mobile banking services. Other researchers also support this notion, and claim that the well supported evidence of a negative effect of risk on new product adoption, is not so obvious. The reasoning behind this is that actual adoption is a function of consumer innovativeness, therefore, the perception of risk may not have much to do with actual adoption (DelVecchio & Smith, 2005; Hirunyawipada & Paswan, 2006; Mitchell & Harris, 2005). As these findings show, risk is extensively analyzed in the innovation literature where researcher have both found support and rejection of their hypothesis testing if risk is a barrier, it will therefore be interesting to test whether risk also can be found as a barrier against IoT adoption.

Several risk dimensions have been discussed in previous research. Kaplan, Szybillo, and Jacoby’s (1974) five type of risk is often cited in previous research, these are: performance, physical, financial, psychological and social risk. Additionally, Roselius (1971) have added time loss (Hoyer & MacInnis, 1997). In this thesis, risk in analyzed as a broad domain, and are therefore not divided in sub categories. Still a brief discussion of the mentioned risk types will be provided, to understand the whole concept of risk. Furthermore, network risk is also perceived, by some, to be a part of the risk dimensions (Hirunyawipada & Paswan, 2006; Kaplan et al., 1974). However, in line with previous research (Hall & Khan, 2003; Risselada et al., 2014), I will discuss network as a barrier on its own further down.

Financial risk has been identified extensively in previous research (Agarwal & Teas, 2001; Fenech, 2002; Liao & Cheung, 2001). Financial risk has been defined by Ram and Sheth as “represent a wrong decision to adopt an innovation instead of waiting for a better and more inexpensive version” of a given product (as cited in Laukkanen et al., 2007, p. 421). This type of risk captures the financially negative outcomes for consumers after they adopt products (Jacoby & Kaplan, 1972). The perceived financial risk can occur before and after adoption (Hall & Khan, 2003). Adoption of new technology is characterized by concerns over future profit streams, irreversibility which creates sunk cost, and the opportunity to delay (Hall & Khan, 2003). When the consumer needs to make a behavior decision, the focus shift toward the cost involved (Trope & Liberman, 2003). This is consistent with loss aversion theory, which assume that consumers will focus more on potential losses than on gains when faced with a decision of behavioral change (Kahneman & Tversky, 1979). Previous literature has found economic risk to be one of the main drivers for consumers to postpone the adoption of innovation. The reasoning behind this is that consumers may not afford the innovation now and have a believe that price will decrease in the future.

Performance risk relates to concerns about products not performing as anticipated (Jacoby & Kaplan, 1972). This type of risk is especially dominant in technology-driven innovations (Antioco & Kleijnen, 2010). Consumers evaluation of performance risk is based on their knowledge and cognitive abilities in a certain product domain (Ram & Sheth, 1989). It is difficult for consumers to anticipate the overall functionality and performance of a product, since there are many insecurities that arises. This is supported by I. Szmigin and Foxall (1998), which found that when consumer's uncertainty is high, they worry especially about performance risk, leading to a postponement of the buying decision until the uncertainty is resolved.

Physical risk refers to consumers perception of a product being harmful (Jacoby & Kaplan, 1972). Physical risk is associated with new product attributes that consumers have never been exposed to (Dholakia, 2001). This type of risk may therefore lead to consumers being worried about their physical wellbeing and generate enhanced information search.

According to Ram and Sheth (1989) *social risk* refers to consumers who may resist an innovation because they feel they will face social avoidance if they adopt the innovation or they have fear of being seen in a negative light by others. Social risk is found to be important in high-tech consumer electronic markets, as these products are used in the public domain among friends and colleagues. Hence, consumers may invest more effort in finding and acquiring information about the innovative products (Hirunyawipada & Paswan, 2006). Social risk is also found to be significant in the adoption of technological innovations (Antioco & Kleijnen, 2010; R. N. Stone & Grønhaug, 1993). Furthermore, social risk is strongly related to *observability* (Rogers, 2010), meaning the extent to which an innovation is visible and communicable to consumers (Kolodinsky, Hogarth, & Hilgert, 2004). Observability is an important factor in consumer decision process, because lack of social support could potentially lead consumers to isolate themselves form their social system if they use a social unaccepted innovation (Kleijnen et al., 2009).

Lastly, *psychological risk* is defined by Perugini and Bagozzi as the "experience of anxiety or psychological discomfort arising from anticipated post behavioral affective reactions such as worry and regret" (as cited in Dholakia, 2001, p. 1342). In the case of consumer electronic market, psychological risk is found to be less important, as there is a lot of information about the latest products. Additionally, there is a certain assurance about the performance, and there exists user-friendly attributes of products (Hirunyawipada & Paswan, 2006).

Time risk relates to the perception that the adoption and use of a product will take too much time (Roselius, 1971). On one hand, consumers would spend a lot of time learning the details about new products. However, a lot of new products, especially high-tech consumer products have a high level of user friendliness, as well as plug and play systems (Hirunyawipada & Paswan, 2006).

Network effect

Network effect for technology products is defined by Hall and Khan (2003) as "the value of the technology to a user increases with the number of total users in the network" (p. 6). As the use of devices increase and the user network grows, the perceived benefit increase. This drives expansion further, which motivates to an increase usage of devices (Bandyopadhyay & Sen, 2011; Weber, 2010; Ziegeldorf et al., 2014). Similarly Hirunyawipada and Paswan (2006) suggests that network externalities of innovation technologies happens when consumer's utilities depend on previous adoption or the adoption of relevant others (Conner, 1995; Katz & Shapiro, 1985; Shapiro & Varian, 1998). Prior research has stated that social influence affects adoption (Godes, 2011). Furthermore, it is also stated that network effect impacts technology adoption, since the network affect the expected benefit from a new technology (Hall & Khan, 2003). It will be interesting to test if network effect also influences IoT adoption. Adoption of high-technology products in a network can affect consumers either by social influence or direct influence (e.g. communication). Social influence derives from the awareness of a specific number of consumers that adopts a product. Both present and past adoption behavior is relevant as the two effects can influence both recent and past adoption (Risselada et al., 2014). The same authors further argue that the effect, for a potential adopter, of adding one additional adopter in a network decreases over time. Furthermore, it is stated that privacy and security will be a major concern wherever networks are at a large scale (Gubbi et al., 2013).

Previous research has also discussed consumer's assessment of the extent to which other people in a network possess a given technology. Given the newness of a technology, consumers may not have the assurance that other people in a network also have that technology. Additionally, consumers may be excited over the feeling that only they own a given technology, however, anxiety over the fact that only they bought this product may also occur. Thus, consumers may not want the innovation to be owned by everyone, but they might want the reassurance of having some of the consumers in the network to own the innovation, so if something goes wrong they can seek help and information. Network effect risk may therefore lead consumers to seek more information about the product and the extent of its market penetration (Hirunyawipada & Paswan, 2006). Previous literature also discusses consumer's assessment of the extent to which other people in a network possess a given technology in relation to were consumers are at the diffusion of innovation proses. Innovators have a low resistance to adopting a new idea, therefore a few or no interpersonal network influences are needed for adoption. In contrast, a consumer at the late majority stage in the diffusion model has a much higher resistance towards adoption of a innovation, therefore these consumers' needs much more influence from the network in order to overcome the resistance (Rogers, 2010). In relation to this, the social network literature distinguishes between two important network metrics. Tie strength, meaning the intensity and tightness of a relationship (Van den Bulte & Wuyts, 2007) and homophily, meaning the similarity between consumers in a network (McPherson, Smith-Lovin, & Cook, 2001). Homophily can act as a barrier against innovations within a social system, since similar people interact in the network, thus preventing a new idea from being adopted of those who do not have a high status (Rogers, 2010).

Previous literature suggests that there exist two network effects in adoption of technology, namely indirect and direct effect. Direct network effect may be present when a user's utility increases with the total size of the network. Indirect network effect also emerges from increased utility due to a bigger network, however, the increase in utility arise from a wider availability of a complementary good. Meaning that complementary and compatibility could be operationalized as factors affecting indirect network effect (Hall & Khan, 2003). *Compatibility* in an innovation context reflects the degree to which an innovation matches the potential adopters needs and values. Compatibility is therefore an important aspect of the innovations' desirability to individuals (Arts et al., 2011). Perceived compatibility has been found to be an important benefit for adoption intention of innovation. However, study show that compatibility has less impact on behavior than intention to adopt (Arts et al., 2011). Furthermore, Ram (1987) discusses pervasiveness, which is closely linked to compatibility. Pervasiveness of an innovation refers to the degree which the innovation requires changes or adjustments from the consumer (Barnett, 1953). The higher the pervasiveness, the more behavioral change is required.

Uncertainty

Uncertainty refers to the fact that consumers do not fully understand the functions and consequences of innovations. It also takes time before consumers know which technology that sets the standard, which leads to uncertainty (Van Heerde et al., 2004). Uncertainty is widely documented as a barrier to innovation adoption (Castaño et al., 2008). For instance Littler and Melanthiou (2006) found that participants in their study were uncertain when using internet banking. Hall and Khan (2003) further discuss uncertainty as one of the factors that characterizes adoption of new technology. The innovation literature suggests that it is, for a long time, unclear for consumers, which technology that is going to set the standard. This triggers uncertainty when consumers are faced with adoption decisions (Van Heerde et al., 2004). This thesis will also test if this is the case in relation to IoT instead of innovations. The literature seems to be conflicting in regard to if uncertainty is a part of risk or not. While Poo and Dalziel (2016) state that uncertainty is a component of risk (Dowling & Staelin, 1994; Hoyer & MacInnis, 1997). Peter and Ryan state that risk and uncertainty is distinct, at least in theory (as citen in Littler & Melanthiou, 2006, p. 433). The literature also discusses multiple types of uncertainty. For instance Littler and Melanthiou (2006) consider brand, information, consequence, and post purchase uncertainty in their research. When consumer's uncertainty is high, they worry especially about the devices' performance, leading to a postponement of the buying decision until the uncertainty is resolved (I. Szmigin & Foxall, 1998).

Furthermore, Arts et al. (2011) discusses adoption of innovations across the intention and behavior stages of the adoption process. They found that perceived uncertainty shows a stronger effect on intention than on adoption behavior. However, uncertainty affect both intention and behavior of adoption of innovation, although in different ways (Arts et al., 2011). While intention is reflected in distant future adoption decisions, behavior is reflected in near future adoption decisions. Uncertainties about benefits are more important, as adoption is more distant (intention). When behavioral change is important (near future), consumers focuses more on cost uncertainties, associated with switching and new learning (Castaño et al., 2008).

Knowledge

The knowledge barrier refers to, what consumers know about different devices. Knowledge also refers to consumers need or no need to gather much information if they should buy a device, and consumers ability to consider different device's quality. Furthermore, in the decision process consumers goes through when they consider buying a product, "knowledge stage" is the first step. Consumers become aware of a new product, and a certain level of passive innovation resistance arises (Kuisma, Laukkanen, & Hiltunen, 2007). If the consumers is very satisfied with the product they currently own and has a tendency to resist changes, they are less likely to engage in seeking additional information about the new product (Talke & Heidenreich, 2014). The brand extension literature discusses the substitute of consumer's knowledge of a company's existing products, for knowledge of the extension products. This will reduce the uncertainty of purchasing, and it will promote product trial. The substitute knowledge should reduce the amount of information consumers' needs to evaluate (D. C. Smith & Park, 1992). This reasoning may also be applicable to IoT devices, something that will be tested in this thesis.

When consumer's knowledge of a product class is low, the level of perceived risk associated with a purchase is high (D. C. Smith & Park, 1992). Therefore, if consumers do not have knowledge about Smart Devices, they may perceive a higher level of risk than if the knowledge was high. However, gaining new knowledge is proven to solve some of the risk associated with innovation resistance. Because consumers tend to postpone the adoption until risk is mitigated by new knowledge (Dowling & Staelin, 1994; Garcia, Bardhi, & Friedrich, 2007; Locander & Hermann, 1979; Ram & Sheth, 1989). On the other hand, consumers can also get too much knowledge and information about products, which makes it difficult for the consumers to organize and evaluate the information and make comparisons between available alternatives (Herbig & Day, 1992; Herbig & Kramer, 1994; Hirschman, 1987).

Previous research suggests that image may make up for lack of knowledge, as it serves as a signaling function. Image is a set of associations related to the innovation, which is a negative extrinsic cue in the case of resistance (Kleijnen et al., 2009). Antioco and Kleijnen (2010) have also discussed tradition barriers in their research, were they reason that consumers are not aware of how different a given innovation is from existing traditions. Consumers can thus exploit this lack of knowledge to downplay the cognitive dissonance they normally experience from adopting an innovation (Engel, Kegerreis, & Blackwell, 1969). Consumers may also experience this lack of knowledge effect for other product related issues. For instance, consumers making purchase decisions based on price may also downplay cognitive dissonance because they do not have the opportunity to obtain perfect information (Morwitz, Greenleaf, & Johnson, 1998).

Jansson et al. (2010) found in their study that whether or not people are able to engage in specific actions depends on their personal capabilities and resources, such as knowledge. Similarly, Jansson et al. (2010) also found that higher educated persons, who also often have a higher income, are more knowledgeable and have better financial capabilities, and thus are more willing to adopt innovations. Supported by C. E. Porter and Donthu (2006), which states that early adopters of new technologies tend to have higher educational levels, which may reflect their abilities to understand "how-to" knowledge more quickly than consumers with less education (Rogers, 2010). Interestingly, previous empirical research have found that less educated individuals report insufficient knowledge as one of the main reasons that they choose not to use the internet (NTIA, 2002). These consumers feel a higher level of computer anxiety and have less sophisticated cognitive structures that hinder their ability to learn in new environments (Hilgard & Bower, 1975). Generally this means that the decision to adopt a new technology is related to the amount of knowledge consumers has regarding how to use that technology appropriately, and complex technologies require more knowledge (Rogers, 2010).

List of barriers

The barriers discussed in this literature review, and which will be tested in the future analysis are presented in the model below. As mentioned the situational barriers are divided between topic specific barriers and non-topic specific barriers. The topic spesific barriers are security and privacy, dependence, intrusiveness, price, ease of use, value perception, self-efficiency, and novelty. The non-topic spesific barriers are risk, network effect, uncertainty, and knowledge barrier. In the following section individual traits will be discussed.

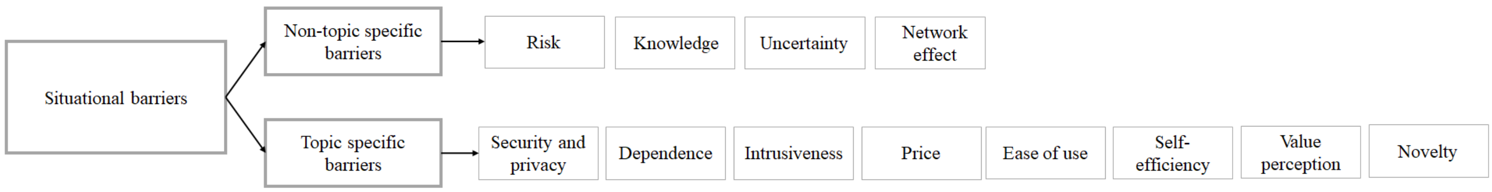


Figure 1. List of barriers

Individual traits

Individual traits have been discussed in previous research and may consist of barriers against change (Kuisma et al., 2007; Ram, 1987), social psychographic characteristics (Arts et al., 2011), openness to change (Schwartz, 1992), habits (Hurter & Rubenstein, 1978; Kleijnen et al., 2009; Oreg, 2003; Ram, 1987; Sheth, 1981), willingness to try new things (Hirunyawipada & Paswan, 2006), trait perspectives (Ram, 1987; Rokeach, 1973), and consumer characteristics (Lassar, Manolis, & Lassar, 2005; Ram, 1987). A personal trait has been defined by Hilgard, Atkinson, and Atkinson as “any characteristic by which a person differs from another in a relatively permanent and consistent way” (as cited in Hirunyawipada & Paswan, 2006, p. 184). In this thesis, individual traits will be analyzed as a moderator, effecting the relationship between the independent and dependent variable. A moderating effect has been defined by Baron and Kenny (1986) as a “variable that affects the direction and/or strength of the relation between an independent or predictor variable and a dependent or criterion variable” (p. 1174). In this thesis, individual traits are operationalized to measure consumerars readiness to technology adoption. In that regard, previous litterature states that technologies often experience a certain amount of resistance from the consumers, when they change from present ways of operating (Sathye, 1999). For consumers to change present ways of operating and adopt new technologies, the technology must fulfil a specific need (Inquiry, 1997). Assurant Inc (2017) found in their study that US consumers have a significant amount of background anxiety about the connected world, across every segment they tested. Previous research suggests that certain social-psychographic characteristics, such as innovative predisposition, opinion leadership, and risk-taking attitude, may be related to new product adoption (Midgley & Dowling, 1978; Rogers, 2010). These findings serve as a basis for why individual traits is expected to moderate the effect of barriers on IoT adoption. Furthermore, it is predicted that the manner in which consumers view and respond to new products will influence IoT adoption. Furthermore, feelings are often tested as mediating effects while psychological factors, such as individual traits are often tested as moderating effects. For instance, Van Doorn et al. (2017) used technology readiness as a moderator when discussing automated social presence (ASP) in organizational frontlines and customers’ service experiences. The authors state that an understanding of consumers technology readiness is important because of consumers potential dispositions that may influence their experience with technologies.

To measure the moderating effect, the Technology Readiness Index (TRI), developed by Parasuraman (2000) is used. According to Parasuraman (2000) the TRI index refers to “peoples’ tendency to embrace and use new technologies for accomplishing goals in home life and at work” (p. 308). This scale is used to measure individual traits as it is suggested that TRI can be used to asses’ customers technology readiness, which is important for making the right choices in terms of designing, implementing, and managing the customer-technology link (Parasuraman, 2000). This is the same objectives as this thesis have.

The TRI model is individual specific (Lin & Hsieh, 2007), compared to other models, such as the technology acceptance model (TAM) which is employee specific (Davis, 1989). The TRI model is proven to be reliable and a good predictor of technology related behavior, as there was detected differences in use of high-technology products and scores on the TRI’s four dimensions. Additionally, Rojas-Méndez, Parasuraman, and Papadopoulos (2015) which tested the cross-cultural validity of the TRI, contributed to the literature by analyzing the model in two dissimilar countries and conducting several statistical studies. Their findings add confidence in that the TRI model may be usable in other environments as well. Further, the study confirms that attitudes toward technology are good predictors of adoption, and use of technology-based products and services.

The TRI model consists of four distinct constructs, these are: *Optimism,* which means that consumers have a positive view of technology and a belief that it offers increased control, flexibility, and efficiency in their lives. Secondly, *innovativeness,* which refers to consumers having a tendency to be technology pioneers and thought leader. Third, *discomfort* express a perceived lack of control over technology and a feeling of being overwhelmed by the technology. Lastly, *Insecurity,* which concern consumers distrusts of technology and skepticism about its ability to work properly. Optimism and innovativeness is drivers of technology readiness, while discomfort and insecurity is inhibitors of technology readiness (Parasuraman, 2000).

Chapter 3: Study 1

Study 1 explores barriers against IoT adoption across segments, and tests the influence of individual trait on barriers against IoT adoption. This part of the thesis consists of a methodology section, results, and lastly a discussion of the results. Study 1 builds on the literature review presented above.

Methodology Study 1

Research type

This thesis will use primary data when analyzing the research question. More specifically, the quantitative method, questionnaire will be used. Quantitative data is research methodology that seeks to quantify the data, and typically, applies some form of statistical analysis. More specific, Study 1 uses a descriptive design, meaning that the aim is to describe something. In descriptive design one cannot prove causal relationship, only the degree of association between variables. Descriptive researched is planned and structured, where the researcher has knowledge about the problem situation and the information needed is clearly defined. The most used type of descriptive design in marketing research is also used in this thesis, namely cross-sectional design. This design involves the collection of information from any given sample of population elements only once. This approach requires a large amount of data collection and is inferior at detecting changes. However, a clear advantages is that this method reduces response bias (Malhotra, 2009).

Data collection

To obtain the data required to perform further analyses, a survey is developed. This method of data collection is used because Study 1 explores barriers against IoT adoption in a quantifying manner, and therefore requires analyses of a large sample. A questionnaire design has three objectives, these are: translate the information needed into a set of specific questions that the respondents can and will answer, motivate the respondents to cooperate and to complete the survey, as well as minimize response error (Malhotra, 2009). Measures are taken to manage the objectives. As the survey will be published on the internet, an internet sampling technique for data collection is used. Internet sampling is convenient for respondents because they can complete the survey where they want, additionally, internet sampling allows for consistency cheches by the researcher.

Furthermore, the data collection is fast and inexpensive. On the other hand, it could be difficult to reach old consumers as they might not own a computer or have internet. Additionally, heavy users of the internet may have a higher chance of being a part of the sample that is drawn from the population (Malhotra, 2009). The ethical criterions addressed by Easterby-Smith, Thorpe, and Jackson (2012) are fulfilled. More specifically, the first seven principles regarding protection of the research subjects or informants interest is counted for by taking care of the participants and following laws regarding anonymity. The last three principals concerning accuracy and lack of bias in the results are also counted for.

Questionnaire

The questionnaire focuses on consumers' perceptions and thoughts regarding Smart Devices, therefore the collected data gathers information from a consumer perspective. The scales used in this survey aims to measure all of the construct, to increase the content validity. As the scales included in the survey is carefully collected, the content validity of the survey is assumed to be high (Malhotra, 2009). The questionnaire follows a normal and logical structure where respondents are given some general information at the beginning, thereafter the respondents receive questions related to the different barriers discussed in the literature review. Furthermore, respondents are asked to answer questions regarding individual traits, and lastly some demographic questions are given (Malhotra, 2009). More specifically, the first message respondents see explain that the questionnaire is going to be used in research concerning Smart Devices, and that the survey will take approximately 15 minutes to complete. There is also given a reassurance that the questionnaire is anonymous and that there are no right or wrong answers. In the following page, a description with examples of Smart Devices are given and further, an open question is presented, asking if the respondents remember an opportunity in which they had the chance to buy a Smart Device, but did not go through with the purchase. This opening question is important because it sets the respondents confident level. There is made an attempt to make the opening question interesting and simple, so respondents want to cooperate through the survey. The theory also states that opening questions asking about respondent’s opinion is advantageous, even if the questions is not needed in the research (Malhotra, 2009).

Furthermore, respondents were asked to answer questions concerning each barrier addressed in the literature review. The questionnaire is design in a way making it possible to separate scales measuring different barriers, which hopefully will lead to a less chance of respondents guessing what is being tested, and therefore increase the construct validity of the study (Van de Ven, 2007). Respondents were first presented with questions regarding privacy concerns from an adopted scale of Mani and Chouk (2016). Thereafter respondents were asked to answer questions regarding collection, unauthorized secondary use, and improper access, all scales adopted from Hsu and Lin (2016). An intrusiveness scale and an dependency scale, both adopted from Mani and Chouk (2016) was also included in the survey. Additionally, the ease of use scale was adapted from Kuisma et al. (2007); Laukkanen et al. (2007); H.-P. Lu et al. (2005), were minor changes were made to the scale. Self-efficacy was measured on a adopted scale from Mani and Chouk (2016). Furthermore, perceived critical mass, and perceived compatibility was adopted from Hsu and Lin (2016), while number of IoT services, and perceived complementarity was adapted from the same source, meaning that small changes to these scales were conducted. A page break was added before the next scale measuring novelty was presented. The novelty scale was adapted from Campbell and Goodstein (2001); D. Cox and Cox (2002); D. S. Cox and Cox (1988); Dimofte, Forehand, and Deshpande (2003), meaning that small changes was done with the scale. The value perception barrier was also adapted with minor changes from Kleijnen, De Ruyter, and Wetzels (2007); Meyers-Levy and Peracchio (1995); Voss, Spangenberg, and Grohmann (2003). Furthermore, respondents were asked to answer questions regarding price, a scale adopted from Haws and Bearden (2006). As novelty, value, and price was measured through a bipolar scale, a page break was added after respondents had answered these questions. Note that the uncertainty barrier scale and the novelty barrier scale where merged. Meaning that the last three questions on the novelty bipolar scale is measuring uncertainty. This decision was made as these questions fit together, and as the three variables measuring uncertainty was uncorrelated. Additionally, the questionnaire was quite long, and merging the two scales was one of the measures taken to make the survey shorter.

Respondents were further presented with questions regarding the dependent variable, adoption of IoT devices, measured through intention to buy (Mano & Oliver, 1993), and Word Of Mouth (WOM) intention (Arnett, German, & Hunt, 2003; Rogers, 2010; Voorhees, Brady, & Horowitz, 2006). Thereafter, respondents were presented with questions measuring risk on a scale adopted from Laroche, Yang, McDougall, and Bergeron (2005); R. N. Stone and Grønhaug (1993), and questions measuring knowledge, on a scale adopted from D. C. Smith and Park (1992). The scales for knowledge and risk are presented after the dependent variable's (purchase intention and WOM intention). The decision is made partly because this was the only place they fitted and partly because they are replicates of other questions included in the survey. This means that the knowledge and risk scales enforce other questions in the survey. After respondents had answered every scale measuring barriers they were presented with questions measuring individual traits. As mentioned in the literature review, individual traits was measured on the Technology Readiness Index (TRI) adopted from Rojas-Méndez, Parasuraman, and Papadopoulos (2017). TRI consist of four subscales, namely optimism, innovativeness, discomfort, and insecurity.

Every scale assessing barriers, dependent variable's, and individual traits are measured on a 7-point Likert scale, labeled strongly disagree to strongly agree. This is also applicable for the novelty, value perception, and price scales, which are measured on a bipolar scale, ranging from 1 to 7. As Likert scale is the scale that is most widely used in marketing research, there is also reason to believe that this scale is applicable in this thesis. The Likert scale is normally on an interval or ratio measurement level, meaning that one can detect characteristics of description, order, and distance. The scale requires respondents to indicate a degree of agreement or disagreement whit each barrier. As it is easy for respondents to understand how to use the Likert scale, it is suitable for electronic distribution. On the other hand, Likert scales may take longer to complete than other itemized scales because respondents need to read each statement. In addition, it may be difficult to interpret the response to a Likert item, especially if it is an unfavorable statement (Malhotra, 2009). In line with previous research, the respondents expressed how many and which Smart Devices they own. This question is included in the questionnaire as the results of Study 1 may depend on wheatear respondents owns Smart Devices or not (Karahanna, Straub, & Chervany, 1999). Lastly, respondents were asked some demographic questions and thanked for completing the questionnaire. The demographic questions are measured on nominal, ordinal, and ratio measurement level. To minimize missing values, each question in the survey has “force response”, meaning that all questions in the survey need to be answered for the respondents to complete the survey. The question wording has also been evaluated to avoid leading and bias questions, as well as implicit alternatives, assumptions, generalization and estimates. Ordinary and unambiguous words have been used, and issues has been defined, such as the definition of Smart Devices in the beginning of the survey (Malhotra, 2009). Some questions are reversed meaning that they have a different direction than the rest of the questions included in the survey. When the reversed scale has a high score (7) it entails a bad thing, and not a good thing. The complete questionnaire can be found in the appendixes.

Sampling

This thesis’ target population is people older than 18 years from the general population. The population is not restricted to any geographical areas as it is made an attempt to detect differences in barriers across countries. One disadvantage of this decision is that there might be differences in countries in terms of accessibility of Smart Devices which can affect the results. These potential differences are not considered as influential since a convenience sample technique is used, and therefore the respondents would most likely be people from the developed world. The minimum age is 18, since all the respondents need to be legal. Since the sample is drawn from the population, the sample will be: the general population above 18 years old. The sampling unit is the same as the sample. A traditional sampling method is used, meaning that the entire sample is selected before the data collection begins (Malhotra, 2009). The sample is targeted mainly through Facebook, both from my personal account but also in specific groups that are interested in IoT, Smart Devices etc. Additionally, the survey is distributed online on forums and survey swap websites. The data was gathered from 23.03.2018 to 12.04.2018, through the Easter holiday. During the same period (17.03.2018) the Facebook-Cambridge Analytica data scandal was extensively discussed in media. The scandal involves collection of personally identifiable information from Facebook, allegedly used to influence voter opinion on behalf of politicians who hired Cambridge Analytica (Rosenberg, Confessore, & Cadwalladr, 2018). This might have influenced my results, as the study addresses improper access and unauthorized secondary use (privacy and security barrier) in particular. However, it is expected that some consumers have concern over privacy and security in general, and that the Facebook-Cambridge Analytica data scandal have not influenced every consumer.

Sampling method

This thesis is using a non-probability sampling method, meaning that the probability of any member of the population being chosen for the sample is unknown. In other words, the selection of elements from the population is non-random, rather the selection relay on the researchers' personal judgment. Using this technique may yield good estimates of the population characteristics, however, they do not allow for objective evaluation of the precision of the sample results. This sampling method is chosen because of the limited resources available. The drawback of using a non-probability sample is that the results may not be generalized to the whole population (Malhotra, 2009). On the other hand, this is an exploration of barriers against IoT adoption, and at this point in the thesis it is more important to detect possible barriers.

From several types of non-probability sample techniques, convenience sampling is chosen. Convenience sampling attempts to obtain a sample of convenient elements, were the selection of sampling units is left primarily to the researcher. This method of sampling is chosen because it is the most convenient sampling method which requires least time and costs. Furthermore, the sampling units are accessible and easy to measure. However, the disadvantages of using this sampling method is that many sources of selection bias are present, including respondent self-selection. Additionally, the results will not be representative for the definable population, hence it is not theoretical meaningful to generalize to any population (Malhotra, 2009). As Study 1 will serve as a basis for the second study conducted in this thesis, this method is chosen to be able to proceed to the second study. Additionally, limited resources have been available (e.g. time and money).

Sample size

There has not been used any quantitative methods to determine sample size, however, several qualitative methods for sample size determination has been used. These are, nature of analyses, number of variables, completion rates, and resource constraints (Malhotra, 2009). Since this thesis aims to detect barriers against IoT adoption, the nature of the analyses implies that a large sample size is needed. Additionally, the questionnaire consists of many variables which requires larger sample. However, as there was not given any incentives to complete the survey, and because the survey was quite long, the completion rate was expected to be fairly low. Sample size used in similar studies ranges between 150 and 500 respondents (Hsu & Lin, 2016; Littler & Melanthiou, 2006; Mani & Chouk, 2016; Ram, 1989), where researchers collecting a large sample commonly have more recourses available. Based on these qualitative methods for sample size determination the initial sample size was determined to be 200 respondents. However, after the survey had been published for a while, it proved itself to be difficult to collect 200 respondents. Reasons for this may be that the survey was quite long, that the survey was distributed during the Easter holidays, and as respondents were not given any incentives to complete the survey. Therefore, the sample size collected was decreased to 150 respondents. Respondents motivation to complete the survey was quite low, which is reflected by the high drop-out rate (126 respondents). This may also serve as another indicator of a long survey. A long survey may lead to inability error to occur, meaning that respondents do not have the ability to provide accurate answers because of fatigue and boredom (Malhotra, 2009). However, it is expected that these respondents rather drop-out than complete the survey with answering randomly, as the drop-out rate was quite high and because respondents do not get any reward for completing the survey.

Reliability and validity

According to Malhotra, researchers have an ethical responsibility to use scales that have reasonable reliability, and validity. Accordingly, in this thesis there will be conducted reliability and validity checks of the studies. Reliability refers to the extent to which a scale produces consistent results if repeated measurements are made on the same characteristics (Malhotra, 2009). Several methods exist to asses' reliability, this thesis uses internal consistency and Cronbach alpha to test the 23 scales' reliability. Internal consistency is an approach for assessing the internal consistency of a set of items when several items are summated in order to form a total score for the scale. Cronbach alpha is one method for testing internal consistency, Cronbach alpha is the average of all possible spilt half coefficients resulting from different splitting's of scale items. The coefficients vary from 0 to 1 and a score of .6 and lower generally indicates unsatisfactorily internal consistency reliability (Malhotra, 2009). Furthermore, in three cases, scales included in this thesis only consists of two items, for these scales a correlation study will be conducted instead of Cronbach alpha to assess reliability. Correlation studies is the simplest way to understand the association between two metric variables. As Person correlation coefficient is most widely used in research, it is also used in this thesis. The Person correlation coefficient indicates the degree to which the variation in one variable is related to the variation in another variable (Malhotra, 2009).

Furthermore, validity refers to the extent to which differences in observed scale score reflects true differences among objects on the characteristic being measured, rather than systematic or random errors. The literature discusses several types of validity, namely content, criterion and construct validity. Construct validity is subsequently divided into convergent, discriminant, and nomological validity (Malhotra, 2009). To assess validity in Study 1, factor analyses is conducted on the scales which have been changed from its original source. More specifically, exploratory factor analyses are used. This approach uncovers the underlying structure of a relatively large set of variables and are commonly used by researchers when developing scales (Malhotra, 2009). The extraction method chosen for these analyses was maximum likelihood, which is often used in marketing research. Further, Promax, a non-orthogonal (oblique) rotation is chosen as it allows for factors to correlate, which can simplify the factor pattern matrix (Malhotra, 2009). To determine the number of factors prior determinations, eigenvalues and scree plot are used (Malhotra, 2009).

Analyses

The following analyses will be conducted to address barriers against IoT adoption. After making the data set ready, some preliminary analyses are being performed, namely *Cronbach alpha* and *correlation* studies for reliability and *factor analyses* for validity checks. As mentioned above, factor analyses are conducted on scales that have been changed from its original source. Furthermore, *descriptive statistic* is performed to gain knowledge about the respondents. The descriptive analyses included are mainly conducted on demographic questions, but there will also be provided a discussion of the open question included in the survey.

The main analyses in Study 1 is a *cluster analysis*, performed to classify objects or cases into relatively homogenous groups called clusters. Objects in each cluster tend to be similar to each other and dissimilar to objects in the other clusters (Malhotra, 2009). A tandem method combining hierarchical and non-hierarchical clustering analysis was used to explore barriers against IoT adoption and to examine wheatear these barriers differ between segments. K-means was used as the non- hierarchical clustering method to create an improved solution (Malhotra, 2009). Before conducting the analyses, all variables were transformed to aggregated variables, meaning average scores for every scale for each of the 150 responses, these was used in the cluster analyses.

Following the tandem method of cluster analyses, hierarchical clustering was performed first, which develop a hierarchy like structure of the data. Agglomerative clustering, which is one form of hierarchical clustering, is chosen as it is commonly used in marketing research. This method starts with having objects in separate clusters, and thereafter forms clusters by grouping objects into bigger and bigger clusters. This procedure is continued until all objects are members of a single cluster. The clustering algorithm, Ward's method is chosen with Squared Euclidian distance, to effectively determine the number of clusters. To determine the number of clusters, an examination of agglomeration coefficients and the dendrogram was performed (Malhotra, 2009). The second step in the tandem method of cluster analyses consist of a non-hierarchical clustering method, namely K-means. In the hierarchical clustering method, the prespecified number of cluster found in the hierarchical clustering is used. Conducting K-means analysis is fast, and the method had merit with large objects. However, the selection of cluster centers may be arbitrary as clustering centers might depend on how the centers are selected (Malhotra, 2009). Number of clusters in the hierarchical clustering are decided based on relative sizes of clusters and the significant levels of the dimensions in the ANOVA table (Malhotra, 2009). This will be discussed more closely in the results part of this thesis.

After conducting some preliminary analyses, a special sample was detected, whereas the respondents are very similar in terms of demographics, knowledge regarding Smart Devices, innovativeness, and number of Smart Devices they own. This made the clustering difficult, as it was hard to detect differences between segments. Because of this, some variables are used in the clustering analysis and the rest of the variables are included as so called descriptive variables, still explaining differences between segments. To asses' these descriptive variables a *one-way ANOVA analysis* is conducted, based on the analysis' robust design, and because it decreases random variability. The ANOVA analysis examines the differences among means for two or more populations, whereas Study 1 examines differences in means between the descriptive variables and the clusters. A post hoc test is also included, to be able to examine which levels are responsible for any factor effect. The post hoc test Turkey is chosen as it is a reliable test and because equal variances are assumed (Janssens, De Pelsmacker, & Van Kenhove, 2008).

Results Study 1

Preliminary analyses

A data cleaning procedure were performed, before any analyses was conducted. Every respondent that did not complete the questionnaire was deleted. In addition, there where one respondent that had used more than one day to complete the questionnaire, this respondent was also deleted. The data did not have any outliers, therefore no respondents were deleted for this reason. To check for the scales' reliability and validity Cronbach alpha, correlation studies and factor analyses was conducted. The results of these preliminary analyses will be discussed in the following sections.

Factor analyses

In this thesis exploratory factor analyses are used to measure the validity of the scales included in the survey that was changes from its original source (Malhotra, 2009). These barriers are ease of use, number of IoT services (network effect), perceived complementarity (network effect), novelty, and value perception (appendix). The results of the factor analyses conducted on ease of use, number of IoT services, and perceived complementarity separately showed that the three scales consisted of one factor each. This means that the validity for the scales is satisfactory and that reliability tests can be conducted. For the value perception scale the scree plot (appendix) showed that the scale consisted of two factors. The scale also had two factors whit eigenvalues above one, supporting the decision to create two factors instead of one. Similarly, the novelty scale also consisted of two factors, determined by the scree plot and eigenvalues above one (appendix). This is not surprising, especially for novelty as this scale was merged with the uncertainty scale. Since two factors were found for both the novelty and value perception scales, new scales needed to be developed in these cases (Malhotra, 2009). Novelty 1 consists of the following items: new/old, original/unoriginal and unusual/common, while novelty 2 consists of familiar/novel, typical/atypical, stable/unstable, and developed/undeveloped. Further, one bipolar question was removed (questionable/unquestionable). As mentioned, uncertainty and novelty scales has been merged, therefore novelty 2 also consist of some uncertainty variables. The difference between novelty 1 and novelty 2 is that novelty 1 perceive the Smart Device's uncommonness or commonness, while novelty 2 concerns the performance and the Smart Device's normalness or non-normalness. Furthermore, value perception was also divided into two factors whereas value perception 1 consists of the following items: ineffective/effective, not functional/functional, impractical/practical, useless/useful, inefficient/efficient, unproductive/productive, and not helpful/helpful, and value perception 2 consists of the following items: boring/exciting, not a worth wile product/ a worth wile product, unappalling/appalling, and common/unique. An assessment of the items included in each factor show that value perception 1 concerns the Smart Devices' advantageousness, and value perception 2 concerns respondents' perception of Smart Devices' attractiveness. Some items were also removed, these are: not necessary/necessary and poorly made/well made. The validity of the scales included in the survey is satisfactory, therefore reliability analyses can be conducted.

Cronbach alpha

As discussed previously Cronbach alpha analyses is conducted to assess scales reliability (Malhotra, 2009). These analyses were conducted on each scale included in the questionnaire. The following scales had an Cronbach alpha score greater than .80: improper access (privacy and security) (3 items; $\alpha = .82$), intrusiveness (5 items; $\alpha = .86$), ease of use (5 items; $\alpha = .93$), number of IoT services (network effect) (3 items; $\alpha = .91$), perceived critical mass (network effect) (4 items; $\alpha = .96$), perceived compatibility (network effect) (3 items; $\alpha = .91$), perceived complementarity (network effect) (3 items; $\alpha = .84$), value perception 1 (7 items; $\alpha = .93$), intention to buy (3 items; $\alpha = .97$), WOM intention (4 items; $\alpha = .91$), knowledge (4 items; $\alpha = .88$), optimism (individual trait) (3 items; $\alpha = .83$), innovativeness (individual trait) (5 items; $\alpha = .91$), and insecurity (individual trait) (5 items; $\alpha = .81$). Elimination of items in these scales to increase alpha is not necessary, therefore summated scales can be calculated immediately (Janssens et al., 2008). These scales also have a satisfying internal consistency reliability as an alpha above .8 is an indicator of internal consistency reliability (Malhotra, 2009). Furthermore, results show that the scales for unauthorized secondary use (privacy and security) (3 items; $\alpha = .69$), dependence (4 items; $\alpha = .78$), novelty 1 (3 items; $\alpha = .73$), and novelty 2 (3 items; $\alpha = .80$) had an alpha above .60. In cases like this, one should evaluate if removing items will increase the alpha remarkable. For these four scales, removing an item would not increase the alpha remarkable, and because an alpha above .60 is acceptable summated scales where calculated (Janssens et al., 2008).

In the case of the last four scales (self-efficacy, value perception 2, price, discomfort (individual trait), some items were removed, these will be discussed in the following section. Initially, self-efficiency consisted of three items ($\alpha = .86$), however by deleting one item the alpha increased remarkable (2 items; $\alpha = .94$). Similarly, price consisted of eight items ($\alpha = .85$) still having a high alpha, however by removing one item the alpha increased remarkable (7 items; $\alpha = .93$). Value perception 2 had a fairly low alpha (4 items; $\alpha = .75$), therefore one item was removed, and the alpha score increased to an acceptable level (3 items; $\alpha = .86$). Lastly, the discomfort scale (individual trait) performs poor in general. The initial alpha was low (6 items; $\alpha = .51$), however removing one item increased the value to an acceptable level (5 items; $\alpha = .67$). However, the alpha still has a fairly low score (Janssens et al., 2008).

Correlation

As mentioned above, correlation studies was conducted on scales consisting of only two variables (Malhotra, 2009). These scales are concern for privacy issues (privacy and security), collection (privacy and security), and risk. Results for privacy concern (privacy and security) shows that the two variables measuring this scale were significantly correlated, $r = .86$, $p < .001$. The Pearson correlation coefficient is close to one, which means that there is a strong relationship between the two variables. Furthermore, a Pearson correlation coefficient close to one also means that changes in one variable is strongly correlated with changes in the second variable. Additionally, the coefficient is positive, meaning that if one variable increase in value, the second variable will also increase in value, and opposite. Furthermore, assessing collection (privacy and security) results show that there is a statistically significant correlation between the two variables measuring collection, $r = .88$, $p < .001$. Lastly, the one-tailed Pearson correlation coefficient for risk show a statistical significant correlation between the two variables measuring risk, $r = .75$, $p < .001$. However, the correlation value is lower than the two other correlations, but still fairly close two one (Janssens et al., 2008).

Descriptive

The sample analyzed in Study 1 have the following demographics: 59% of the respondents are women, most of the respondents are aged between 18 and 30 years old (75%). 45% of respondents are undergraduate educated people, while 37% are graduate educated respondents. As much as 62% of the sample are students, while only 29% are employees. Approximately half of the respondents are Norwegian (49%), and the other half of respondent's nationality varies much, where no other countries where especially prominent. The demographics is summarized in the appendix.

As mentioned, the survey included an open question to attain information about respondents believes. This open question asked if respondents could recall a recent opportunity in which they had the possibility to buy a Smart Device, but did not go through with the purchase. Respondents were also asked to explain why they did not purchase the device and what kind of Smart Device it was. A summary of the answers is given in the table 2, which show that price (40%) is a huge concern for respondents. This result may not be too surprising as the majority of respondents in this study is young consumers, which often have a low budget. The second highest reason for not to purchase a Smart Device is no need (13.3%), followed by no need to upgrade (12%). Interestingly, most of the reasons for why respondents did not buy the Smart Device, is addressed as barriers in this thesis.

Table 2

Qualitative comments to barriers against Smart Devices, ordered by category

Category	**% of respondents**	**Qualitative comments**
Price	40%	- HomePod, due to price vs. student payout. Will buy 3 when start working. - Alexa add on that enables you to turn on/off lights. I did not purchase it because I thought it was extremely expensive.
No need	13.3%	- When I brought my new iPhone, they offered me an iWatch at a discounted price, but I didn't want it because firstly I had just spent a lot of money on a new phone, secondly, I think the iWatches are unattractive and thirdly I have no need for one of them, I think they are a bit pointless if you have a phone and a watch.

		- I could have purchased a smart Tv however I am currently happy with my normal television as I can access many things via my laptop. I feel it was going to be unnecessary.
No need to upgrade	12%	- Could have bought a Galaxy S9, but didn't because I have the Galaxy S8 and I didn't see much difference between the two.
Wait for new better version or better functionalities	0.80%	- Apple Smart Watch version 3. I did not buy it because version 4 or 5 will soon arrive with even better functionality. - Fitness tracker. Too limited functionality. Need many devices for all my needs. - Smart watch, because the technology isn't quite there yet. There are too many tradeoffs. - I will wait until there is one watch that scores good on "all" parameters... Design, GPS, sim card, nfc, apps... Etc...
Likes traditional products	0.33%	- Calendar, I rather want to use almanac on paper. - I don’t like to try new products, I just want to use what I am used to.
Knowledge	0.33%	- A sales person wanted to sell me something at the store but I did not understand what it was.
Privacy and security	0.28%	- Surveillance camera for my home. I didn’t purchase it because it could violate my children’s privacy rights. - Smart door handle (numbers instead of key), did not buy because fear of someone can break into the house easier.
Reliability	0.13%	- Door lock as I am not sure it is reliable.
Technology is scary	0.13%	- I had an upgrade due on my cell phone contract, I decided to stick with what I have because technology is becoming for advanced and actually scary, newer devices cause more harm the more advanced they get.

Note: other reasons for non-purchasing was also mentioned, but not included in the table as there were only one respondents which states these reasons.

Main analyses

The main analysis conducted in Study 1 is a cluster analysis. Also, a One-way ANOVA is conducted to detect differences between segments. These analyses will be discussed in the following sections.

Cluster analysis

A cluster analysis was performed to analyze the presence or absence of different barriers consumers may have to IoT adoption. Additionally, this analyze was performed to test if the barriers against IoT adoption differ between segments. As mentioned, a tandem method of clustering is used, meaning that both a hierarchical and a non-hierarchical clustering analyses is performed (Malhotra, 2009). The cluster analyses – both the hierarchical and non- hierarchical – consisting of all metric variables was conducted multiple times because the results always showed a cluster solution where one cluster had very few respondents and the rest of the clusters consisted of several respondents. This result was consistent through any number of cluster solutions that was tested. Further, doing the same analysis without the dependent variables (adoption, measured through purchase intention and WOM intention) gave the same result. A more thorough analysis of the descriptive statistics showed the evidence of a special sample, as respondents are very similar in terms of knowledge (cluster 1: M = 4.46, SD = 1.63; cluster 2: M = 4.23, SD = 1.19), innovativeness (cluster 1: M = 4.59, SD = 1.71; cluster 2: M = 4.48, SD = 1.33), and how many Smart Devices they own (cluster 1: M = 3.70, SD = 1.41; cluster 2: M = 3.97, SD = 1.54). Additionally, most of the respondents are between 18 and 30 years old (75%) and students (62%), where other demographic groups are weakly represented. In other words, this is a homogenous and small sample. A further problem with the initial cluster analysis was that some of the scales included in the survey was reversed, meaning that they have a different direction than the rest of the scales. There were also detected some confounding variables as respondents scored at the low end on some scales and at the high end on some scales. This made the clustering difficult, as it was hard to detect differences between segments.

Conducting cluster analysis with only some of the scales measuring barriers, solved the problem with the special sample. As Study 1 is a preliminary study, used in an explorational way, it was decided to analyze the special sample instead of collecting new data to be able to proceed to the second study. Variables included in the final cluster analyses are the four subscales of privacy and security: privacy concern, collection, unauthorized secondary use, and improper access. Further, intrusiveness, dependency, and price are included, as well as novelty 1, novelty 2, value perception 1, and value perception 2. The variables included in the analyses is viewed as the most important barriers against IoT adoption. All of the variables included in the final cluster analysis is topic-specific barriers. Additionally, these scales also showed to have the biggest difference between segments.

The hierarchical clustering method conducted on the 11 barriers mentioned above, gave a 2-cluster solution. This is based on the agglomeration schedule, and dendrogram. The agglomeration schedule (appendix) shows a big jump in coefficients from stage 148 to stage149, suggesting a 2-cluster solution. The icicle plot displays this graphically. Further, the distances between objects, shown in the dendrogram, provide an indication of the appropriate number of clusters. Read from the left to the right, the dendrogram also suggests a 2-cluster solution (Janssens et al., 2008). Subsequently, a non-hierarchical clustering method (K-means) was conducted to create an improved solution. The same 11 variables used in the hierarchical clustering is also used in this K-means cluster analyses. This non- hierarchical, K-means technique was used to develop a 2-cluster solution, which corresponds to the number of cluster groups input under the hierarchical clustering. In determining the final number of clusters, the relative size of the cluster is assessed. Cluster 1 consist of 90 respondents while cluster 2 consists of 60 respondents, this is satisfying. Furthermore, the ANOVA analysis (appendix) shows that every variable is significant, except from novelty 1, meaning that this dimension has the least impact on the formation of clusters (Janssens et al., 2008). The K-mean clustering analysis supports the hierarchical clustering analysis, and the final cluster solution is therefore two. The variables not included in the cluster analyses will serve as descriptive variables, still explaining differences between segments. To asses' the descriptive variables a *one-way ANOVA analysis* is conducted, discussed below.

ANOVA

As the literature suggests, it is often helpful to profile clusters in terms of variables not used for clustering (Malhotra, 2009). Because of the special sample, some variables where excluded from the clustering analyses. These variables will serve as descriptive variables, used to describe the different clusters. To get an overview of the variables not included in the cluster analyses, a one-way ANOVA analyses was conducted. The descriptive variables are: ease of use, self-efficiency, network effect's four subscales, knowledge, risk, and the number of Smart Devices the respondents own. Additionally, the dependent variables' purchase intention and WOM intention, as well as the individual traits' four subscales, are not included in the analyses. The one-way ANOVA analysis (table 3) indicates that there are significant difference between the two clusters in terms of purchase intention, $F(1,148) = 6.93$, $p = .009$, and WOM intention, $F(1,148) = 9.77$, $p = .002$. Interestingly cluster 2 have a higher purchase intention and WOM intention than cluster 1. Furthermore, the ANOVA analysis indicates that there are significant differences between cluster 1 and cluster 2 in terms of risk, $F(1,148) = 7.00$, $p = .009$, optimism, $F(1,148) = 4.95$, $p = .028$, discomfort, $F(1,148) = 19.00$, $p < .001$, insecurity, $F(1,148) = 21.55$, $p < .001$, self-efficacy, $F(1,148) = 4.96$, $p = .027$, number of IoT services, $F(1,148) = 5.72$, $p = .018$, and perceived compatibility, $F(1,148) = 7.08$, $p = .009$. As these barriers are significant, they describe the differences across segments best. Another finding worth mentioning is that consumers in the two segments do not differ considerably in terms of the four sub categories of individual traits (optimism, innovativeness, discomfort, and insecurity). Therefore, it is assumed that individual traits do not moderate the effect of barriers on IoT adoption. As the two segments do not differ significantly in regard to individual traits, there has not been performed analyses to check for a moderating effect of individual traits.

Table 3

Consumer's characteristics based on clustering variables and descriptive variables

		Clusters					Total
		Smart Device Likers	Smart Device Lovers				
	Cluster size	90	60				150
		Cluster 1 (SD)	**Cluster 2 (SD)**	**F**	**df**	**P**	**M (SD)**
Clustering variables	Privacy concern	5.60 (.99)	2.65 (1.00)	315.96	148	.000	4.42 (1.76)
	Collection	5.74 (.98)	2.76 (1.06)	314.90	148	.000	4.55 (1.78)
	Unauthorized secondary use	6.67 (.56)	6.11 (1.12)	16.43	148	.000	6.44 (.87)
	Improper access	6.51 (.67)	5.76 (1.05)	31.71	148	.000	6.21 (.99)
	Intrusiveness	3.47 (1.25)	2.11 (.83)	54.86	148	.000	2.92 (1.29)
	Dependency	4.23 (1.43)	3.00 (1.24)	35.04	148	.000	3.74 (1.38)
	Price	3.89 (1.29)	4.40 (1.06)	3.36	148	.013	4.09 (1.23)
	Novelty 1	3.23 (1.43)	3.26 (1.16)	0.03	148	.874	3.24 (1.32)
	Novelty 2	3.51 (1.43)	2.67 (1.08)	15.02	148	.000	3.18 (1.36)
	Value perception 1	5.54 (1.25)	6.20 (.74)	13.49	148	.000	5.80 (1.12)
	Value perception 2	5.32 (1.19)	5.87 (.87)	9.52	148	.002	5.54 (1.11)

Descriptive variables	How many Smart Devices do you own?	3.7 (1.41)	3.97 (1.54)	1.20	148	.276	3.81 (1.46)
	Purchase intention	5.37 (1.61)	5.99 (1.07)	6.93	148	.009	5.62 (1.45)
	WOM intention	4.59 (1.56)	5.31 (1.05)	9.77	148	.002	4.88 (1.41)
	Risk	3.67 (1.61)	2.99 (1.39)	7.00	148	.009	3.40 (1.56)
	Knowledge	4.46 (1.63)	4.23 (1.19)	.82	148	.367	3.70 (1.47)
	Optimism	5.17 (1.34)	5.61 (.95)	4.95	148	.028	5.34 (1.21)
	Innovativeness	4.59 (1.71)	4.48 (1.33)	.18	148	.675	4.54 (1.57)
	Discomfort	4.10 (1.02)	3.39 (.94)	19.00	148	.000	3.82 (1.05)
	Insecurity	4.23 (1.37)	3.23 (1.18)	21.55	148	.000	3.83 (1.38)
	Ease of use	5.45 (1.36)	5.7 (.92)	2.80	148	.096	5.59 (1.21)
	Self-efficacy	5.84 (1.40)	6.2 (.88)	4.96	148	.027	6.02 (1.24)
	Numbers of IoT services	5.70 (1.34)	6.18 (.98)	5.72	148	.018	5.89 (1.23)
	Perceived critical mass	5.81 (1.52)	5.89 (1.26)	.12	148	.735	5.84 (1.42)
	Perceived compatibility	5.06 (1.52)	5.67 (1.12)	7.08	148	.009	5.30 (1.41)
	Perceived complementary	5.90 (1.21)	6.14 (.92)	1.74	148	.189	5.99 (1.10)

Discussion Study 1

As the results show, the sample used in Study 1 is a special sample, as the respondents are quite similar. This will also be clearer during the discussion of the two different clusters, as there are few differences that really distinguish the two clusters. Anyway, there are some interesting differences between the clusters, and these will be discussed in the following section. This discussion will also serve as the basis for Study 2, which will build on Study 1.

Cluster descriptions

In the following part a cluster description will be given. The description is based on both the clustering variables (privacy and security, intrusiveness, dependency, price, novelty 1, novelty 2, value perception 1, as well as value perception 2) and descriptive variables (ease of use, self-efficiency, knowledge, risk, purchase intention, WOM intention, individual traits, and the number of Smart Devices the respondents own). Cluster 1 is named Smart Device Likers and cluster 2 is named Smart Device Lovers, the reasoning behind this is discussed below.

Cluster 1 - Smart Device Likers

Cluster 1 is named Smart Device Likers because they think Smart Devices is advantageous (value perception 1), somewhat attractive (value perception 2), easy to use (ease of use), and they generally believe that their ability to use Smart Devices is good (self-efficiency). However, these consumers are concerned for privacy and security threats, specifically collection of personal information, unauthorized secondary use, and improper access. Still, Smart Device Likers mostly associate devices with non-intrusiveness and they do not associate

Smart Devices with a lot of risk. Furthermore, these consumers own approximately 4 (M = 3.70, D = 1.41) devices each on average, which is quite a lot. The cluster analyses show that consumers in cluster 1 are moderately dependent (dependency) on Smart Devices, which implies that dependency may be a barrier against IoT adoption.

This segment finds the price more unfair than fair, but still acceptable. On the other hand, this segment consists of a higher portion of employed (32.3%) people than cluster 2 (25%), which do not have any price concerns, therefore it was expected that cluster 1 would not have any price concerns. Even though cluster 1 have a higher employee rate, this segment still consists of many students (56.7%). In line with these findings, most of cluster 1's consumers are between 18-30 years old (68.9%). However, this cluster still consist of older consumers (31- above 60: 31%), whereas the rates are much higher than cluster 2 (31- above 60:17%). The education levels of consumers in cluster 1 range between master degree (38.9%), and bachelor degree (43.3%). A summary of the demographics is provided in the appendixes.

Cluster 1 perceive Smart Devices as neither normal or unnormal, and believe that these devices' performance is average (novelty 2). Smart Device Likers perceive Smart Devices as slightly novel. As previous research has found a negative impact of novelty on consumer resistance to Smart Devices (Mani & Chouk, 2016; Wells et al., 2010), there is reasons to imply that novelty have a positive effect on adoption, and therefore are novelty 1 not a barrier against IoT adoption for this segment. Even if cluster 1 perceive Smart Devices as something new and novel, these consumers feel knowledgeable about these devices.

Smart Device Likers scores relatively high on every subscale of network effect, meaning that they find Smart Devices as both compatible and complementary. Additionally, these consumers find's relatively many situations in which they can use Smart Devices and most of their friends and family use Smart Devices. Which could be a reason for the high purchase and WOM intention. Most consumers in cluster 1 are form Norway (50%), this is a developed and fairly rich country where several people can afford Smart Devices and where these devices are available. Lastly, this segments scores relatively high on individual traits' four sub scales, meaning that this segment has a relatively positive view of technology and they have the tendency to feel fairly knowledgeable about technology issues. On the other hand, they may feel some discomfort and might be insecure when using technologies.

Cluster 2 - Smart Device Lovers

The second cluster is named Smart Device Lovers. Contrary to the initial predictions, cluster 2 are not concerned for privacy and security treats or collection of personal information. However, they are concerned for unauthorized secondary use and improper access (subscales of privacy and security). This means that these consumers do not worry about someone collecting personal information about them, but they do fear that someone whiteout permission will get access to their personal information. Therefore, cluster 2 is less concerned about privacy and security issues than cluster 1. One of the main factors that describes Smart Device Lovers is that they do not find Smart Devices to be intrusive, rather they own a lot of Smart Devices on average

(*M* = 3.97, *SD* = 1.54). Even though cluster 2 owns a lot of Smart Devices on average they are less than slightly dependent on these devices (dependency).

This cluster is characterized with the following demographics: most of consumers in cluster 2 are between 18 and 30 years old (83.3%), most of them are students (70%), with either a bachelor (48.3%) or master degree (35%). Still some consumers in cluster 1 are older, employed and with both higher and lower education. However, there are fewer older and employed consumers in cluster 2 compared to cluster 1. Smart Device Lovers also consist of a lot more women (66.7%) than men (33.3%). A summary of the demographics is provided in the appendixes.

Cluster 2 perceive Smart Devices as advantageous (value perception 1), attractive (value perception 2), and think of Smart Devices as normal products that has good performance (novelty 2). Cluster 2 find Smart Devices as easy to use (ease of use), and these consumers believe that their ability to use Smart Devices is satisfactory (self-efficiency). In line with this, cluster 2 have knowledge about Smart Devices, meaning that they could buy these devices whiteout any need to gather information and they can distinguish the quality of different devices. Also, they do not associate Smart Devices with a lot of risk, suggesting that risk is not a barrier for IoT adoption for Smart Device Lovers.

Cluster 2 perceive the price of Smart Devices to be fairly low, but still close to average. Consumers in cluster 2 owns 4 (*M* = 3.97, *SD* = 1.54) Smart Devises on average. Given the high purchase and WOM intention this is not surprisingly. Similar as cluster 1, cluster 2 perceive Smart Devices as something slightly uncommon and novel (novelty 1). In line with previous research, novelty 1 have a positive effect on IoT adoption and are therefore not found to be a barrier against IoT adoption (Mani & Chouk, 2016; Wells et al., 2010). Smart Device Lovers scores high on every sub scale of network effect, they also score higher than cluster 1. A high score on these sub scales means that network effect is not a barrier against IoT adoption, it may even be a reason for adoption. The last factor to be discussed are individual traits. Cluster 2 have a positive view of technology, but they are less innovative than cluster 1. On the other hand, Smart Device Lovers primarily do not feel any discomfort when using technologies and they do not seem to be insecure when using technologies.

Table 4

Summary of barriers and other characteristics explaining the two clusters

	Smart Device Likers	**Smart Device Lovers**
Barriers	Collection (privacy and security) Unauthorized secondary use (privacy and security) Improper access (privacy and security) Privacy and security concerns Price Dependency	Unauthorized secondary use (privacy and security) Improper access (privacy and security)

Other characteristics	More older consumers Some employees They are knowledgeable regarding SD SD do not have much risk Not insecure when operating a SD Owns 4 SD on average	Young consumers Many students Many women The network effect is very good SD is very advantageous SD is attractive High positive WOM High purchase intention Do not have problems with the use of SD Owns 4 SD on average

To sum up, cluster 2 consist of young consumer, most of them are students having either a bachelor or master degree. On the other hand, cluster 1 also consist of many young consumers (68.9%), still there are a higher portion of older consumers in cluster 1 compared to cluster 2. In line with this, many consumers in this segment are students, however, a larger portion of consumers are employees, self-employees, retired and unemployed in cluster 1 compared to cluster 2. As described in table 4, dependency and price is found to be barriers against IoT adoption for Smart Device Likers. Interestingly, all four subscales of privacy and security (concern, collection, unauthorized secondary use, and improper access) is found to be barriers against IoT adoption for Smart Device Likers. However, only improper access and unauthorized secondary use are barriers against IoT adoption for Smart Device Lovers. This is an interesting finding as Smart Device Likers has concerns for privacy and security threats in general while Smart Device Lovers only express uncertainties for someone to get access to their personal information and possible use of the information. The differences in privacy and security concerns between segments is compelling results which will be analyzed further in Study 2. Interestingly, some consumers (Smart Device Lovers) allow companies to collect personal information, while other consumers do not (Smart Device Likers). Let us call this a collection problem, the fact that only one segment is concerned about personal information collection. Is it possible to solve this collection problem? What should companies offer consumers to influence them to disclose their personal information?

Chapter 4: Study 2

Before any analysis are conducted, a discussion of the theory related to collection of personal information, benefit, and control is provided. Hypothesis and predictions are made, before an explanation of the methodology of Study 2 is provided. Thereafter, analyses are conducted and explained, lastly, a discussion of the results are given where also the results from Study 1 are mentioned.

Theory and hypothesis development

Study 2 will discuss this collection problem related to the privacy and security barrier in Study 1. Companies can target customers better and increase sales if they have customers personal information, but customers can also receive benefits from companies if they disclose their personal information. Such benefits may be personalized and relevant information from companies. However, with personal information disclosure follows concerns from consumers, such as privacy concerns (e.g. collection) and reward preferences (Y. Xu, Tan, & Hui, 2003). Researchers suggest that reasons for why consumers are afraid of personal information collection are data breaches or misuse of personal information (Martin, Borah, & Palmatier, 2017). Further reasons for why some consumers do not want to disclose their personal information to companies will be analyzed in this part of the thesis.

Multiple models asses consumers concerns about information privacy, such as the “internet users information privacy concerns” (IUIPS) model, consisting of collection, control, and awareness of privacy practices (Malhotra et al., 2004). Concern for information privacy (CFIP) developed by H. J. Smith, Milberg, and Burke (1996) is also discussed in previous literature and consist of collection, improper access, unauthorized secondary use, and error. Several of these variables will be investigated in Study 2. More specific, an experiment is being conducted, testing wheatear benefit (self/others) have positive effect on personal information collection. Additionally, it will be hypothesized that control (high/low) will moderate the effect of benefit on collection of personal information. It is assumed that benefit will affect collection of personal information in a positive way, and that self-benefit will be better than others-benefit. Further, it is predicted that high control is better than low control, and that the moderating effect of control is positive on the benefit-collection effect. In the following sections collection, benefit and control is discussed respectively. Study 2 aims to test three hypotheses, presented in the discussion below.

Collection

Collection is referred to as the degree to which a person is concerned about the amount of personal information that is being possessed by others compared to the value of benefits received (Malhotra et al., 2004). While H. J. Smith et al. (1996) have described concern for collection of personal information as “concern that extensive amounts of personally identifiable data are being collected and stored in databases (p. 172). Previous research claim that the act of data collection, whether it is legal or illegal, is the starting point of various information privacy concerns and negative effects on behavior (Lee & Cranage, 2011). In a fair exchange, consumers give up some information in return for something of value from a company. Consumers evaluates the costs and benefits associated with the transaction. Therefore, consumers will be reluctant to release their personal information if they expect negative outcomes (Cohen, 1987).

Often consumers have different opinions of what is fair and not fair concerning companies’ collection and use of personal information. The difference in perception of fairness is present because consumers perception of external conditions, personal characteristics, and past experience vary (Malhotra et al., 2004). By applying social contract theory to information privacy, the collection of personal information is considered fair when the consumer have control over the information and when the consumer is informed about the company’s intended use of the information (Malhotra et al., 2004). However, data collected for one purpose may be combined with other data and used for other purposes (Milne & Boza, 1999). In terms of the social contract theory, this is not perceived as fair.

Previous litterature presents a perception of there being too much data collection in the society (Miller, 1982; H. J. Smith et al., 1996). The growing collection of personal information has been a theme in privacy literature since the 1970s. Consumers have also observed the great quantities of personal data that are being collected, which the consumers often resent (H. J. Smith et al., 1996). More specifically, previous research has found that the majority (85.6%) of consumers want to limit the amount of personal information collected by marketers (Phelps, Nowak, & Ferrell, 2000). Further, it is argued that consumers have an individual "privacy threshold" level for the amount of information they are willing to disclose (Cespedes & Smith, 1993). A reasons for why consumers do not want to disclose personal information is fear of the information being shared with others (Cranor, Reagle, & Ackerman, 2000). More shocking is Culnan's (1995) findings which suggest that some consumers are unaware of organizations collection of consumers personal information. This is supported by Ziegeldorf et al. (2014) which suggests that consumers become less aware of when they are being tracked because data collection becomes more passive, more pervasive, and less intrusive. On the other hand, some consumers actually avoid the use of services which requires collection of personal information (Harris & Westin, 1990; Milne & Gordon, 1993). Meaning that consumers attitude toward collection of personal information is high, not only their opinion that collection of personal information is unacceptable. However, this is being analyzed in Study 2, more specific, if benefit and control can influence these consumers to disclose their personal information.

Benefit

Prior research states that providing the right rewards may induce consumers do disclose personal information to internet businesses (Tam, Hui, & Tan, 2002). Building on this, benefit is included in this thesis as a variable that could influence collection of personal information. In this thesis, benefit involves consumers disclosing personal information to a firm, and in return consumers receive a benefit based on the personal information they disclosed. Following Fisher, Vandenbosch, and Antia (2008), there is made a distinction between self-benefit and others-benefit. While self-benefit refers to consumers who receive a benefit tailored specially for them based on the personal information they disclose. Others-benefit means that a consumer discloses personal information to a company, and based on this information other consumers receives a benefit from the company. This thesis will examine if consumers share their personal information for self-interest or altruism (others-benefit), this is possible as benefit is divided into self and others. To assess self and others-benefit more closely altruism and personalization are discussed respectively.

Benefit for others may be seen as an altruistic behavior, meaning that consumers act unselfish to enhance the welfare of others (Price, Feick, & Guskey, 1995). In a privacy context this means that companies want consumers help others when they disclose their personal information. According to Tam et al. (2002) altruism is an intrinsic reward, which have been suggested to be useful to induce information disclosure. It is also stated that experience gained from an altruistic behavior is appreciated for selfish reasons. For example, companies implementing a benefit to others scheme may be able to induce consumers to disclose personal information, which the company gain from (Tam et al., 2002).

Self-benefit is a type of personalization, which is extensively discussed in previous research. Personalization is defined by Chellappa and Sin (2005) as "the ability to proactively tailor products and product purchasing experiences to tastes of individual consumers based upon their personal and preference information" (p. 181). Personalization is dependent on two factors, (1) companies' ability to acquire and process consumer information, and (2) consumers' willingness to share information and use personalization services (Chellappa & Sin, 2005). Comparing personalization with benefit, it is clear that companies also tailor self-benefits, which could be a product purchase experience based on the products a consumer purchases most frequently. Furthermore, benefit is also dependent on companies' ability to acquire and process consumers personal information, and consumers' willingness to share personal information.

As personalization can lead to positive customer response, such as increased willingness to give personal information and intention to buy, it is predicted that benefit can lead to increased intention to use and positive WOM intention. Using personalization companies can target customers on a one-to-one basis, which helps companies improving customer satisfaction, develop customer loyalty, and increase cross-selling possibilities (Alba et al., 1997; Peppers, Rogers, & Dorf, 1999). However, investments in personalized benefits may be weaken if consumer do not use services due to privacy concerns. An important question is therefore, if consumers will use services that offer personalized benefits. The literature discusses a personalization-privacy paradox, which refers to companies continued use of personalized services because they contribute positively to their business, even if consumers have negative feelings about personalization as consumers may suspect that their personal information is being collected and tracked without their knowledge (Lee & Cranage, 2011). Social exchange theory, which is commonly used to explain the efficacy of self-benefit suggest that people invest in relationships on the basis of comparative levels of costs and rewards (Blau, 1964). This means that consumers allow companies to collect their personal information when the benefits outweigh the costs of the disclosure of personal information.

Based on the discussion above, it is made a prediction that self-benefit is better than others-benefit in terms of collection of personal information. Additionally, this prediction is made based on the believe that consumers are more willing to disclose personal information if they get a benefit in return, compared to someone else getting a benefit. As stated above, even if people is acting altruistic, the reasoning for why people are acting altruistic may be for their own sake (Tam et al., 2002). Furthermore, it is expected that benefit will influence consumers to disclose their personal information to companies, as it is found that the right reward may induce consumers do disclose personal information. More specific, intrinsic reward (e.g. altruism) has been found to be useful to induce information disclosure (Tam et al., 2002), and personalization (self-benefit) can lead to positive customer response. The following hypothesis is therefore developed:

H1: *Benefit has a positive effect on collection*

Control

Even if there exist many definitions of information privacy, there is little variance in the elements of the definitions, which typically include control (Belanger, Hiller, & Smith, 2002). Similarly, in the general privacy literature, the elements of control are included in most conceptual arguments and definitions of privacy (Altman, 1975; Culnan, 1993; Kelvin, 1973; Margulis, 1977; H. J. Smith et al., 1996; Westin, 1967). For instance, Goodwin (1991) explains privacy in terms of consumer control over personal information disclosure. Information disclosure refers to how and when consumer information is captured and stored. It is stated that the aim of control is to enhance autonomy and minimize vulnerability (Margulis, 1977).

A common thread throughout the literature is to explain control in terms of consumers control over their disclosure of personal information (Johnson, 1974; Shils, 1966; Westin, 1967). More specific, Phelps et al. (2000) defines control over personal information in terms of “control over who has access to personal data (i.e. disclosure), how personal data are used (i.e. appropriation and false light), and what volume of advertising and marketing offers arises from the use of personal data (i.e. intrusion)” (p. 29). It is suggested that notice and choice create control, as it informs the consumer that personal information is collected, consumers can subsequently make a choice themselves if they want to provide their personal information at that time (Sheehan & Hoy, 2000). Malhotra et al. (2004) further discusses the principle of procedural justice which suggest that individuals view procedures as fair when they have control over the procedures. Consequently, consumers want to control and influence changes in organizational policies they find to be displeasing (Gilliland, 1993; Thibaut & Walker, 1975). Goodwin (1991) state that consumers desire two types of information control, namely dissemination control, meaning the ability to influence how marketers use personal information and environmental control, meaning the ability to influence the types and volumes of use, that results from marketers use of personal information. Other researchers have stated that control is often exercised through approval, modification, and opportunity to exit. Additionally, it is suggested that consumers should be allowed to add, delete, and modify the information in companies’ database (Malhotra et al., 2004). The newly implemented General Data Protection Regulation (GDPR) includes some of these aspects. In short, GDPR is a regulation on data protection and privacy for all individuals within EU and EEA. The aim is to provide citizens control over their personal data (Salami, 2017).

Consumers exchange of personal information can be viewed as a social contract, where consumers control is a fundamental component of a fair social contract. This social contract is considered breached if consumers are unaware of collection of personal information, or if marketers rents consumer's personal information to third parties without consumers permission. Additionally, the contract is considered breached if consumers are not given an opportunity to restrict the distribution of personal information (Culnan, 1995; Milne, 1997; Milne & Gordon, 1993). Control is especially important when consumers take high risk in the submission of personal information, such as when there is a large potential for an opportunistic behavior breach in the social contract (Malhotra et al., 2004). The importance of privacy control is further demonstrated through the American Federal Trade Commission's' current privacy policy guidelines, where control is the core of these privacy policy guidelines. Additionally, control is viewed as the most important explanation of privacy concern (Sheehan & Hoy, 2000).

Previous research have found that 85% of adults believe that controlling access to their personal information is very important (Bélanger & Crossler, 2011). Supported by, E. F. Stone, Gueutal, Gardner, and McClure (1983), which states that consumers control over their personal information is an important issue for consumers. Additionally, it is also stated that most consumers desire more control over collection and use of personal information. The reason why consumers find control important may be because control can reduce many data privacy vulnerabilities (Martin et al., 2017). However, prior research has found that consumers may disclose too much information when they perceive greater control over their personal information, which also lead to the consumers being vulnerable (Brandimarte, Acquisti, & Loewenstein, 2013). Furthermore, over 50% of respondents in a research studying information control, stated that they wanted more control over how companies used information about them (Phelps et al., 2000). The same research also found, that of six factors influencing privacy concern, type of information collected and the amount of control consumers have over future distribution of personal information, is the most important factors. Similarly, Phelps et al. (2000) state that nearly every consumers, even those who are relatively unconcerned about collection and use of personal information, desire more control over their personal information. This is consistent with Milne's (1997) findings, studying consumer participation in mailing lists. Malhotra et al. (2004) further states that online consumers consider it most important to be aware and have direct control over personal information stored in marketer's databases. Nowak and Phelps (1995) also demonstrates that people are less worried about companies' collection personal information when they give the company permission or are given the choice to exit the agreement. Interestingly, it is found that internet users are more willing to consider providing persona information when websites explicitly inform them how the information is going to be used (Sheehan & Hoy, 2000). Previous research has found that control can reduce consumers privacy concerns. Furthermore, previous research has discussed privacy vulnerability in relation to the gossip theory. This theory identifies control and transparency as two factors that reduces privacy concern. Transparency refers to consumers awareness of and details about which information is being shared about them, and is closely linked to control. The gossip theory states that consumers should have control over information use and data management decisions, which may also help consumers feel empowered in high vulnerability contexts. When consumers have control, they can determine whether they want to participate in certain forms of data sharing, which reduces uncertainty. Studies show that participants who were provided with greater control over their personal information, shared more sensitive information with a broader audience (H. Xu, Teo, Tan, & Agarwal, 2009). The same reasoning is also made by Culnan (1995), in relation to consumers sharing personal information to third parties (Milne, 1997). In line with previous research high control is predicted to be better than low control on collection of personal information (Ziegeldorf et al., 2014). Based on the above discussion the following hypothesis is made:

H2: *Control has a positive effect on collection*

It is expected that control will change the relationship between benefit and collection in a positive way, meaning that control is a moderator. This implies that the effect of benefit (IV) on collection (DV) differs at different values (high/low) of control (moderator). For instance, a consumer receiving self-benefit from a company, in addition to having high control of its personal information is predicted to be more likely to disclose its personal information than a consumer that have self-benefit and low control. The following hypothesis is therefore developed:

H3*: The positive effect of benefit on collection is positively moderated by control*

Conceptual model

The conceptual model is developed based on the discussion above. The idea is that benefit, either for self or others, is expected to influence collection of personal information in a positive way. It is further predicted that self-benefit will increase collection of personal information. Additionally, perceived control (high/low), is expected to moderate the relationship between benefit and collection. A moderator is defined by Baron and Kenny (1986) as a “variable that affects the direction and/or strength of the relation between an independent or predictor variable and a dependent or criterion variable” (p. 1174). This means that high control is hypothesized to influence the effect of benefit on collection in a positive way. Figure 2 presents these relationships.

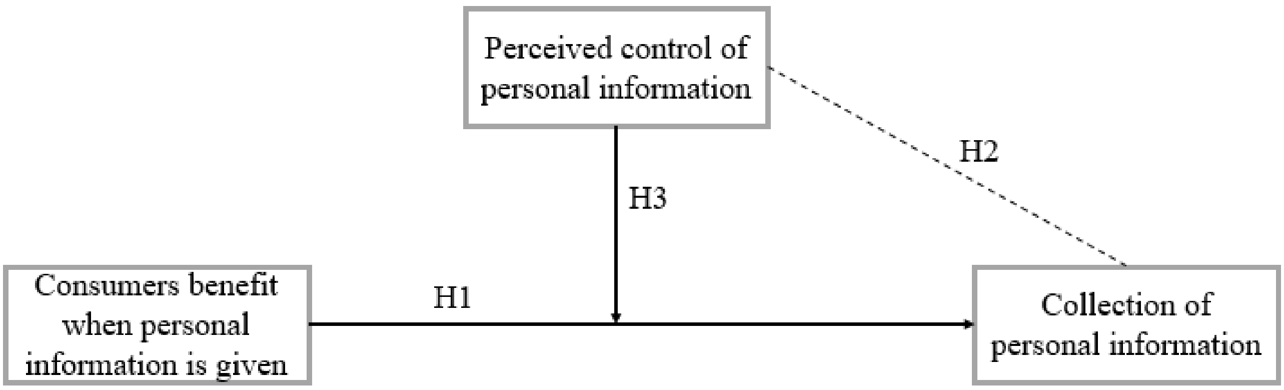


Figure 2. Conceptual model, Study 2

Methodology Study 2

Research type

Study 2 applies quantitative data as the selected research methodology, this method seeks to quantify data and typically applies some form of statistical analysis. Where a descriptive design where used in Study 1, a causal design is used in Study 2. This is a conclusive research where the objective is to obtain evidence regarding cause and effect relationships. This method is appropriate when there is a need to understand which variables are the cause and which variables are the effect of a phenomena (Malhotra, 2009). This thesis examines if benefit (self/others), and level of control (high/low) is the cause and if collection is the effect of the collection problem. However, one can only infer and never prove a cause and effect relationship. As Study 2 test the effect of two independent variables on one dependent variable, a factorial design is used. More specific, a 2 x 2 between subject factorial design is used to test for interaction between the two independent variables (benefit and control). The main method of causal research is experimentation, which is also used in this thesis. More specifically an experimentation survey is used (Malhotra, 2009).

Data collection

As mentioned above an experimentation survey is conducted to test the hypothesis presented in the theory part of this thesis. An experimental survey is classified as a laboratory experiment rather than a field experiment. A laboratory experiment is an artificial setting for experimentation in which the researcher constructs the desired conditions. This data collection method is chosen as it offers a high degree of control, therefore history effect can be minimized. The experimentation survey was distributed online containing a scenario and questions regarding the dependent and independent variables. This data collection method was chosen because it requires less resources than a field experiment and an experiment conducted in a lab. In marketing research, laboratory experiments are more common than filed experiments, which support the chosen method of data collection. Further advantages with a laboratory experiment is that it tends to produce the same results if repeated with similar subjects, meaning that the internal validity is high. Additionally, laboratory experiments require small number of test units, lasts for a shorter time, is less expensive, easier to implement and easier to conduct than a field experiment. On the other hand, laboratory experiment is conducted in an artificial environment, which can cause reactive error and respondents may attempt to guess the purpose of the experiment and respond accordingly. The artificial environment may lower the external validity and the ability to generalize the results to the real world. However, it is argued that artificiality or lack of realism does not need decrease external validity. Being aware of the differences between the lab and the real situation in which the generalization is being made, improves the external validity. The external validity is only reduced if these aspects interface with the manipulated independent variables in the experiment. Additionally, laboratory experiments allows for more complex designs than field experiments, hence one can control for more factors or variables in the lab, which increase external validity (Malhotra, 2009). Furthermore, as discussed in Study 1, the ethical criterions addressed by Easterby-Smith et al. (2012) are fulfilled.

Manipulation

The 2 x 2 between subject factorial design used in this thesis consists of control (high/low) and benefit (self/others), which was manipulated using scenarios. Every scenario consisted of the same general information, explaining the context that were used, this general information stated that the training center respondents normally train at had developed an app. Respondents were asked to give their personal information to the fictive training center through the app. A fictive training center was used so people's judgements and perceptions of a brand would not affect the participants answers. Using a between subject design, respondents were randomly selected to one of four conditions. respondents in the self-benefit condition learned that they could receive personalized training and nutrition plans. Respondents in the others-benefit condition learned that other members at the training center received tutorials regarding new training methods if the participant disclosed his/her personal information. In combination with the benefit manipulation respondents also received either low or high control over their personal information. Low control means that the training center will manage the personal information and the participants will be unaware of what it will be used for. While high control means that participants could decide which information the training center receives, how it is used, and it is easy to change the privacy settings. Additionally, a control group for the benefit manipulation was included to reduce causal factors (Malhotra, 2009). However, this control group is later removed as it was not perceived as natural in the experiment, this will be discussed in the results section of this thesis. Green Jinn's web page (GreenJinn, 2018) is used as an inspiration to write the scenarios for benefit as it explains the benefits consumers receives by using this service in a good way. All the scenarios can be seen in its entirety in the appendixes.

Measurements

After being exposed to the scenarios, respondents were asked the same questions regarding benefit, control, collection, improper access, intention to use, WOM intention, and demographic questions. To measure the control manipulation an adopted scale from H. Xu, Dinev, Smith, and Hart (2008) was used. Further, benefit where measure using two questions, simply asking the respondents to which degree they perceived a benefit for them self or others. In addition, there were added a manipulation question to check if respondents were paying attention and reading the questions carefully. The question asked the respondents to not answer this specific question. However, many respondents did answer this question and were therefore deleted. Other reasons than the respondents not paying attention could be that they clicked on the scale by an accident and could not dele the answer afterword. Additionally, even if the respondents did not read this question, they might have read the scenario and the other questions carefully. Other type of manipulation checks could rather have been used. For example, the question could rather have asked the respondents to answer seven on the scale. The dependent variable, collection was measured using a adapted scale developed by Hsu and Lin (2016). Lastly, respondents were also asked questions regarding Intention to use, WOM intention, and improper access, to obtain additional insights regarding respondent's perceptions. The intention to use scale was adopted from Davis (1989); Shin (2010), the WOM intention scale was adopted from Laroche et al. (2005); R. N. Stone and Grønhaug (1993), while the improper access scale was adopted from Hsu and Lin (2016). All questions where measured on a 7-point Likert scale ranging from strongly disagree to strongly agree. A Likert scale requires respondents to indicate a degree of agreement or disagreement whit each statement related to the objects. As it is easy for respondents to understand how to use the Likert scale, it is suitable for electronic distribution (Malhotra, 2009). Furthermore, the order of the questions included in the experimentation survey is evaluated, the scale of the dependent variable (collection) is presented first to decrease the chance of other questions influencing respondent's answers to the dependent variable (question order bias). There is a page break between the collection scale and scales measuring other variables such as intention to use, WOM intention, and improper access to reduce question order bias. These questions are followed by the manipulation checks and lastly demographic questions. However, it is stated that privacy related factors cannot be completely isolated since privacy attributes have ramifications for non-privacy attributes and vice versa. For example, other factors such as annoyance could be confounded with privacy concerns (Milne & Gordon, 1993). This could decrease the internal validity of the study. However, there is made attempts to limit confounding variables, such as including a control group for the benefit variable (Malhotra, 2009). The scenarios were also pretested to check if respondents perceived the scenarios as wanted.

Pre-test

Two pretests have been conducted to test if both the control manipulation and the benefit manipulation were perceived as intended. When developing the low control scenario there was focused on making it as realistic as possible, but still highlight that the respondents had low control. To test whether the respondents viewed the control scenarios as low or high an adopted scale developed by H. Xu's et al. (2008) was used. Furthermore, when pretesting the benefit manipulation, the same introduction (context) as the control pretest was used, but the control manipulation was replaced by a paragraph describing a situation where the participant received either a self-benefit or others-benefit. A control group was also included in this pretest. To measure the manipulation of benefit participants was simply asked which degree they felt benefit for (1) self and (2) others. Both pretest also contained additional manipulation checks, such as if the participants found the scenarios to be clear and understandable. Additionally, participants where asked if they could put them self in the position of the scenario, and if they actually read the scenarios. The majority of the questions were asked on a 7-point Likert scale, ranging from strongly disagree to strongly agree. Respondents in both pretests was drawn from the same population as the experiment, meaning that respondents in the pretest is similar to respondents conducting the actual experiment. The sample size of control pretest was 41, whereas 18 participants assigned to the low control condition and 23 participants in the high control condition. For the benefit pretest the sample size was 39, were 15 participants were assigned to the control group, 13 participants were assigned to the self-benefit condition and 11 participants were assigned to the others-benefit condition. This is in line with Malhotra's (2009) recommendations.

Sampling

The target population for Study 2 is: people above 18 from general the population. The population is not restricted to any geographical areas as there is a wish to generalize the study to more than one country. However, since the data is collected through MTurk, which is from USA, most people answering the experimental survey is from USA. The minimum age is 18, since all the respondents need to be legal. Since the sample is drawn from the population, the sample will be: the general population above 18 years. The sampling unit is the same as the sample. A traditional sampling method is used, meaning that the entire sample is selected before the data collection begins (Malhotra, 2009). The sample is aimed to be as similar to the population to increase external validity. The sample is targeted through MTurk in the following dates: 12.05.18 and 16.05.18. The data was collected in multiple days because one of the manipulation checks lead to deletion of many respondents. Additionally, a discussion of deleting the control groups for benefit was made because the respondents did not perceive the control condition as natural, before making the final decision, more respondents were collected, to test if it improved the perception of the control condition.

Sample method

The data in Study 2 was collected through Amazon Mechanical Turk (MTurk), a wesite where researchers can pay people to conduct their research. Using MTurk as data collection method is perceived to be satisfactory in terms of data quality and samples from MTurk is viewed to be more representative than other convenience samples (Buhrmester, Kwang, & Gosling, 2011; Goodman, Cryder, & Cheema, 2013). Therefore, using this data collection method could minimize the influence of causal factors and increase the internal validity (Malhotra, 2009). This is a nonprobability sampling technique as it does not use chance selection. This type of sample method selection is made because it is cheaper than probability sampling techniques, and it requires very little time to collect data. As the method used for data collection is experimental surveys, it is convenient for respondents to participate in the study because they can complete the survey where they want. However, the sample may consist of heavy users of the internet and one may not reach old consumers since they are less likely to own a computer and have internet (Malhotra, 2009). On the other hand, most privacy issues have an online and digital context, therefore, having a sample containing of heavy users of the internet would most likely not do any harm.

Sample size

When determining the sample size, a great effort was made to find the balance between an inadequate and excessive number of respondents. There was not used any quantitative methods to determine the sample size, however multiple qualitative methods have been used. These are, nature of analyses, number of variable s, completion rates, and resource constraints (Malhotra, 2009). As Study 2 is conducted through an experiment, less respondents are needed than in a survey. At the same time, a between subject design requires a larger sample than a within subject design. The experiment is fairly short and contains of few variables, which implies that a small sample size is needed. In regard to the completion rate, a lot of respondents was deleted due to the screening question, asking respondents to not answer a question. Therefore, many respondents were collected, however, many of the respondents were deleted. Compared to Study 1, there was used more resources to collect the data in Study 2. Using MTurk allows an efficient collection of respondents, which suited perfectly with the limited time available. However, using MTurk can be expensive. Lastly, sample size in similar studies ranges between 50 and 60 respondents (Romani, Grappi, Bagozzi, & Barone, 2018). Based on these determinations of sample size, there was initially collected 300 respondents. However, during the data collection many respondents was deleted as they failed the question included to test if they were reading the questions. After doing preliminary analysis of this data, there was made a decision to collect 100 additional respondents, as respondents did not perceive the control condition for benefit as natural. Before making a decision to remove the control condition for benefit, more respondents were collected to test if it improved the perception of the control condition. The sample size for Study 2 is 391 respondents, meaning approximately 65 respondents in each of the six conditions. However, as briefly mentioned, the control groups for benefit were deleted as they were not perceived as natural. Therefore, the final sample size is 269 respondents, meaning that approximately 67 respondents were assigned to each of the four manipulation groups.

Reliability and validity

To measure reliability, internal consistency and Cronbach alpha analysis are being conducted for the five scales used in the experiment, these are: collection, intention to use, WOM intention, improper access, and control. As mentioned in the methodology chapter for Study 1, an alpha below .6 generally indicates unsatisfactory internal consistency reliability. If this is the case for some of the scales, items needs to be deleted before summated scales can be calculated (Malhotra, 2009). To assess Study 2's validity, factor analysis is conducted on the scales that are changed, in the experiment only one variable has been changed from its original source, being collection. More specifically, exploratory factor analyses and the extraction method maximum likelihood is used. This extraction method is commonly used in marketing research. Further, Promax, a non-orthogonal (oblique) rotation is chosen as it allows for factors to correlate which can simplify the factor pattern matrix. To determine the number of factors prior determinations, eigenvalues, and scree plot are used (Malhotra, 2009).

Analyses

After making the data set ready, some preliminary analyses were performed, namely *Cronbach alpha* studies for reliability and *factor analyses* for validity checks. As mentioned above, factor analyses are conducted on scales that have been changed. Further, some *descriptive statistic* is conducted to obtain knowledge about the respondents. The descriptive analyses were mainly conducted on demographic variables.

To examine if there exist any main and interaction effects, a *univariate linear regression* was conducted. This analysis is conducted on the following variables: benefit (self/others), control (high/low) and collection (dependent variable). In univariate statistics a set of observations in one variable is analyzed across different group of respondents, and the statistical meaningfulness of the differences between these groups are assessed (Janssens et al., 2008). In this thesis the difference in average collection of personal information between self-benefit and others-benefit, and between high and low control is tested. Further, it is also tested if this difference is statistical meaningful. As the data's measurement level is metric and the sample consist of four independent groups, the univariate technique, one-way ANOVA is conducted (Malhotra, 2009). As previously mentioned, ANOVA decreases random variability and has a robust design, this technique should therefore be appropriate (Janssens et al., 2008).

Furthermore, to assess the interaction effect more closely two *independent sample t-tests* are conducted. T-test is the most popular parametric test, conducted to examine means. There has been performed one independent sample t-test for control on collection and one independent sample t-test for benefit on collection. Both control (high/low) and benefit (self/others) consist of two samples. These samples are independent, meaning that the samples are not experimentally related. The measurement of one sample does not have an effect on the values of the second sample. Therefore, two group t-test is conducted (Malhotra, 2009). The aim of these analyses is to assess the contracts of the interaction effect. The sample will be split based on control, which makes it possible to verify the different effect of benefit on collection under each specific control condition (high/low).

Lastly, *ANOVA analyses* was used to examine the effect of intention to use and WOM intention on benefit and control. Two one-way ANOVA analyses was conducted to examine the difference among means for two populations. The variables included in the analyses was either control or benefit compared to either intention to use or WOM intention (Janssens et al., 2008). By conducing these analyses, one can evaluate for example if the mean value of intention to use will be different in self-benefit compared to others-benefit. A comparison of the category mean values will further indicate the nature of the effect of benefit on intention to use (Malhotra, 2009).

Results Study 2

Results pretest

As mentioned above, two pre-tests have been conducted, one assessing the control manipulation and the second, assessing the benefit manipulation. The results of these pretests will be discussed in this section. Before performing a ANOVA analysis to examine if respondents have perceived the manipulations as wanted, some preliminary analyses were conducted. First, data cleaning was performed, where missing values was deleted, consistency checks was conducted, and variables was named. Second, one Cronbach alpha analyses was performed in the first pretest, to test the control scale's reliability. This was the only scale used in the pretest. As there was not done any changes to the scale, no factor analysis was performed. The control variable (4 items; $\alpha = .94$) had an alpha higher than .80, therefore elimination of items in this scale to increase the alpha is not necessary. Summated scales were calculated and used in further analyses. For the second pretest assessing benefit, there was not used any scales, therefore no reliability or validity analyses was conducted (Janssens et al., 2008). Both pretest consisted of some manipulation checks, asking if respondents understood the scenarios, and if the they could put them self in the situation of the scenarios. As shown in the appendixes, results from both pretests show that respondents found the scenarios clear, understandable, and readable. The majority of respondents could also put themselves in the position of the scenario.

To examine if the scenarios was perceived as wanted, one-way ANOVA analyses was conducted. Assessing the pretest for control (high/low) first, the ANOVA analysis show that there is a significant difference between low and high control, $F(1,39) = 8.48$, $p = .006$. Meaning that the respondents perceived the low control condition as low control, and the high control condition as high control. However, the descriptive table (appendix) show that the differences in mean between high control ($M = 5.65$, $SD = 1.27$) and low control ($M = 4.26$, $SD = 1.78$) is not too big, however, the results are significant and therefore the same manipulations will be used in the experiment. As expected, high control has a greater effect on collection than low control. Similar findings were found for the second pretest, concerning the benefit manipulations (self/ others/control group). Measuring others-benefit, results show that others-benefit is in fact perceived different from self-benefit and the control group, $F(2,36) = 3.77$, $p = .033$. Similar to pretest one, the differences in mean are not too big, however, the ANOVA analysis is significant, which means that there is a statistically significant difference between the tree conditions (self/ others/ control group), probably due to the manipulation. The descriptive table (appendix) show that the means for others-benefit ($M = 6.18$, $SD = 1.08$) is higher than self-benefit ($M = 4.62$, SD = 1.66), and the control group ($M = 5.00$, $SD = 1.65$) in the others-benefit scenario. Importantly, the control group perceive the manipulation as lower than the others-benefit group and higher than the self-benefit group. In sum, the others-benefit scenario is perceived as being a benefit to others. Furthermore, measuring self-benefit, results show that self-benefit is perceived different from others-benefit and the control group, $F(2,36) = 3.83$, $p = .031$.This means that respondents perceive the scenario as having self-benefit ($M = 5.38$, $SD = 1.50$) more than others-benefit ($M = 3.55$, $SD = 2.25$), while the control condition ($M = 5.07$, $SD = 1.44$) was perceived to be in the middle of self-benefit and others-benefit. Again, the difference in mean is relatively small, but the findings are significant, meaning that the self-benefit scenario is perceived by respondents as self-benefit.

Results experiment

In the following sections results from the preliminary analyses and results from the main analysis will be discussed respectively.

Preliminary analyses

Before any analyses was conducted, some preliminary analyses were performed. First, data cleaning consisting of deleting missing values, consistency checks, and recoding of variable name was performed. Secondly, factor analyses for validity checks and Cronbach alpha for reliability checks are conducted. Third, some descriptive statistics are examined, being demographic variables.

Reliability and validity measurements

One Factor analysis were conducted on the collection scale as there were made changes in the items from the references it was found. The factor analyses showed that collection consist of one factor, this is determined by assessing the scree plot and eigenvalues (appendix). As the result of the factor analysis showed one factor, the validity of the scales is satisfactory and reliability test can be conducted (Malhotra, 2009). The Cronbach alpha analyses for assessing reliability of collection (4 items; $\alpha = .95$) was satisfactory, showing an alpha above .80, elimination of items in this scale to increase alpha is not necessary and summated scales can be calculated (Janssens et al., 2008). The alpha for intention to use (3 items; $\alpha = .95$), WOM intention (4 items; $\alpha = .96$), improper access (3 items; $\alpha = .81$), and control (4 items; $\alpha = .94$) is also satisfactory and summated scales are calculated also for these scales.

Descriptives

The majority for respondents in this experiment where between 18 and 30 years old (43.1%) whereas 61.3% of respondents where male. Most respondents have a Bachelor degree (58.4%) and are employees (66.5%). Even if the majority of respondents are between 18 and 30 years old, only 8.2% are students. As the data was collected through MTurk, the majority of respondents are from USA (45.7%). A summary of the demographics can be seen in the appendixes.

Main analysis

Even if pretests were performed to test if participants perceived the scenarios as intended, a One-way ANOVA was also performed based on the sample from the experimentation survey (appendix). The results are significant and therefore satisfactory. However, the manipulation check for benefit indicate that the control group did not perceive the control manipulation as natural. Therefore, the main study will be conducted without the control group for the benefit manipulation. Thus, the analyses conducted in Study 2 will be a 2 (benefit: self/others) x 2 (control: high/low) design as described in the methodology section. There will be conducted a univariate linear regression to examine if there exist any main and interaction effects. Further, a t-test will be used to investigate the contracts of the interaction effect more closely. Lastly, ANOVA analyses are performed to examine the additional variables included in the experiment (WOM intention and intention to use).

Univariate linear regression

As hypothesized high control is found to be better than low control, as respondents having low control (M = 4.80, SD = 1.68) are more concerned for personal information collection than respondents having high control

(M = 4.69, SD = 1.70). For benefit, results show that self-benefit is better than others-benefit, as people receiving self-benefit (M = 4.38, SD = 1.78) are less concerned for personal information collection than respondents receiving others-benefit (M = 5.10, SD = 1.53) (appendix). However, there need to be conducted more test to assess the significance of these results (table 5). Results show a significant main effect of benefit on collection, $F(1,265) = 13.72$, $p < .001$, indicating a significant difference between self and others-benefit. However, the main effect of control on collection was not significant, $F(1,265) = .57$, $p = .45$. A main effect refers to the effect of an independent variable on a dependent variable averaging across the levels of any other independent variables (Malhotra, 2009). More important than the main effect, is the interaction effect. The results show that the interaction effect between control and benefit is moderately significant, $F(1,265) = 2.99$, $p = .085$. This means that specific combinations of these factors will differ significantly from other combinations (Janssens et al., 2008). In other words, this means that the effect of benefit (independent variable) on collection (dependent variable) is different for different categories of control (independent variable) (Malhotra, 2009).

Table 5

Results for the analysis for the four-group experimental design

	Sum of Squares	**df**	**Mean Square**	**F**	**P**
Corrected Model	44.45[a]	3	14.82	5.43	.001
Intercept	6029.9	1	6029.49	2210.22	.000
Control	1.56	1	1.56	.57	.451
Benefit	37.44	1	37.44	13.72	.000
Control * Benefit	8.16	1	8.16	2.99	.085
Error	722.92	265	2.73		
Total	6822.44	269			
Corrected Total	767.37	268			

a. R Squared = .058 (Adjusted R Squared = .047)

To further asses the interaction effect, an examination of the "estimated marginal means" are performed (figure 3). Figure 3 shows that the two lines are not parallel to each other, and they do even cross, meaning that there is an interaction effect (Janssens et al., 2008). The moderately significant interaction effect between benefit and control means that the effect of control is factor-dependent on the level of the benefit factor. More specifically, this means that consumers having low control over their personal information will need self-benefits in order to justify the collection. The moderately significant interaction effect observed earlier is thus confirmed graphically.

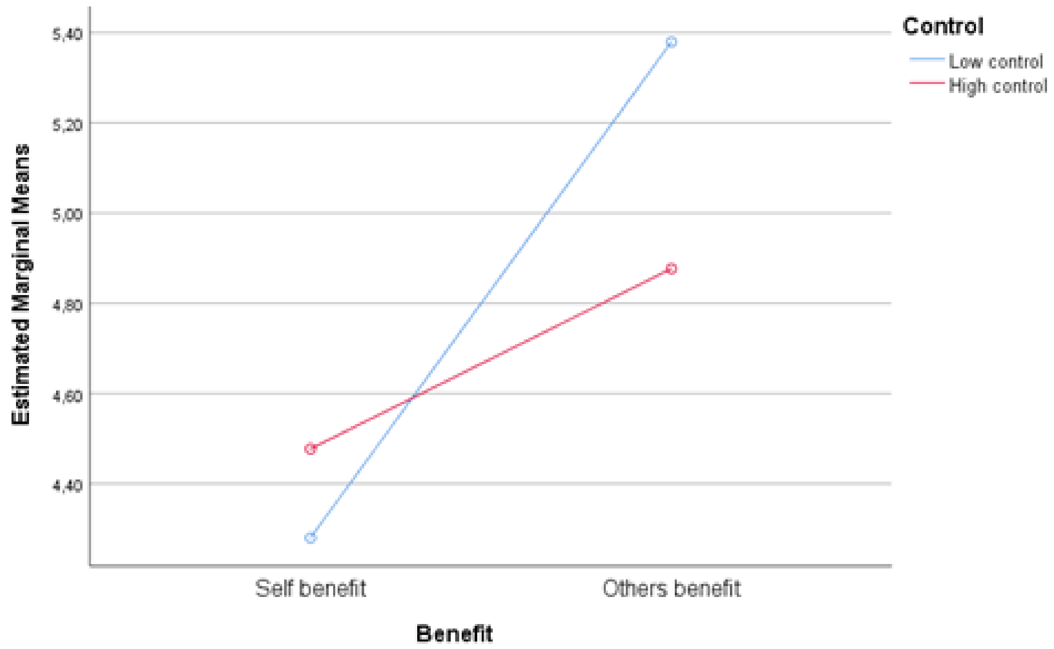


Figure 3. Estimated marginal mean for Collection. This figure illustrates the moderately significant interaction effect of control and benefit.

Investigation of contrasts for interaction effect

To assess the contracts of the interaction effect, independent sample t-test analyses is conducted. The sample is split based on control (moderator variable), therefore the different effects of benefit on collection can be verified under each specific control condition (high/low). Assessing variance first, the Levene's test for Equality of Variances, which hypothesize that equal variances is assumed, show that the hypothesis is rejected and equal variances is not assumed. The Levene's test for Equality of Variances test is presented in the independent sample t-test table in the appendixes. Furthermore, the t-test for Equality of Means examine wheatear the average between self-benefit and others-benefit are equal under low control. The results show that under low control of personal information, the collection score differ in case of self-benefit versus others-benefit. More specific, self-benefit (M = 4.28, SD = 1.85) allows for more collection of personal information than others-benefit (M = 5.38, SD = 1.27), t(115.77) = -3.85, p < .001. This means that self-benefit adds much in regard to collection under low control. In other words, if consumers have low control over their personal information companies will need to provide self-benefits to the consumers in order to justify the collection of their personal information. Assessing the independent sample t-test for high control secondly (appendix), indicates that the Levene's test for Equality of Variances hypothesis cannot be rejected, equal variances is therefore assumed (appendix). Furthermore, the t-test for Equality of Means show that there is not a significant difference in collection of personal information between self-benefit (M = 4.48, SD = 1.73) and others-benefit (M = 4.88, SD = 1.67), t(141) = -1.40, p = .163 under high control.

ANOVA

As briefly mentioned, some additional variables were included in the experiment to obtain additional insights in respondent's perceptions. These variables are: Intention to use, WOM intention, and improper access. A one-way ANOVA analyses has been conducted on intention to use and WOM intention as these variables are the most interesting to investigate further (appendix). In terms of benefit (self/others), the one-way ANOVA analysis indicates that there are significant differences between self-benefit and others-benefit in terms of WOM intention, $F(1,267) = 4.91$, $p = .028$. Assessing this more closely the results shows that self-benefit ($M = 4.69$, $SD = 1.57$) is better than others-benefit ($M = 4.26$, $SD = 1.51$) in terms of positive WOM intention. Furthermore, the same analysis indicates that there also is a significant difference between self-benefit and others-benefit in terms of intention to use the app described in the scenarios, $F(1,267) = 4.27$, $p = .040$. Again, self-benefit ($M = 4.58$, $SD = 1.68$) is better than others-benefit ($M = 4.16$, $SD = 1.66$) in terms of intention to use. This means that when respondents receive self-benefit they have a higher possibility to use the app and spread positive WOM to others, compared to if respondents received benefit to others. In terms of control, the one-way ANOVA analysis show that there was not a significant difference in the scores for low control ($M = 4.31$, $SD = 1.68$) and high control ($M = 4.60$, $SD = 1.51$) in terms of WOM intention, $F(1,267) = 2.22$, $p = .138$. Similar findings are present for intention to use, were the analysis show that there was not a significant difference in the scores for low control ($M = 4.27$, $SD = 1.77$) and high control ($M = 4.45$, $SD = 1.60$) in terms of intention to use the app described in the scenarios, $F(1,267) = .75$, $p = .388$.

General discussion

It is important for companies to understand why the expected growth of IoT have not happened, to be able to facilitate growth. Therefore, the aim of this thesis was to require an understanding of possible barriers consumers have against IoT adoption, additionally, a further investigation of the privacy and security barrier was made to solve the issues related to this barrier. Therefore, two studies were conducted, using different research methods (survey and experiment). The results of these studies provided interesting implications, both for researchers and actors in the IoT industry. The quantitative research in Study 1 detected consumers barriers against IoT adoption across two clusters. In line with previous research, price (Balta-Ozkan et al., 2013; Björnsjö et al., 2016; Mani & Chouk, 2016; Nakyung & Kim, 2015), dependency (Licoppe & Heurtin, 2001), as well as privacy and security (Björnsjö et al., 2016; Gubbi et al., 2013; Hsu & Lin, 2016; Malhotra et al., 2004; Miorandi et al., 2012; Ziegeldorf et al., 2014) was found to be barriers against IoT adoption in at least one of the two segments constructed in Study 1. However, Study 1 was composed of a special sample consisting of a small and homogenous group of consumers. As privacy and security was the only barrier present in both clusters, a further investigation of this barrier was conducted. Interestingly, cluster 1, named Smart Device Likers, was concerned for every aspect of privacy and security, while cluster 2, named Smart Device Lovers, only were concerned for unauthorized secondary use and improper access, and not collection and threats. This was investigated further in Study 2, where the aim was to solve the collection problem, being why some consumers are concerned for personal information collection and other consumers not. It was expected that benefit (self/others) and control (high/low) would influence consumers disclosure of personal information. This is in line with prior research as providing consumers with valuable benefits to obtain personal information is consistent with the benefit congruency principle of marketing (Chandon, Wansink, & Laurent, 2000; Y. Xu et al., 2003). Additionally, previous research have found that 85% of adults believe that controlling access to their personal information is very important (Bélanger & Crossler, 2011), indicating that high control could lead to consumers consent of personal information collection. The results of Study 2 confirm the predictions of self-benefit leading to a greater disclosure of personal information than others-benefit and that high control leads to greater disclosure of personal information than low control.

H1 is supported as there is a main effect of benefit on collection. This means that consumers who receive self-benefit from a company, would be more likely to share their personal information with that company. This is in line with previous research stating that even if people is acting altruistic, the reasoning for why they do it may be for personal interest (Tam et al., 2002). Furthermore, H2 is not supported, as there is no main effect of control on collection. The reason for this may be that respondents expresses their attitudes toward high or low control which may not reflect their actual behavior. Additionally, consumers may not want companies to have their personal information regardless if they are in control or not, because they do not trust companies with their personal information. Previous research has also stated that consumers are continually engaged in a process of adjustment to find a balance between the desire of privacy control and disclosure of personal information (Westin, 1967). More importantly than the main effect is the interaction effect, whereas H3 is supported as there is a moderately significant interaction effect of control and benefit on collection. More specifically, it is found that there is a positive effect of self-benefit on collection under low control. Additionally, that there is no effect of benefit on collection under high control, as the contrast variables is non-significant under high control. This means that if consumers have low control over their personal information companies will need to provide self-benefits to the consumers in order to justify the collection. From a theoretical perspective this thesis extends recent research with a further investigation of barrier against IoT adoption in a quantitative manner. Also, this thesis makes an attempt to solve one of the barriers against IoT adoption, the collection problem.

Implications

Overall the results provide important insights in which barriers consumers have when considering buying a IoT device. This serves as a scientific contribution to previous literature, even when the sample used in Study 1 was a special sample. Additionally, applying quantitative research in the exploration of barriers against IoT adoption, is a major contribution. An understanding of barriers for adoption is important, as companies needs to understand the problem before they can solve it. Growth in the IoT industry will create increased revenues for companies. As Mazhelis, Luoma, and Warma (2012) stated, IoT represent a tremendous opportunity for various types of firms, including telecom operators, application and service providers, as well as platform providers and integrator. The development of new integrated IoT devices may also help consumers. For instance, old people can continue to live at home with Smart Devices such as robot vacuum cleaner, smart thermostat, and flowers that water themselves. Furthermore, analyzing barriers across segments provided insights into the difference between segments and their perception of barriers. Meaning that companies does not need to use resources to solve a barrier for consumer groups that does not perceive this particular barrier as influential for non-purchase. For instance, as Study 1 showed, dependency is only perceived to be a barrier for Smart Device Likers (cluster 1) and not Smart Device Lovers (cluster 2). Similarly, price was only found to be a barrier in cluster 1 and not cluster 2. Managers can therefore implement price discrimination and offer a lower price to cluster 1, but keep the higher price for cluster 2. Alternatively, managers can keep a high price but offer better value to ignite growth. This is in line with recommendations given in Accenture's 2016 report.

Another contribution of this thesis, is the suggestion of how to solve the collection problem. As discussed, self-benefit has a positive effect on collection under low control. Benefit and personalization is an important tool to improve customer satisfaction and retention. Benefit and personalization could therefore decrease companies' costs, because acquiring a new customer costs more than retaining an existing customer (Chellappa & Sin, 2005). Personalization and control has further been extensively research in regard to privacy concerns, both individually (Acquisti, Brandimarte, & Loewenstein, 2015; Chellappa & Sin, 2005) and collectively to influence privacy concerns (Malhotra et al., 2004). By applying control and benefit – which is a form of personalization – in a personal information collection context, Study 2 also makes a scientific contribution. Solving the collection problem is also important for managers, as collection of customers personal information can increase companies' profitability. For instance, it is suggested that firms can use customers information to generate productivity and profit gains that are five to six percent higher than competitors (Biesdorf, Court, & Willmott, 2013). Further, companies spend 36 billion dollars annually to capture and leverage customer data (Martin et al., 2017). This illustrate the importance for companies to obtain an understanding of factors that influence customers to disclose their personal information, while companies keep consumers privacy concerns in mind.

The main finding in Study 2 is that companies need to provide consumers with self-benefit when they have low control, to justify the collection of personal information. However, this does not mean that companies can prevent consumers of having control and use consumers personal information as wanted as long as the company provide consumers with self-benefit. In that regard, previous research state that firms that commit to authentic data privacy practices in long-term will experience positive performance including favorable market response, customer loyalty, and engagement benefits (Martin & Murphy, 2017). Previous research suggests two methods of how companies can protect customers privacy, the first method relies on the customer trustworthiness, and the other relies on customer anonymity (Sicari et al., 2015). It is also states that organizational policies should limit data collection to minimal levels required for business (H. J. Smith et al., 1996). The highly relevant General Data Protection Regulation (GDPR) highlights these aspects.

Overall, the results in this thesis provides important insights for managers and organizations that are interested in Smart Device development, privacy concerns, collection of personal information. This thesis could also serve as a basis for improving critical aspects of Smart Devices such as privacy and security.

Limitations

This thesis consists of some limitations, discussed for Study 1 firstly, and Study 2 secondly. Study 1 consist of a small and homogenies sample, the reason for this is probably due to the data collection method chosen. As the data was collected through my personal Facebook account, the sample consisted mostly of students, because that is who I am friends with on Facebook. The sample owned a lot of Smart Devices and was familiar with technology. This could limit the generalizability of the results. However, understanding this consumer group is important for technology-related industries, as young consumers (digital natives) are heavy users of technological devices and services. Of course, there was an opportunity to collect new or additional data, however, as Study 1 served as a basis for Study 2, I chose to move further to the second study. However, using this special sample may have destroyed the possibility to find a moderating effect of individual traits. Additionally, the sample may also have demolished the possibility to detect more differences between segments, and the possibility to detect more barriers. Some may say that the sample used in Study 2 consisted of many respondents per condition. To add more and more respondents in a sample to get statistical results is unacceptable. However, the sample size used in Study 2 is in line with similar studies. However, a greater attempt to choose a sample size that equate statistical and practical significance could have been performed (Van de Ven, 2007). Furthermore, the scenarios used in Study 2 could have been developed better so the differences between the scenarios would have been perceived stronger. This lead to the need to delete the control condition for benefit in the analyses, as this manipulation was not perceived as natural.

Future research

Three possible avenues of future research are suggested: (1) future research could test other possible barriers against IoT adoption, such as awareness of Smart Devices, perceived uselessness, and social barriers such as trust and fit to current and changing lifestyles. A further analysis of barriers against IoT adoption is needed, to get a deeper understanding of why consumers do not adopt IoT devices in the expected pace. Alternatively, researchers could replicate Study 1 with a better sample. There is also a need to test consumers behavior and not only attitudes in relation to the barriers. Therefore, further research streams could investigate consumers attitudes regarding barriers to IoT adoption using experimentation. (2) Future research could also analyze the influence of individual traits on barriers, either as a moderation effect as attempted in this thesis or as a variable influencing adoption. This could give a better understanding of why barriers differ across segments. (3) Lastly, researchers could try to solve other barriers to IoT adoption, such as dependency. This could me a major contribution to the literature, as well as it would be extremely relevant for IoT companies. Alternatively, there is a possibility to test other variables influencing collection of personal information. Such variables could be sensitivity of data, individual traits, and prior online disclosure.

Chapter 5: Conclusion

This thesis contributes to a better understanding of factors that explain why consumers do not adopt IoT devices. An exploration of barriers from the IoT literature (topic-specific barriers) and the innovation literature (non-topic specific barriers) was introduced and tested across segments. Findings of Study 1 show – despite the use of a special sample – that price, dependency and all sub categories of privacy and security (concern for privacy issues, collection, improper access, and unauthorized secondary use) are barriers for the first cluster constructed, named Smart Device Likers. Further, only improper access and unauthorized secondary use was found to be barriers that hinder IoT adoption in the second cluster, named Smart Device Lovers. This means that some consumers worry about all the aspects of privacy and security while other consumers only worry about the chance of someone getting access to their personal information and possible use of this personal information. Detecting these barriers against IoT adoption serves as an important contribution to the existing literature. Study 2 aims to solve the collection problem, referring to an understanding of what is needed for consumers to allow companies to collect consumers personal information. It was predicted that high (vs. low) control of personal information and self-benefit (vs. others-benefit) would lead to increased disclosure of personal information. Findings of Study 2 show a main effect of benefit on collection meaning that if consumers get benefits (self or others), they would be more likely to share their personal information with a company. There is also found a marginal significant interaction effect of benefit and control on collection, which means that if consumers have low control over their personal information, they will need self-benefits in order to justify companies' collection of consumers personal information. The collection problem can therefore be solved providing self-benefits to consumers when they have low control. Study 2 contributes to previous literature by solving the collection problem. Even if the interaction effect found in this study is marginal significant, the results indicates some interesting results.

Appendixes

Questionnaire Study 1

Introduction (page 1)

Thank you for taking this survey which will be used in my Master Thesis at Luiss University. The answer is completely anonymous and the survey will take approximately 15 minutes. However, I kindly ask you to read the questions carefully and answer as honestly as you can keeping in mind that there are no right or wrong answers. The survey is concerning smart devices, below you can see a description of what this means.

Page 2

A smart device is an electronic device, generally connected to other devices or networks via different wireless protocols such as Bluetooth, NFC, Wi-Fi, 3G, etc., that can operate to some extent interactively and autonomously. Smart devices can be designed to support a variety of form factors, a range of properties pertaining to ubiquitous computing and to be used in three main system environments: physical world, human-centered environments and distributed computing environments. With their features, all the smart devices understand simple commands sent by users and help in daily activities (such as working, training, monitoring our physical conditions or taking care of our home).

Several notable types of smart devices are:

- Smartphones
- Smart TVs
- Tablets
- Phablets (a class of smart devices that combines smartphones and tablets features)
- Smartwatches
- Smart bands (wearable devices, e.g. fitness trackers, that aim to measure body temperature, heart rate, brain activity, muscle motion and other critical data for medical or athletic purposes)
- Smart Home systems (sets of smart devices such as smart thermostats, smart fridges or smart security cameras that help managing the home environment)

Page 3

In page three respondents were kindly asked to answer the following “open question” about Smart Devices.

Open question, were respondents expressed their view points

Please recall a recent opportunity in which you had the possibility of purchasing a Smart Device but you did not do it. What kind of smart device was it? Why didn’t you purchase it? Write down below a short text to explain it. (Max 300 words.)

Thereafter, the respondents were asked to answer the following scales. They were given the following description first: Thinking about Smart Devices, please answer whether you agree or disagree with the given statements considering a scale from 1 to 7 where 1= "strongly disagree" and 7= "strongly agree".

Scales	**Items**	**Source**
Privacy concerns (Privacy and security)	Q1: I'm concerned about threats to my personal privacy coming from Smart Devices Q2: I'm concerned about data collected by Smart Devices without my permission	Mani and Chouk (2016)
Collection (Privacy and security)	Q3: I am concerned that Smart Devices producers are collecting too much personal information about me Q4: It bothers me to give personal information to so many Smart Devices producers	Hsu and Lin (2016)
Unauthorized secondary use (Privacy and security)	Q5: Smart Devices producers should not use personal information for any purpose not specifically authorized by the user Q6: Smart Devices producers should never sell personal information to other companies Q7: Smart Devices producers should never share personal information with other companies unless specifically authorized to do so by the user	Hsu and Lin (2016)
Improper access (Privacy and security)	Q8: Smart Devices producers should devote more time and effort to preventing unauthorized access to personal information Q9: Smart Devices producers should take more steps to ensure that the personal information in their files is accurate Q10: Smart Devices producers should take more steps to ensure that unauthorized people cannot access personal information in their computers	Hsu and Lin (2016)
Intrusiveness	Q11: Smart Devices are intrusive Q12: Smart Devices are irritating Q13: Smart Devices are indiscreet Q14: I'm not comfortable with Smart Devices Q15: Smart Devices are disturbing	Mani and Chouk (2016)
Dependence	Q16: I'm afraid of becoming dependent on Smart Devices Q17: Smart Devices will reduce my autonomy Q18: Smart Devices will strengthen my addiction to technology Q19: I think my social life will suffer from my use of Smart Devices	Mani and Chouk (2016)
Ease of use	Q20: In my opinion, Smart Devices are easy to use Q21: In my opinion, Smart Devices are fast to use Q22: In my opinion, progress in Smart Devices is clear Q23: My interaction with Smart Devices is understandable Q24: Interacting with Smart Devices does not require a lot of my mental effort	Kuisma et al. (2007) Laukkanen et al. (2007) H.-P. Lu et al. (2005)

Self-efficacy	Q25: I know how to use Smart Devices Q26: I am confident in my ability to understand the use the Smart Devices Q27: I think I am able to operate Smart Devices although I've never used it before	Mani and Chouk (2016)
Number of IoT services (Network effect)	Q28: I think a good number of Smart Devices can be used Q29: I could easily find circumstances in which I can use Smart Devices Q30: I think there are many reasons in daily life to use Smart Devices	Hsu and Lin (2016)
Perceived critical mass (Network effect)	Q31: Most people in my peer group frequently use Smart Devices Q32: Most people in my community frequently use Smart Devices Q33: My family/friends frequently use Smart Devices Q34: Most people I know use Smart Devices	Hsu and Lin (2016)
Perceived compatibility (Network effect)	Q35: Using Smart Devices is compatible with all aspects of my work Q36: I think that using Smart Devices fits well with the way I like to work Q37: Using Smart Devices fits into my work style	Hsu and Lin (2016)
Perceived complementarity (Network effect)	Q38: A wide range of Smart Device products is available Q39: Using Smart Devices will allow me to finish various tasks (i.e., payments, identification and information exchange, home management, fitness monitoring etc.) Q40: A wide range of apps concerning Smart Devices are available on smartphone	Hsu and Lin (2016)
Novelty	Q41: I find Smart Devices to be: New / Old Original / Unoriginal Unusual / Common Familiar / Novel Typical / Atypical Stable/ Unstable Developed/ Undeveloped Questionable/ Unquestionable	Campbell and Goodstein (2001) D. Cox and Cox (2002) D. S. Cox and Cox (1988) Dimofte et al. (2003)
Value perception (The three last variables are	Q42: The value of Smart Devices is: Ineffective / Effective Not functional / Functional Impractical / Practical	Kleijnen et al. (2007) Meyers-Levy and Peracchio (1995) Voss et al. (2003)

measuring uncertainty)	Useless / Useful Inefficient / Efficient Unproductive / Productive Not helpful/ Helpful Not necessary/Necessary Poorly made / Well made Boring / Exciting Not a worthwhile product / A worthwhile product Unappealing / Appealing Common / Unique	
Price	Q43: The price of Smart Devices is: Unfair/Fair Unreasonable/Reasonable Dishonest/Honest Unacceptable/Acceptable Not justified/Justified Unsatisfactory/Satisfactory Extremely low/Extremely high Bad value for money/Good value for money	Haws and Bearden (2006)
Intention to buy	Q44: How likely are you to purchase Smart devices? Q45: How probable is it that you will purchase Smart Devices? Q46: How possible is it that you will purchase Smart Devices?	Mano and Oliver (1993)
WOM intention	Q47: I will recommend friends to buy Smart Devices Q48: I will say good things about Smart Devices to others Q49: I bring up Smart Devices in a positive way in conversations I have with friends and acquaintances Q50: In social situations, I often speak favorably about Smart Devices	Arnett et al. (2003) Rogers (2010) Voorhees et al. (2006)
Risk	Q51: There is a good chance I will make a mistake if I purchase a Smart Device Q52: Smart Device is a very risky purchase	Laroche et al. (2005) R. N. Stone and Grønhaug (1993)
Knowledge	Q53: I feel very knowledgeable about Smart Devices Q54: If I had to purchase Smart Devices today, I would need to gather very little information in order to make a wise decision Q55: I feel very confident about my ability to tell the difference in quality among different brands of Smart Devices Q56: If a friend asked me about Smart Devices, I could give them advice about different brands	D. C. Smith and Park (1992)
Optimism (Individual trait)	Q57: Technology gives you more freedom of mobility Q58: Products and services that use the newest technologies are much more convenient to use Q59: You find new technologies to be mentally stimulating	Rojas-Méndez et al. (2017)

Innovativeness (Individual trait)	Q60: You can usually figure out new high-tech products and services without help from others Q61: Other people come to you for advice on new technologies Q62: You find you have fewer problems than other people in making technology work for you Q63: You keep up with the latest technological developments in your areas of interest Q64: In general, you are among the first in your circle of friends to acquire new technology when it appears	Rojas-Méndez et al. (2017)
Discomfort (Individual trait)	Q65: Sometimes, you think that technology systems are not designed for use by ordinary people Q66: It is embarrassing when you have trouble with a high-tech gadget while people are watching Q67: Technology always seems to fail at the worst possible time Q68: Many new technologies have health or safety risks that are not discovered until after people have used them Q69: There is no such thing as a manual for a high-tech product or service that's written in plain language Q70: If you buy a high-tech product or service, you prefer to have the basic model over one with a lot of extra features	Rojas-Méndez et al. (2017)
Insecurity (Individual trait)	Q71: You do not consider it safe giving out a credit card number over a computer Q72: The human touch is very important when doing business with a company Q73: You do not consider it safe to do any kind of financial business online Q74: You do not feel confident doing business with a place that can only be reached online Q75: You worry that information you send over the internet will be seen by other people	Rojas-Méndez et al. (2017)
Own Smart Device	Q76: How many Smart Devices do you own? Q77: Which kind of Smart Devices do you own?	
Demographics	Gender, age, education level, profession, and nationality	

Note: *Novelty, value and price is measured on a bipolar scale. Own Smart Device is measured on nominal and ordinal measurement level. Demographics is measured on nominal, ordinal and ratio measurement level. Privacy and security, collection, unauthorized secondary use, improper access, intrusiveness, dependency, ease of use, self-efficacy, number of IoT services, perceived critical mass, perceived compatibility, perceived complementarity, intention to buy, WOM intention, risk, knowledge, optimism, innovativeness, discomfort, and insecurity is measured on a 7-point Likert scale and are metric variables.*

Page 8

Thank you very much for your time and for your extraordinary willingness to participate to this research project.

Experimental survey for pretest 1

Introduction (page 1)

Thank you for taking this survey which will be used in my Master Thesis at Luiss University. The answer is completely anonymous and the survey will take approximately 4 minutes. I kindly ask you to read the questions carefully and answer as honestly as you can keeping in mind that there are no right or wrong answers. The survey is concerning control of consumer's privacy information.

Page 2

Please read the following scenario carefully, and have this in mind when you are answering the following questions.

Respondents were assigned to one of the two conditions presented below:

Natural condition, High control	Consider a scenario where you are a member of a training center, which recently have developed an app. This app gives you various information, such as timetable for group workouts, openings hours, special events etc. You can also use the app to enter the center, which means that the training center can track how often you exercise. The center also wants you to rate, on the app, the intensity of your workouts, how often and how many calories you eat, your weight, age, as well as your height. This is a trial project which will last for 3 months. In order to give this information to the training center, accept the privacy terms and conditions about how the training center will manage your information (cookies policy, secondary use...). To accept the privacy terms and conditions simply tick off the "I agree" button. After agreeing with the privacy terms, the training center will manage the personal information you provided.
Natural condition, Low control	Consider a scenario where you are a member of a training center, which recently have developed an app. This app gives you various information, such as timetable for group workouts, openings hours, special events etc. You can also use the app to enter the center, which means that the training center can track how often you exercise. The center also wants you to rate, on the app, the intensity of your workouts, how often and how many calories you eat, your weight, age, as well as your height. This is a trial project which will last for 3 months. If you consent to give this information to the training center, you would have great control of how the center manage your personal information. You can for instance at any time decide which information the center receives and how it is used (i.e. you could allow the center to just have access to information about your weight and height but not your training intensity). On the app, it will also be very easy to find the page where you could change the privacy settings.

Page 3

Thinking about the scenario you just read, please answer whether you agree or disagree with the given statements considering a scale from 1 to 7 where 1= "strongly disagree" and 7= "strongly agree".

Scale	**Items**	**Source**
Manipulation check	Q1: Did you read the scenario?	
Manipulation check	Q2: I think the scenario was clear and understandable	
Manipulation check	Q3: I can easily put myself in the position in which the scenario describes	

Control	Q4: I believe I have control over who can get access to my personal information collected by the training center Q5: I think I have control over what personal information is released by the training center Q6: I believe I have control over how personal information is used by the training center Q7: I believe I can control my personal information provided to the training center	H. Xu et al. (2008)
The first question is a simple yes or no question. The rest of the questions is measured on a 7-point Likert scale		

Page 4

Thank you very much for your time and for your extraordinary willingness to participate to this research project.

Experimental survey for pretest 2

Introduction (page 1)

Thank you for taking this survey which will be used in my Master Thesis at Luiss University. The answer is completely anonymous and the survey will take approximately 3 minutes. I kindly ask you to read the questions carefully and answer as honestly as you can keeping in mind that there are no right or wrong answers. The survey is concerning consumers privacy information.

Page 2

Please read the following scenario carefully, and have this in mind when you are answering the following questions.

Respondents were randomly assigned to one of the three conditions presented below:

Control group	Consider a scenario where you are a member of a training center, which recently have developed an app. This app gives you various information, such as timetable for group workouts, openings hours, special events etc. You can also use the app to enter the center, which means that the training center can track how often you exercise. The center also wants you to rate, on the app, the intensity of your workouts, how often and how many calories you eat, your weight, age, as well as your height. This is a trial project which will last for 3 months.
Self-benefit	Consider a scenario where you are a member of a training center, which recently have developed an app. This app gives you various information, such as timetable for group workouts, openings hours, special events etc. You can also use the app to enter the center, which means that the training center can track how often you exercise. The center also wants you to rate, on the app, the intensity of your workouts, how often and how many calories you eat, your weight, age, as well as your height. This is a trial project which will last for 3 months. If you agree to give this information to the training center they will be able to use your data to make algorithms which makes it possible to develop personal training-and nutrition plan only to use by you. This will enrich your training experience, as the plans is built on the data you provide to the training center. This means that you will get training-and nutrition plans personalized to your needs, through the app. If you wish, the app will also give you notifications when there is a new training- and nutrition plan developed to you.

Others-benefit	Consider a scenario where you are a member of a training center, which recently have developed an app. This app gives you various information, such as timetable for group workouts, openings hours, special events etc. You can also use the app to enter the center, which means that the training center can track how often you exercise. The center also wants you to rate, on the app, the intensity of your workouts, how often and how many calories you eat, your weight, age, as well as your height. This is a trial project which will last for 3 months. If you agree to give this information to the training center they will be able to use your data to make algorithms which makes it possible to develop weekly tutorials featuring new training methods, dieting etc. easily accessible in the app. As you are a part of the first group using the app, you will not have access to any tutorials during the three months of the project. However, the next group using the app will receive tutorials based on your privacy information. In other words, your personal information will be used to help other people gain more knowledge regarding training methods and dieting.

Page 3

Thinking about the scenario you just read, please answer whether you agree or disagree with the given statements considering a scale from 1 to 7 where 1= "strongly disagree" and 7= "strongly agree".

Scale	Items	Source
Manipulation check	Q1: Do not answer this question, simply move further to the next questions whiteout answering this question	
Manipulation check	Q2: I think the scenario was clear and understandable	
Manipulation check	Q3: I think the scenario was readable	
Manipulation check	Q4: I can easily put myself in the position which the scenario describes	
Self-benefit	Q5: Providing my personal data to the training center helps me	
Others-benefit	Q6: Providing my personal data to the training center helps others	

Every scale was measured on a 7-point Likert scale

Page 4

Thank you very much for your time and for your extraordinary willingness to participate to this research project.

Experimental survey for Study 2

Introduction (page 1)

Thank you for taking this survey which will be used in my Master Thesis at Luiss University. The answer is completely anonymous and the survey will take approximately 5 minutes. I kindly ask you to read the questions carefully and answer as honestly as you can keeping in mind that there are no right or wrong answers. The survey is concerning consumers privacy information.

Page 2

Please read the following scenario carefully, and have this in mind when you are answering the following questions.

Respondents were randomly assigned to one of the six conditions

	Control group	**Self-benefit**	**Others-benefit**
High control	Consider a scenario where you are a member of a training center, which recently have developed an app. This app gives you various information, such as timetable for group workouts, openings hours, special events etc. You can also use the app to enter the center, which means that the training center can track how often you exercise. The center also wants you to rate, on the app, the intensity of your workouts, how often and how many calories you eat, your weight, age, as well as your height. This is a trial project which will last for 3 months. If you consent to give this information to the training center, you would have great control of how the center manage your personal information. You can for instance at any time decide which information the center receives and how it is used (i.e. you could allow the center to just have access to information about your weight and height but not your training intensity). On the app, it will also be very easy to find the page where you could change the privacy settings.	Consider a scenario where you are a member of a training center, which recently have developed an app. This app gives you various information, such as timetable for group workouts, openings hours, special events etc. You can also use the app to enter the center, which means that the training center can track how often you exercise. The center also wants you to rate, on the app, the intensity of your workouts, how often and how many calories you eat, your weight, age, as well as your height. This is a trial project which will last for 3 months. If you agree to give this information to the training center they will be able to use your data to make algorithms which makes it possible to develop personal training-and nutrition plan only to use by you. This will enrich your training experience, as the plans is built on the data you provide to the training center. This means that you will get training-and nutrition plans personalized to your needs, through the app. If you wish, the app will also give you notifications when there is a new training- and nutrition plan developed to you. If you consent to give this information to the training center, you would have great control of how the center manage your personal information. You can for instance at any time decide which information the center receives and how it is used (i.e. you could allow the center to just have access to information about your weight and height but not your training intensity). On the app, it will also be very easy to find the page where you could change the privacy settings.	Consider a scenario where you are a member of a training center, which recently have developed an app. This app gives you various information, such as timetable for group workouts, openings hours, special events etc. You can also use the app to enter the center, which means that the training center can track how often you exercise. The center also wants you to rate, on the app, the intensity of your workouts, how often and how many calories you eat, your weight, age, as well as your height. This is a trial project which will last for 3 months. If you agree to give this information to the training center they will be able to use your data to make algorithms which makes it possible to develop weekly tutorials featuring new training methods, dieting etc. easily accessible in the app. As you are a part of the first group using the app, you will not have access to any tutorials during the three months of the project. However, the next group using the app will receive tutorials based on your privacy information. In other words, your personal information will be used to help other people gain more knowledge regarding training methods and dieting. If you consent to give this information to the training center, you would have great control of how the center manage your personal information. You can for instance at any time decide which information the center receives and how it is used (i.e. you could allow the center to just have access to information about your weight and height but not your training
Low control	Consider a scenario where you are a member of a training center, which	Consider a scenario where you are a member of a training center, which	Consider a scenario where you are a member of a training center, which

recently have developed an app. This app gives you various information, such as timetable for group workouts, openings hours, special events etc. You can also use the app to enter the center, which means that the training center can track how often you exercise. The center also wants you to rate, on the app, the intensity of your workouts, how often and how many calories you eat, your weight, age, as well as your height. This is a trial project which will last for 3 months. In order to give this information to the training center, accept the privacy terms and conditions about how the training center will manage your information (cookies policy, secondary use...). To accept the privacy terms and conditions simply tick off the "I agree" button. After agreeing with the privacy terms, the training center will manage the personal information you provided.	recently have developed an app. This app gives you various information, such as timetable for group workouts, openings hours, special events etc. You can also use the app to enter the center, which means that the training center can track how often you exercise. The center also wants you to rate, on the app, the intensity of your workouts, how often and how many calories you eat, your weight, age, as well as your height. This is a trial project which will last for 3 months. If you agree to give this information to the training center they will be able to use your data to make algorithms which makes it possible to develop personal training-and nutrition plan only to use by you. This will enrich your training experience, as the plans is built on the data you provide to the training center. This means that you will get training-and nutrition plans personalized to your needs, through the app. If you wish, the app will also give you notifications when there is a new training- and nutrition plan developed to you. In order to give this information to the training center, accept the privacy terms and conditions about how the training center will manage your information (cookies policy, secondary use...). To accept the privacy terms and conditions simply tick off the "I agree" button. After agreeing with the privacy terms, the training center will manage the personal information you provided.	recently have developed an app. This app gives you various information, such as timetable for group workouts, openings hours, special events etc. You can also use the app to enter the center, which means that the training center can track how often you exercise. The center also wants you to rate, on the app, the intensity of your workouts, how often and how many calories you eat, your weight, age, as well as your height. This is a trial project which will last for 3 months. If you agree to give this information to the training center they will be able to use your data to make algorithms which makes it possible to develop weekly tutorials featuring new training methods, dieting etc. easily accessible in the app. As you are a part of the first group using the app, you will not have access to any tutorials during the three months of the project. However, the next group using the app will receive tutorials based on your privacy information. In other words, your personal information will be used to help other people gain more knowledge regarding training methods and dieting. In order to give this information to the training center, accept the privacy terms and conditions about how the training center will manage your information (cookies policy, secondary use...). To accept the privacy terms and conditions simply tick off the "I agree" button. After agreeing with the privacy terms, the training center will manage the personal information you provided.

Page 3

Thinking about the scenario you just read, please answer whether you agree or disagree with the given statements considering a scale from 1 to 7 where 1= "strongly disagree" and 7= "strongly agree".

Scales	**Items**	**Source**
Collection	Q1: I am concerned that the training center are collecting too much personal information about me Q2: It bothers me to give personal information to the training center	Hsu and Lin (2016)

	Q3: I need to think twice before providing my personal information to the training center Q4: It bothers me when the training center ask me for personal information	
Intention to use	Q5: I intend to use the app in the future Q6: I intend to visit the app as much as possible Q7: I intend to continue using the app in the future	Shin (2010) Davis et al. (1989)
WOM intention	Q8: I will recommend friends to train at this training center and use its app Q9: I will say good things about the training center and its app to others Q10: I bring up the training center and its app in a positive way in conversations I have with friends and acquaintances Q11: In social situations, I often speak favorably about the training center and its app	Laroche et al. (2005) R. N. Stone and Grønhaug (1993)
Improper access	Q12: The training center should devote more time and effort to preventing unauthorized access to personal information Q13: The training center should take more steps to ensure that the personal information in their files is accurate Q14: The training center should take more steps to ensure that unauthorized people cannot access personal information in their computers	Hsu and Lin (2016)
Manipulation check	Q15: Do not answer this question, simply move further to the next questions whiteout answering this question	
Manipulation check: Control	Q16: I believe I have control over who can get access to my personal information collected by the training center Q17: I think I have control over what personal information is released by the training center Q18: I believe I have control over how personal information is used by the training center Q19: I believe I can control my personal information provided to the training center	H. Xu et al. (2008)
Manipulation check: benefit of program	Q20: providing my personal information to the training center helps me	
Manipulation check: benefit of program	Q21. providing my personal information to the training center helps others	
Demographics	Age, gender, education, profession, nationality	

Every item was measured on a 7-point Likert scale, expect for the demographic questions.

Page 7

Thank you very much for your time and for your extraordinary willingness to participate to this research project.

Factor analyses, Study 1

Table 1
Factor analysis for ease of use

	Factor	Communalities
	1	
In my opinion, Smart Devices are easy to use	.92	.84
In my opinion, Smart Devices are fast to use	.89	.78
In my opinion, progress in Smart Devices is clear	.83	.69
My interaction with Smart Devices is understandable	.87	.76
Interacting with Smart Devices does not require a lot of my mental effort	.79	.62
Eigenvalue	3.95	
% of total variance	78.93	
Total variance	78.93	

Extraction Method: Maximum Likelihood.

Figure 1
Scree plot, ease of use

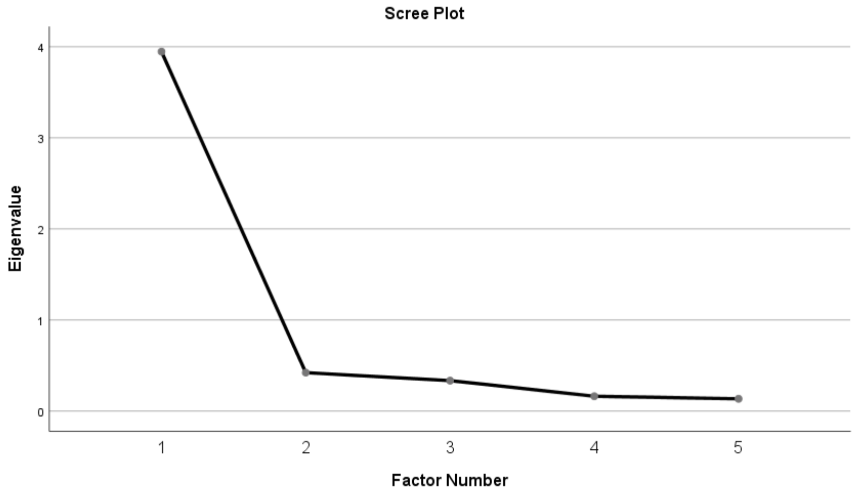


Table 2
Factor analysis for novelty

	Factor		Communalities
	1	2	
I find Smart Devices to be: New: Old	.25	.79	.51
I find Smart Devices to be: Original: Unoriginal		.86	.64
I find Smart Devices to be: Unusual: Common	-.44	.56	.72
I find Smart Devices to be: Familiar: Novel	.69		.53
I find Smart Devices to be: Typical: Atypical	.73	-.26	.77
I find Smart Devices to be: Stable: Unstable	.73	.29	.43
I find Smart Devices to be: Developed: Undeveloped	.77		.50
I find Smart Devices to be: Questionable: Unquestionable			.02
Eigenvalue	3.23	1.745	
% of total explained	40.37	21.83	
Total variance		62.20	

Extraction Method: Maximum Likelihood.

Figure 2
Scree plot, novelty

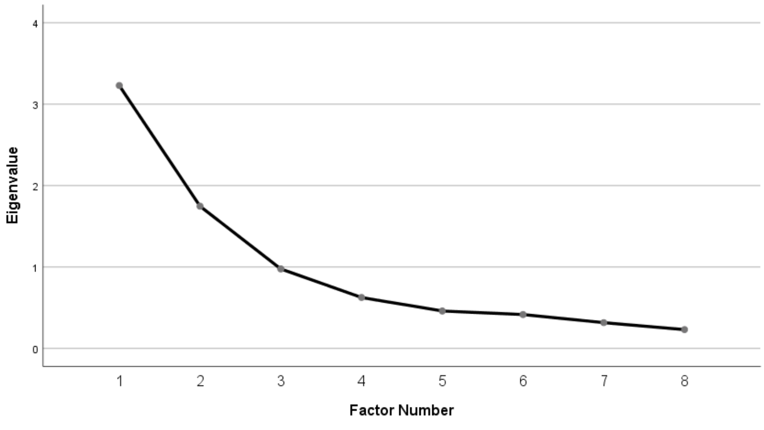


Table 3
Factor analysis for value perception

	Factor		Communalities
	1	2	
The value of Smart Devices is: Ineffective: Effective	.72		.56
The value of Smart Devices is: Not functional: Functional	.92		.73
The value of Smart Devices is: Impractical: Practical	.92		.74
The value of Smart Devices is: Useless: Useful	.98		.85
The value of Smart Devices is: Inefficient: Efficient	.83		.73
The value of Smart Devices is: Unproductive: Productive	.67		.57
The value of Smart Devices is: Not helpful: Helpful	.87		.82
The value of Smart Devices is: Not necessary: Necessary		.39	.28
The value of Smart Devices is: Poorly made: Well made	.31		.18
The value of Smart Devices is: Boring: Exciting		.80	.66
The value of Smart Devices is: Not a worthwhile product: A worthwhile product	.26	.61	.62
The value of Smart Devices is: Unappealing: Appealing		.73	.80
The value of Smart Devices is: Common: Unique	-.37	.63	.28
Eigenvalue	6.85	1.73	
% of total explained	52.67	13.32	
Total variance		65.99	

Extraction Method: Maximum Likelihood.

Figure 3
Scree plot, value perception

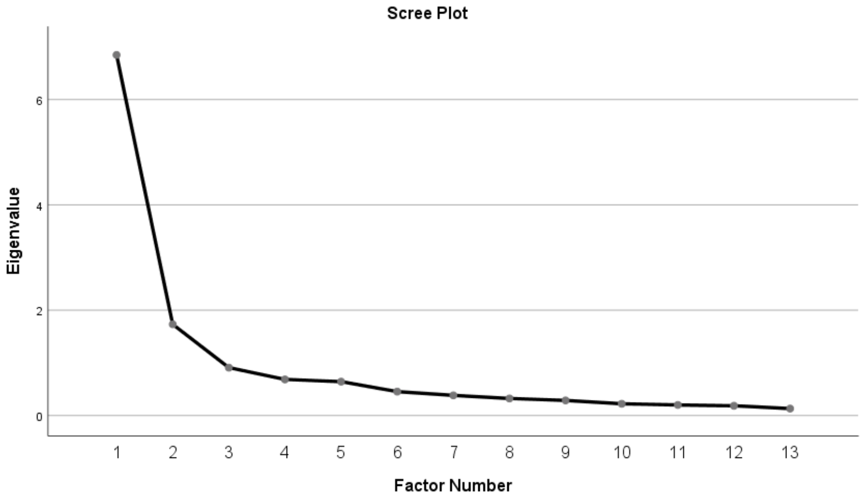


Table 4
Factor analysis for perceived complementarity

	Factor	Communalities
	1	
A wide range of Smart Device products is available	.83	.69
Using Smart Devices will allow me to finish various tasks (i.e., payments, identification and information exchange, home management, fitness monitoring etc.)	.87	.75
A wide range of apps concerning Smart Devices are available on smartphone	.91	.83
Eigenvalue	2.28	
% of total explained	75.84	
Total variance	75.84	

Extraction Method: Maximum Likelihood.

Figure 4
Scree plot, perceived complementarity

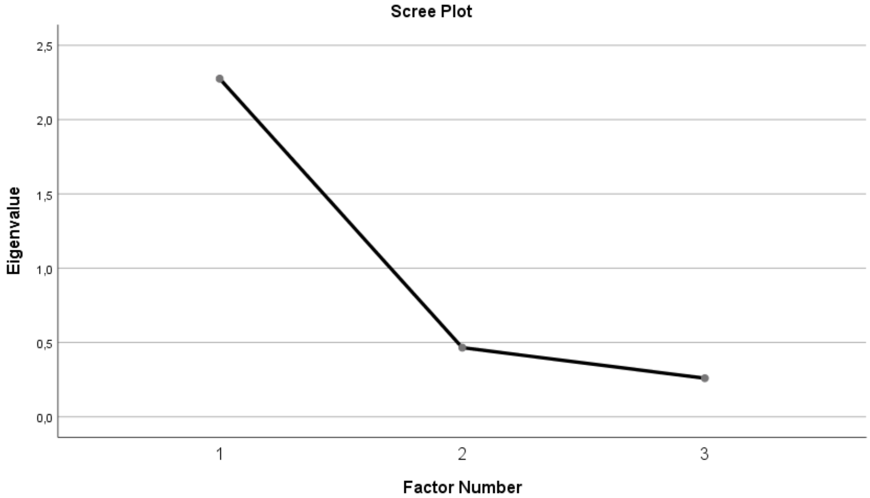
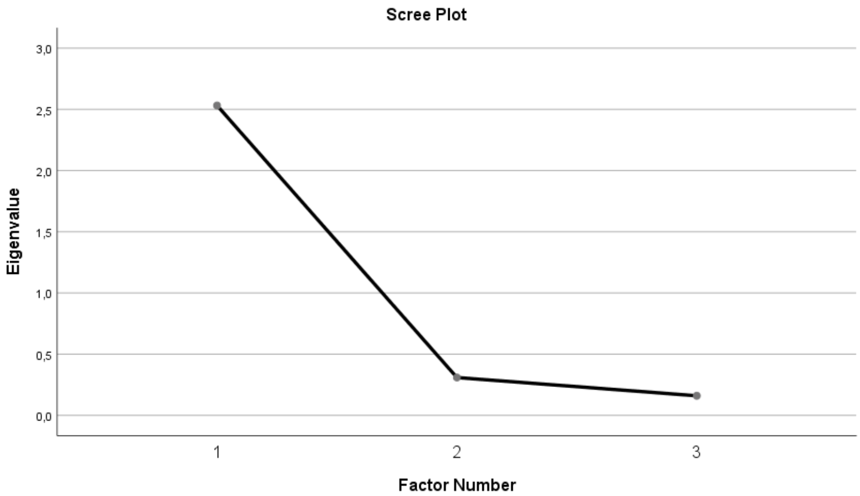


Table 5
Factor analysis for number of IoT services

	Factor	**Communalities**
	1	
I think a good number of Smart Devices can be used	.89	.79
I could easily find circumstances in which I can use Smart Devices	.94	.89
I think there are many reasons in daily life to use Smart Devices	.92	.85
Eigenvalue	2.53	
% of total explained	84.37	
Total variance	84.37	

Extraction Method: Maximum Likelihood.

Figure 5
Scree plot, number of IoT services



Cronbach alpha and correlation, Study 1

Table 6
Cronbach alpha and correlational results for every scale included in the questionnaire

Scales	M	SD	Reliability/ Correlation	Items
Privacy and security (Privacy and security)	4.42	1.76	r = .86, p = .000	3
Collection (Privacy and security)	4.55	1.78	r = .88, p = .000	2
Unauthorized secondary use (Privacy and security)	6.44	.87	α = .69	3
Improper access (Privacy and security)	6.21	.88	α = .82	2
Intrusiveness	2.92	1.29	α = .86	5
Dependence	3.74	1.38	α = .78	4
Ease of use	5.59	1.21	α = .93	5
Self-efficacy	6.02	1.24	α = .86	2 (3)
Number of IoT services (Network effect)	5.89	1.23	α = .91	3
Perceived critical mass (Network effect)	5.84	1.42	α = .96	4
Perceived compatibility (Network effect)	5.30	1.41	α = .91	3
Perceived complementarity (Network effect)	5.99	1.10	α = .84	3
Novelty 1	3.24	1.32	α = .73	3
Novelty 2	3.18	1.36	α = .80	3
Value perception 1	5.80	1.24	α = .93	7
Value perception 2	5.54	1.11	α = .86	3 (4)
Price	4.09	1.23	α = .93	7 (8)
Intention to buy	5.62	1.45	α = .97	3
WOM intention	4.88	1.42	α = .91	4
Risk	3.40	1.56	r = .75, p = .000	2
Knowledge	4.37	1.47	α = .88	4
Optimism (individual trait)	5.34	1.21	α = .83	3
Innovativeness (individual trait)	4.54	1.57	α = .91	5
Discomfort (individual trait)	3.82	1.05	α = .65	5 (6)
Insecurity (individual trait)	3.83	1.38	α = .81	5

Demographics, Study 1

Table 7
Demographic characteristics of the whole sample used in Study 1

		Frequency	Percent
Gender	Male	61	40.67
	Female	89	59.33
	Total	150	100
Age	18 - 30	112	74.67
	31 - 45	16	10.67
	46 - 60	16	10.67
	Over 60	6	4.00
	Total	150	100
Education	Lower than High School	1	.67
	High School	24	16.00

	Bachelor Degree	68	45.33
	Master Degree	56	37.33
	PhD	1	.67
	Total	150	100
Profession	Student	93	62.0
	Employee	44	29.3
	Self-Employee	3	2.0
	Retired	5	3.3
	Unemployed	3	2.0
	Other	2	1.3
	Total	150	100

Agglomeration schedule

Table 8

Agglomeration schedule used in the clustering analysis to determine number of clusters.

Stage	Cluster Combined			Stage Cluster First Appears		
	Cluster 1	Cluster 2	Coefficients	Cluster 1	Cluster 2	Next Stage
1	58	104	.31	0	0	44
2	141	144	.99	0	0	101
3	59	60	1.88	0	0	13
4	106	110	2.87	0	0	18
5	15	74	3.99	0	0	83
6	93	94	5.38	0	0	61
7	86	89	6.78	0	0	29
8	112	143	8.29	0	0	19
9	57	133	9.82	0	0	30
10	12	102	11.44	0	0	35
11	10	147	13.07	0	0	26
12	64	68	14.74	0	0	52
.						
.						
.						
.						
142	14	30	1260.91	140	127	145
143	2	3	1322.13	141	139	144
144	1	2	1386.52	136	143	149
145	7	14	1472.20	135	142	146
146	7	23	1591.47	145	138	148
147	76	77	1719.29	137	128	148
148	7	76	2007.11	146	147	149
149	1	7	2823.39	144	148	0

Note: there is made a jump from the 12. stage to the 142. as the model would have been very long otherwise and because the most interesting part is between the 148. stage and 149. stage.

Demographics, Cluster 1

Table 9
Demographic characteristics of respondents in cluster 1

		Frequency	Percent
Gender	Male	41	45.56
	Female	49	54.44
	Total	90	100
Age	18 - 30	62	68.89
	31 - 45	11	12.22
	46 - 60	12	13.33
	Over 60	5	5.56
	Total	90	100
Education	Lower than High School	0	0
	High School	16	17.78
	Bachelor Degree	39	43.33
	Master Degree	35	38.89
	PhD	0	0
	Total	90	100
Profession	Student	51	56.67
	Employee	29	32.22
	Self-Employee	2	2.22
	Retired	5	5.56
	Unemployed	2	2.22
	Other	1	1.11
	Total	90	100

Demographics, Cluster 2

Table 10
Demographic characteristics of respondents in cluster 2

		Frequency	Percent
Gender	Male	20	33.33
	Female	40	66.67
	Total	60	100
Age	18 - 30	50	83.33
	31 - 45	5	8.33
	46 - 60	4	6.67
	Over 60	1	1.67
	Total	60	100
Education	Lower than High School	1	1.67
	High School	8	13.33
	Bachelor Degree	29	48.33
	Master Degree	21	35.00
	PhD	1	1.67
	Total	60	100

Profession	Student	42	70.00
	Employee	15	25.00
	Self-Employee	1	1.67
	Retired	0	0
	Unemployed	1	1.67
	Other	1	1.67
	Total	60	100

Cronbach alpha, pretest

Table 11
Pretest 1: Cronbach alpha analysis for control

Scales	M	SD	Reliability	Items
Control	4.13	1.78	α = .94	4

Manipulation checks, pretest 1

Table 12
Pretest 1: Manipulation checks of the quality of the control scenarios

	Score	Frequency	Percent
I can easily put myself in the position which the scenario describes	3	1	2.44
	4	5	12.20
	5	9	21.95
	6	11	26.83
	7	15	36.59
	Total	41	100
I think the scenario was clear and understandable	3	0	0
	4	1	2.44
	5	10	24.39
	6	18	43.90
	7	12	29.27
	Total	41	100

Manipulation checks, control scenario (pretest 1)

Table 13
Pretest 1: Manipulation check for control scenario. One-way ANOVA

		N	M	SD		df	SS	MS	F	P
Control	Low control	18	4.26	1.78	Between groups	1	19.46	19.46	8.48	.006
	High control	23	5.65	1.27	Within groups	39	89.53	2.30		
	Total	41	5.04	1.65	Total	40	108.99			

Manipulation checks, pretest 2

Table 14

Pretest 2: Manipulation checks of the quality of the benefit scenarios

	Score	Frequency	Percent
I can easily put myself in the position which the scenario describes	3	1	2.56
	4	5	12.82
	5	11	28.21
	6	10	25.64
	7	12	30.77
	Total	39	100
I think the scenario was readable	3	2	5.13
	4	0	0
	5	7	17.95
	6	9	23.08
	7	21	53.85
	Total	39	100
I think the scenario was clear and understandable	3	1	2.56
	4	2	5.13
	5	4	10.26
	6	14	35.90
	7	18	46.15
	Total	39	100

Manipulation checks, benefit scenario (pretest 2)

Table 15

Pretest 2: Manipulation check for benefit scenarios. One-way ANOVA

		N	M	SD		df	SS	MS	F	P
Providing my personal information to the training center helps **me**	Control group	15	5.07	1.44	Between Groups	2	22.70	11.35	3.83	.031
	Self-benefit	13	5.38	1.50	Within Groups	36	106.74	2.97		
	Others-benefit	11	3.55	2.25	Total	38	129.44			
	Total	39	4.74	1.85						
Providing my personal information to the training center	Control group	15	5.00	1.46	Between Groups	2	15.65	7.82	3.77	.033
	Self-benefit	13	4.62	1.66	Within Groups	36	74.71	2.08		
	Others-benefit	11	6.18	1.08	Total	38	90.36			
	Total	39	5.21	1.54						

helps
others

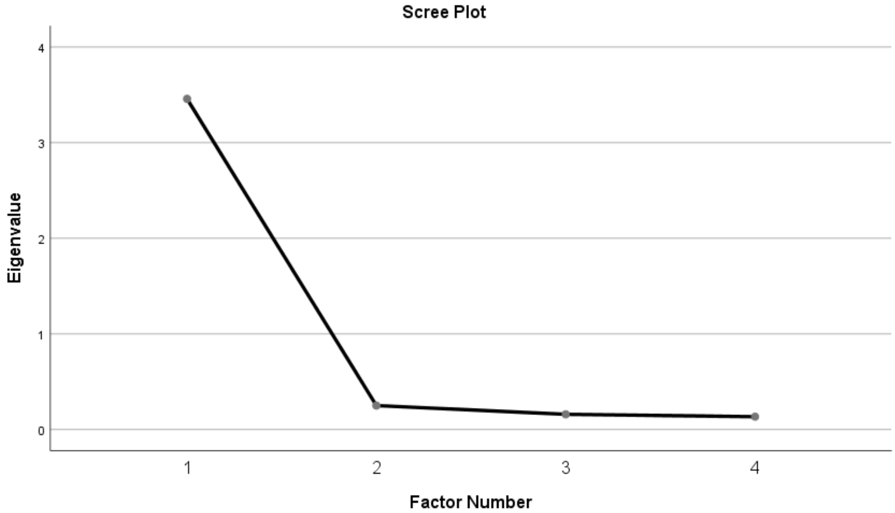
Factor analysis, Study 2

Table 16
Factor analysis for collection

	Factor	Communalities
	1	
I am concerned that the training center are collecting too much personal information about me	.89	.79
It bothers me to give personal information the training center	.93	.86
I need to think twice before providing my personal information to the training center	.85	.72
It bothers me when the training center ask me for personal information	.93	.87
Eigenvalue	3.43	
% of total explained	85.64	
Total variance	85.64	

Extraction Method: Maximum Likelihood.

Figure 6
Scree plot, collection



Cronbach alpha, Study 2

Table 17
Study 2: Cronbach alpha analysis for collection, intention to use, WOM intention, improper access, and control

Scales	M	SD	Reliability	Items
Collection	4.74	1.69	α = .95	4
Intention to use	4.37	1.68	α = .95	3
WOM intention	4.47	1.60	α = .96	4
Improper access	5.72	1.11	α = .81	3
Control	4.13	1.78	α = .94	4

Demographics, Study 2

Table 18
Study 2: Descriptive statistics of the sample, namely profession, education level, age, and gender.

		Frequency	Percent
Profession	Student	22	8.18
	Employee	179	66.54
	Self-Employee	44	16.36
	Retired	5	1.89
	Unemployed	14	5.20
	Other	5	1.89
	Total	269	100
Education level	Lower than High School	1	.37
	High School	57	21.19
	Bachelor Degree	157	58.36
	Master Degree	48	17.84
	PhD	6	2.23
	Total	269	100
Age	18 - 30	116	43.12
	31 - 45	106	39.41
	46 - 60	37	13.75
	Over 60	10	3.72
	Total	269	100
Gender	Male	165	61.34
	Female	104	38.66
	Total	269	100

Manipulation checks control (Study 2)

Table 19

Desciptives statistics for manipulation check for control.

		N	M	SD
Control	Low control	188	3.83	1.90
	High control	203	4.31	1.57
	Total	391	4.08	1.75

Table 20

One-way ANOVA for manipulation check of control.

		df	SS	MS	F	P
Control	Between Groups	1	22.64	22.64	7.51	.006
	Within Groups	389	1173.39	3.02		
	Total	390	1196.03			

Manipulation checks benefit (Study 2)

Table 21

Desciptives statistics for manipulation check for benefit.

		N	M	SD
Providing my personal information to the training center helps **me**	Control group	122	4.54	1.65
	Self-benefit	132	4.97	1.52
	Others-benefit	137	4.05	1.78
	Total	391	4.51	1.70
Providing my personal information to the training center helps **others**	Control group	122	4.58	1.53
	Self-benefit	132	4.48	1.73
	Others-benefit	137	5.01	1.59
	Total	391	4.70	1.63

Table 22

One-way ANOVA for manipulation check of benefit.

		df	SS	MS	F	P
Providing my personal information to the training center helps **me**	Between Groups	2	56.86	28.43	10.34	.000
	Within Groups	388	1066.82	2.75		
	Total	390	1123.67			
	Between Groups	2	20.75	10.37	3.95	.020

Providing my personal information to the training center helps **others**	Within Groups	388	1019.64	2.63
	Total	390	1040.39	

Descriptive statistics for ANOVA analysis

Table 23

Descriptive statistics for benefit under high and low control, related to the univariate linear regression

		N	**M**	**SD**
Low control	Self-benefit	66	4.28	1.85
	Others-benefit	60	5.38	1.27
	Total	126	4.80	1.68
High control	Self-benefit	66	4.48	1.73
	Others-benefit	77	4.88	1.67
	Total	143	4.69	1.70
Total	Self-benefit	132	4.38	1.78
	Others-benefit	137	5.10	1.53
	Total	269	4.74	1.69

Independent sample t-test (low control)

Table 24

Study 2: Independendent sample T-test for low control of personal information

		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	**P**	**t**	**df**	**Sig. (2-tailed)**	**Mean Difference**	**Std. Error Difference**	**Lower**	**Upper**
Collection	Equal variances assumed	13.67	.000	-3.85	124.00	.000	-1.10	.29	-1.66	-.53
	Equal variances not assumed			-3.92	115.77	.000	-1.10	.28	-1.65	-.54

a. Control = Low control

Independent sample t-test (high control)

Table 25

Study 2: Independendent sample T-test for high control of personal information

		Levene's Test for	t-test for Equality of Means

		Equality of Variances								
									95% Confidence Interval of the Difference	
		F	**P**	**t**	**df**	**Sig. (2-tailed)**	**Mean Difference**	**Std. Error Difference**	**Lower**	**Upper**
Collection	Equal variances assumed	.04	.833	-1.40	141	.163	-.40	.28	-.96	.16
	Equal variances not assumed			-1.40	136.27	.164	-.40	.29	-.96	.16

a. Control = High control

ANOVA, Study 2

Table 26

Desciptives statistics for WOM intention and intention to use under high and low control

		N	**M**	**SD**
WOM intention	Low control	126	4.31	1.68
	High control	143	4.60	1.51
	Total	269	4.47	1.60
Intention to use	Low control	126	4.27	1.77
	High control	143	4.45	1.60
	Total	269	4.37	1.68

Table 27

One-way ANOVA of WOM intention and intention to use on control

		df	**SS**	**MS**	**F**	**P**
WOM intention	Between Groups	1	5.62	5.62	2.21	.138
	Within Groups	267	677.16	2.54		
	Total	268	682.78			
Intention to use	Between Groups	1	2.11	2.11	.75	.388
	Within Groups	267	752.37	2.82		
	Total	268	754.48			

ANOVA, Study 2

Table 28

Desciptives statistics for WOM intention and intention to use under self-benefit and others-benefit

		N	**M**	**SD**
WOM intention	Self-benefit	132	4.69	1.57
	Others-benefit	137	4.26	1.60
	Total	269	4.47	1.60
Intention to use	Self-benefit	132	4.58	1.68
	Others-benefit	137	4.16	1.66
	Total	269	4.37	1.68

Table 29

One-way ANOVA of WOM intention and intention to use on benefit

		df	**SS**	**MS**	**F**	**P**
WOM intention	Between Groups	1	12.33	12.33	4.91	.028
	Within Groups	267	670.45	2.51		
	Total	268	682.78			
Intention to use	Between Groups	1	11.87	11.87	4.27	.040
	Within Groups	267	742.61	2.78		
	Total	268	754.48			

References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*(6221), 509-514.

Acquity Group. (2014). *Acquity Group 2014 Internet of Things study, part of Accenture Interactive*. Retrieved from https://acquitygroup.wordpress.com/2014/08/21/acquity-group-2014-internet-of-things-study/

Agarwal, S., & Teas, R. K. (2001). Perceived value: mediating role of perceived risk. *Journal of Marketing theory and Practice*, *9*(4), 1-14.

Ajzen, I., & Fishbein, M. (1980). Understanding attitudes and predicting social behaviour. *Michigan: Prentice-Hall*.

Alba, J., Lynch, J., Weitz, B., Janiszewski, C., Lutz, R., Sawyer, A., & Wood, S. (1997). Interactive home shopping: consumer, retailer, and manufacturer incentives to participate in electronic marketplaces. *The Journal of Marketing*, 38-53.

Altman, I. (1975). The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding.

Andersson, P., & Heinonen, K. (2002). Acceptance of mobile services-insights from the Swedish market for mobile telephony. *Working Paper Series in Business Administration, 2002*(16).

Antioco, M., & Kleijnen, M. (2010). Consumer adoption of technological innovations. *European Journal of Marketing, 44*(11/12), 1700-1724. doi:10.1108/03090561011079846

Arnett, D. B., German, S. D., & Hunt, S. D. (2003). The identity salience model of relationship marketing success: The case of nonprofit marketing. *Journal of Marketing, 67*(2), 89-105.

Arts, J. W. C., Frambach, R. T., & Bijmolt, T. H. A. (2011). Generalizations on consumer innovation adoption: A meta-analysis on drivers of intention and behavior. *International Journal of Research in Marketing, 28*(2), 134-144. doi:10.1016/j.ijresmar.2010.11.002

Assurant Inc. (2017). *The Connected Future. Navigating promise and risk*. Retrieved from https://www.assurant.com/documents/assurant/publications/aiz-news-connectedfuturereportbrief-2017-01-05.pdf?sfvrsn=8

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks, 54*(15), 2787-2805. doi:10.1016/j.comnet.2010.05.010

Balta-Ozkan, N., Davidson, R., Bicket, M., & Whitmarsh, L. (2013). Social barriers to the adoption of smart homes. *Energy Policy, 63*, 363-374.

Bandyopadhyay, D., & Sen, J. (2011). Internet of things: Applications and challenges in technology and standardization. *Wireless Personal Communications, 58*(1), 49-69.

Barnett, H. G. (1953). *Innovation: the basis of cultural change*. New York, US: McGraw-Hill.

Baron, R. M., & Kenny, D. A. (1986). The moderator–mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. *Journal of personality and social psychology, 51*(6), 1173.

Bearden, W. O., & Shimp, T. A. (1982). The use of extrinsic cues to facilitate product adoption. *Journal of marketing research*, 229-239.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in information systems. *MIS quarterly, 35*(4), 1017-1042.

Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. *The Journal of Strategic Information Systems, 11*(3-4), 245-270.

Biesdorf, S., Court, D., & Willmott, P. (2013). Big data: What's your plan. *Mckinsey Quarterly 2013*.

Björnsjö, A., Viglino, M., & Lovati, G. (2016). *Accenture Igniting Growth in Consumer Technology. Digital Consumer Survey 2016*. Retrieved from https://www.accenture.com/_acnmedia/PDF-3/Accenture-Igniting-Growth-in-Consumer-Technology.pdf

Blau, P. (1964). *Exchange and power in social life*. New York John Wiley & Sons.

Boeck, H., Roy, J., Durif, F., & Grégoire, M. (2011). The effect of perceived intrusion on consumers' attitude towards using an RFID-based marketing program. *Procedia Computer Science, 5*, 841-848.

Borgia, E. (2014). The Internet of Things vision: Key features, applications and open issues. *Computer Communications, 54*, 1-31. doi:10.1016/j.comcom.2014.09.008

Bradley, J., Barbier, J., & Handler, D. (2013). *Embracing the Internet of Everything To Capture Your Share of $14.4 Trillion* Retrieved from https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoE_Economy.pdf

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced confidences: Privacy and the control paradox. *Social Psychological and Personality Science, 4*(3), 340-347.

Brody, P., & Pureswaran, V. (2015). The next digital gold rush: how the internet of things will create liquid, transparent markets. *Strategy & Leadership, 43*(1), 36-41.

Buhrmester, M., Kwang, T., & Gosling, S. D. (2011). Amazon's Mechanical Turk: A new source of inexpensive, yet high-quality, data? *Perspectives on psychological science, 6*(1), 3-5.

Campbell, M. C., & Goodstein, R. C. (2001). The moderating effect of perceived risk on consumers' evaluations of product incongruity: Preference for the norm. *Journal of consumer research, 28*(3), 439-449.

Castaño, R., Sujan, M., Kacker, M., & Sujan, H. (2008). Managing consumer uncertainty in the adoption of new products: Temporal distance and mental simulation. *Journal of marketing research, 45*(3), 320-336.

Castellion, G., & Markham, S. K. (2013). Perspective: new product failure rates: influence of argumentum ad populum and self interest. *Journal of Product Innovation Management, 30*(5), 976-979.

Cavoukian, A., Polonetsky, J., & Wolf, C. (2010). Smartprivacy for the smart grid: embedding privacy into the design of electricity conservation. *Identity in the Information Society, 3*(2), 275-294.

Cespedes, F. V., & Smith, H. J. (1993). Database marketing: New rules for policy and practice. *Sloan Management Review, 34*(4), 7.

Chandon, P., Wansink, B., & Laurent, G. (2000). A benefit congruency framework of sales promotion effectiveness. *Journal of Marketing, 64*(4), 65-81.

Chang, M. K., & Cheung, W. (2001). Determinants of the intention to use Internet/WWW at work: a confirmatory study. *Information & Management, 39*(1), 1-14.

Chang, Y., Dong, X., & Sun, W. (2014). Influence of characteristics of the Internet of Things on consumer purchase intention. *Social Behavior and Personality: an international journal, 42*(2), 321-330.

Charlton, J. P. (2002). A factor analytic investigation of computer 'addiction'and engagement. *British journal of psychology, 93*(3), 329-344.

Chellappa, R. K., & Sin, R. G. (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information technology and management, 6*(2-3), 181-202.

Chui, M., Markus, L., & Roger, R. (2010). The Internet of things. *McKinsey Quarterly*.

Cohen, R. L. (1987). Distributive justice: Theory and research. *Social justice research, 1*(1), 19-40.

Compeau, D. R., & Higgins, C. A. (1995). Computer self-efficacy: Development of a measure and initial test. *MIS quarterly*, 189-211.

Conner, K. R. (1995). Obtaining strategic advantage from being imitated: When can encouraging "clones" pay? *Management Science, 41*(2), 209-225.

Cox, D., & Cox, A. D. (2002). Beyond first impressions: The effects of repeated exposure on consumer liking of visually complex and simple product designs. *Journal of the Academy of Marketing Science, 30*(2), 119-130.

Cox, D. S., & Cox, A. D. (1988). What does familiarity breed? Complexity as a moderator of repetition effects in advertisement evaluation. *Journal of consumer research, 15*(1), 111-116.

Cranor, L. F., Reagle, J., & Ackerman, M. S. (2000). Beyond concern: Understanding net users' attitudes about online privacy. *The Internet upheaval: raising questions, seeking answers in communications policy*, 47-70.

Culnan, M. J. (1993). " How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use. *MIS quarterly*, 341-363.

Culnan, M. J. (1995). Consumer awareness of name removal procedures: Implications for direct marketing. *Journal of Interactive Marketing, 9*(2), 10-19.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly*, 319-340.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: a comparison of two theoretical models. *Management Science, 35*(8), 982-1003.

DelVecchio, D., & Smith, D. C. (2005). Brand-extension price premiums: the effects of perceived fit and extension product category risk. *Journal of the Academy of Marketing Science, 33*(2), 184-196.

Desarnauts, B. (2015, November 30). Dissatisfaction Learnings. First insights into unsatisfied Apple Watch owners. Retrieved from https://medium.com/wristly-thoughts/dissatisfaction-learnings-48c26d564bc1

Dhir, A., Chen, S., & Nieminen, M. (2015). Predicting adolescent Internet addiction: The roles of demographics, technology accessibility, unwillingness to communicate and sought Internet gratifications. *Computers in Human Behavior, 51*, 24-33.

Dholakia, U. M. (2001). A motivational process model of product involvement and consumer risk perception. *European Journal of Marketing, 35*(11/12), 1340-1362.

Dimofte, C. V., Forehand, M. R., & Deshpande, R. (2003). Ad schema incongruity as elicitor of ethnic self-awareness and differential advertising response. *Journal of Advertising, 32*(4), 7-17.

Dowling, G. R., & Staelin, R. (1994). A model of perceived risk and intended risk-handling activity. *Journal of consumer research, 21*(1), 119-134.

Easterby-Smith, M., Thorpe, R., & Jackson, P. R. (2012). Management research. *Sage*, pp. 95-97.

Edwards, S. M., Li, H., & Lee, J.-H. (2002). Forced exposure and psychological reactance: Antecedents and consequences of the perceived intrusiveness of pop-up ads. *Journal of Advertising, 31*(3), 83-95.

Ellen, P. S., Bearden, W. O., & Sharma, S. (1991). Resistance to technological innovations: an examination of the role of self-efficacy and performance satisfaction. *Journal of the Academy of Marketing Science, 19*(4), 297-307.

Engel, J. F., Kegerreis, R. J., & Blackwell, R. D. (1969). Word-of-mouth communication by the innovator. *The Journal of Marketing*, 15-19.

Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-services adoption: a perceived risk facets perspective. *International journal of human-computer studies, 59*(4), 451-474.

Fenech, T. (2002). Exploratory study into wireless application protocol shopping. *International Journal of Retail & Distribution Management, 30*(10), 482-497.

Ferreira, J. B., da Rocha, A., & da Silva, J. F. (2014). Impacts of technology readiness on emotions and cognition in Brazil. *Journal of Business Research, 67*(5), 865-873.

Fisher, R. J., Vandenbosch, M., & Antia, K. D. (2008). An empathy-helping perspective on consumers' responses to fund-raising appeals. *Journal of consumer research, 35*(3), 519-531.

Garcia, R., & Atkin, T. (2006). Coopetition for the diffusion of resistant innovations: a case study in the global wine industry using an agent-based model. *Agent-Based Models of Market Dynamics and Consumer Behaviour, Institute of Advanced Studies, University of Surrey, Guildford*.

Garcia, R., Bardhi, F., & Friedrich, C. (2007). Overcoming consumer resistance to innovation. *MIT Sloan management review, 48*(4), 82.

Gartner, I. (2014). *"Gartner Says 4.9 Billion Connected 'Things' Will Be in Use in 2015; In 2020, 25 Billion Connected 'Things' Will Be in Use," Press Release, Gartner*. Retrieved from http://www.gartner.com/newsroom/id/2905717

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS quarterly, 27*(1), 51-90.

Gilliland, S. W. (1993). The perceived fairness of selection systems: An organizational justice perspective. *Academy of management review, 18*(4), 694-734.

Godes, D. (2011). Commentary—Invited Comment on "Opinion Leadership and Social Contagion in New Product Diffusion". *Marketing Science*, *30*(2), 224-229.

Goodman, J. K., Cryder, C. E., & Cheema, A. (2013). Data collection in a flat world: The strengths and weaknesses of Mechanical Turk samples. *Journal of Behavioral Decision Making*, *26*(3), 213-224.

Goodwin, C. (1991). Privacy: Recognition of a consumer right. *Journal of Public Policy & Marketing*, 149-166.

GreenJinn. (2018). GreenJinn.com. Retrieved from https://www.greenjinn.com/

Greenough, J. (2016). *How the 'Internet of Things' will impact consumers, businesses, and governments in 2016 and beyond. Business insider*. Retrieved from http://www.businessinsider.com/how-the-internet-of-things-market-will-grow-2014-10?IR=T

Grewal, D., Monroe, K. B., & Krishnan, R. (1998). The effects of price-comparison advertising on buyers' perceptions of acquisition value, transaction value, and behavioral intentions. *The Journal of Marketing*, 46-59.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645-1660. doi:10.1016/j.future.2013.01.010

Hadlington, L. J. (2015). Cognitive failures in daily life: Exploring the link with Internet addiction and problematic mobile phone use. *Computers in Human Behavior, 51*, 75-81.

Hall, B. H., & Khan, B. (2003). Adoption of new technology. *UC Berkeley Working Papers Departent of Economics*.

Harris, L., & Westin, A. F. (1990). The Equifax Report on Consumers in the Information Age. *Atlanta, GA: Equifax Inc*.

Haws, K. L., & Bearden, W. O. (2006). Dynamic pricing and consumer fairness perceptions. *Journal of consumer research, 33*(3), 304-311.

Heidenreich, S., Kraemer, T., & Handrich, M. (2016). Satisfied and unwilling: Exploring cognitive and situational resistance to innovations. *Journal of Business Research*, *69*(7), 2440-2447. doi:10.1016/j.jbusres.2016.01.014

Hérault, S., & Belvaux, B. (2014). Privacy paradox et adoption de technologies intrusives Le cas de la géolocalisation mobile/Privacy paradox and the adoption of intrusive technologies. The case of mobile location-based services. *Décisions Marketing*(74), 67.

Herbig, P. A., & Day, R. L. (1992). Customer acceptance: the key to successful introductions of innovations. *Marketing Intelligence & Planning, 10*(1), 4-15.

Herbig, P. A., & Kramer, H. (1994). The effect of information overload on the innovation choice process: Innovation overload. *Journal of Consumer Marketing, 11*(2), 45-54.

Herzenstein, M., Posavac, S. S., & Brakus, J. J. (2007). Adoption of new and really new products: The effects of self-regulation systems and risk salience. *Journal of marketing research, 44*(2), 251-260.

Hilgard, E. R., & Bower, G. H. (1975). *Theories of learning*.

Hill, T., Smith, N. D., & Mann, M. F. (1986). Communicating innovations: Convincing computer phobics to adopt innovative technologies. *ACR North American Advances*.

Hirschman, E. C. (1987). Adoption of an incredibly complex innovation: propositions from a humanistic vantage point. *ACR North American Advances*.

Hirunyawipada, T., & Paswan, A. K. (2006). Consumer innovativeness and perceived risk: implications for high technology product adoption. *Journal of Consumer Marketing*, *23*(4), 182-198. doi:10.1108/07363760610674310

Hoeffler, S. (2003). Measuring preferences for really new products. *Journal of marketing research, 40*(4), 406-420.

Hoffman, D. L., & Novak, T. (2015). Emergent experience and the connected consumer in the smart home assemblage and the internet of things. *The center of the connected consumer, the George Washington University School of Business*.

Hoffman, D. L., Novak, T. P., & Venkatesh, A. (2004). Has the Internet become indispensable? *Communications of the ACM, 47*(7), 37-42.

Hong, A., Nam, C., & Kim, S. (2017). Analysis of the barriers that consumers encounter when smart home service is introduced in South Korea.

Hoyer, W. D., & MacInnis, D. J. (1997). Consumer Behavior. Boston. *NY: Houghton Mifflin Company*.

Hsu, C. L., & Lin, J. C. C. (2016). An empirical examination of consumer adoption of Internet of Things services: Network externalities and concern for information privacy perspectives. *Computers in Human Behavior, 62*, 516-527. doi:10.1016/j.chb.2016.04.023

Hurter, J. A. P., & Rubenstein, A. H. (1978). Market penetration by new innovations: the technological literature. *Technological Forecasting and Social Change, 11*(3), 197-221.

IDC. (2014). Retrieved from http://www.zdnet.com/article/internet-of-things-market-to-hit-7-1-trillion-by-2020-idc/.Iimi

Inquiry, W. (1997). Financial System Inquiry Final Report. In: Canberra: Commonwealth of Australia.

Jacoby, J., & Kaplan, L. B. (1972). The components of perceived risk. *ACR Special Volumes*.

Janssens, W., De Pelsmacker, P., & Van Kenhove, P. (2008). *Marketing research with SPSS*: Pearson Education.

Jansson, J., Marell, A., & Nordlund, A. (2010). Green consumer behavior: determinants of curtailment and eco-innovation adoption. *Journal of Consumer Marketing, 27*(4), 358-370.

Jarvenpaa, S. L., Lang, K. R., Takeda, Y., & Tuunainen, V. K. (2003). Mobile commerce at crossroads. *Communications of the ACM, 46*(12), 41-44.

John, A., & Klein, J. (2003). The boycott puzzle: consumer motivations for purchase sacrifice. *Management Science, 49*(9), 1196-1209.

Johnson, C. A. (1974). Privacy as personal control. *Man-environment interactions: evaluations and applications: part, 2*, 83-100.

Kahneman, D., & Tversky, A. (1979). Prospect Theory: An Analysis of Decision under Risk. *Econometrica, 47*(2), 263-291.

Kang, Y., & Kim, S. (2009). Understanding user resistance to participation in multihop communications. *Journal of Computer-Mediated Communication, 14*(2), 328-351.

Kaplan, L. B., Szybillo, G. J., & Jacoby, J. (1974). Components of perceived risk in product purchase: A cross-validation. *Journal of applied psychology, 59*(3), 287.

Karahanna, E., & Limayem, M. (2000). E-mail and v-mail usage: Generalizing across technologies. *Journal of organizational computing and electronic commerce, 10*(1), 49-66.

Karahanna, E., Straub, D. W., & Chervany, N. L. (1999). Information technology adoption across time: a cross-sectional comparison of pre-adoption and post-adoption beliefs. *MIS quarterly*, 183-213.

Katz, M. L., & Shapiro, C. (1985). Network externalities, competition, and compatibility. *The American economic review, 75*(3), 424-440.

Kelvin, P. (1973). A social psychological examination of privacy. *British Journal of Clinical Psychology, 12*(3), 248-261.

Kim, H. W., Chan, H. C., & Gupta, S. (2007). Value-based adoption of mobile internet: an empirical investigation. *Decision support systems, 43*(1), 111-126.

Kleijnen, M., De Ruyter, K., & Wetzels, M. (2007). An assessment of value creation in mobile service delivery and the moderating role of time consciousness. *Journal of retailing, 83*(1), 33-46.

Kleijnen, M., Lee, N., & Wetzels, M. (2009). An exploration of consumer resistance to innovation and its antecedents. *Journal of Economic Psychology, 30*(3), 344-357.

Klerck, D., & Sweeney, J. C. (2007). The effect of knowledge types on consumer perceived risk and adoption of genetically modified foods. *Psychology & Marketing, 24*(2), 171-193.

Kolodinsky, J. M., Hogarth, J. M., & Hilgert, M. A. (2004). The adoption of electronic banking technologies by US consumers. *International Journal of Bank Marketing, 22*(4), 238-259. doi:10.1108/02652320410542536

Kuisma, T., Laukkanen, T., & Hiltunen, M. (2007). Mapping the reasons for resistance to Internet banking: A means-end approach. *International Journal of Information Management, 27*(2), 75-85.

Laroche, M., Yang, Z., McDougall, G. H. G., & Bergeron, J. (2005). Internet versus bricks-and-mortar retailers: An investigation into intangibility and its consequences. *Journal of retailing, 81*(4), 251-267.

Lassar, W. M., Manolis, C., & Lassar, S. S. (2005). The relationship between consumer innovativeness, personal characteristics, and online banking adoption. *International Journal of Bank Marketing, 23*(2), 176-199. doi:10.1108/02652320510584403

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*(7), 2432-2439. doi:10.1016/j.jbusres.2016.01.013

Laukkanen, T., & Lauronen, J. (2005). Consumer value creation in mobile banking services. *International journal of mobile Communications, 3*(4), 325-338.

Laukkanen, T., Sinkkonen, S., Kivijärvi, M., & Laukkanen, P. (2007). Innovation resistance among mature consumers. *Journal of Consumer Marketing, 24*(7), 419-427. doi:10.1108/07363760710834834

Lazar, A., Koehler, C., Tanenbaum, J., & Nguyen, D. H. (2015, 2015). *Why we use and abandon smart devices.* Paper presented at the In Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing

Lee, C. H., & Cranage, D. A. (2011). Personalisation–privacy paradox: The effects of personalisation and privacy assurance on customer responses to travel Web sites. *Tourism Management, 32*(5), 987-994.

Liao, Z., & Cheung, M. T. (2001). Internet-based e-shopping and consumer attitudes: an empirical study. *Information & Management, 38*(5), 299-306.

Licoppe, C., & Heurtin, J. P. (2001). Managing one's availability to telephone communication through mobile phones: A French case study of the development dynamics of mobile phone use. *Personal and Ubiquitous Computing, 5*(2), 99-108.

Lin, J.-S. C., & Hsieh, P.-L. (2007). The influence of technology readiness on satisfaction and behavioral intentions toward self-service technologies. *Computers in Human Behavior, 23*(3), 1597-1615.

Littler, D., & Melanthiou, D. (2006). Consumer perceptions of risk and uncertainty and the implications for behaviour towards innovative retail services: The case of Internet Banking. *Journal of Retailing and Consumer Services, 13*(6), 431-443. doi:10.1016/j.jretconser.2006.02.006

Lo, S.-K., Wang, C.-C., & Fang, W. (2005). Physical interpersonal relationships and social anxiety among online game players. *Cyberpsychology & behavior, 8*(1), 15-20.

Locander, W. B., & Hermann, P. W. (1979). The effect of self-confidence and anxiety on information seeking in consumer risk reduction. *Journal of marketing research*, 268-274.

López, T. S., Ranasinghe, D. C., Harrison, M., & McFarlane, D. (2011). Adding sense to the Internet of Things. *Personal and Ubiquitous Computing, 16*(3), 291-308. doi:10.1007/s00779-011-0399-8

Lu, H.-P., Hsu, C.-L., & Hsu, H.-Y. (2005). An empirical study of the effect of perceived risk upon intention to use online applications. *Information Management & Computer Security, 13*(2), 106-120.

Lu, J., Yao, J. E., & Yu, C.-S. (2005). Personal innovativeness, social influences and adoption of wireless Internet services via mobile technology. *The Journal of Strategic Information Systems, 14*(3), 245-268.

Madakam, S., Ramaswamy, R., & Tripathi, S. (2015). Internet of Things (IoT): A Literature Review. *Journal of Computer and Communications, 03*(05), 164-173. doi:10.4236/jcc.2015.35021

Malhotra, N. K. (2009). *Marketig Research. An applied orientation* (Vol. 6). New Jersey, USA.

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.

Malina, L., Hajny, J., Fujdiak, R., & Hosek, J. (2016). On perspective of security and privacy-preserving solutions in the internet of things. *Computer Networks, 102*, 83-95. doi:10.1016/j.comnet.2016.03.011

Mallat, N. (2007). Exploring consumer adoption of mobile payments–A qualitative study. *The Journal of Strategic Information Systems, 16*(4), 413-432.

Mani, Z., & Chouk, I. (2016). Drivers of consumers’ resistance to smart products. *Journal of Marketing Management, 33*(1-2), 76-97. doi:10.1080/0267257x.2016.1245212

Mano, H., & Oliver, R. L. (1993). Assessing the dimensionality and structure of the consumption experience: evaluation, feeling, and satisfaction. *Journal of consumer research, 20*(3), 451-466.

Manyika, J., Chui, M., Bisson, P., Woetzel, J., Dobbs, R., Bughin, J., & Aharon, D. (2015). *Unlocking the potential of the Internet of Things. McKinsey Global Institute*. Retrieved from https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world

Margulis, S. T. (1977). Conceptions of privacy: Current status and next steps. *Journal of Social Issues, 33*(3), 5-21.

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing, 81*(1), 36-58.

Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science, 45*(2), 135-155.

Martins, C., Oliveira, T., & Popovič, A. (2014). Understanding the Internet banking adoption: A unified theory of acceptance and use of technology and perceived risk application. *International Journal of Information Management, 34*(1), 1-13.

Mazhelis, O., Luoma, E., & Warma, H. (2012). Defining an internet-of-things ecosystem. In *Internet of Things, Smart Spaces, and Next Generation Networking* (pp. 1-14): Springer.

McPherson, M., Smith-Lovin, L., & Cook, J. M. (2001). Birds of a feather: Homophily in social networks. *Annual review of sociology, 27*(1), 415-444.

Meola, A. (2016). *What is the Internet of Things (IoT)?* Retrieved from http://www.businessinsider.com/internet-of-things-definition?IR=T

Meyers-Levy, J., & Peracchio, L. A. (1995). Understanding the effects of color: How the correspondence between available and required resources affects attitudes. *Journal of consumer research, 22*(2), 121-138.

Midgley, D. F., & Dowling, G. R. (1978). Innovativeness: The concept and its measurement. *Journal of consumer research, 4*(4), 229-242.

Miller, A. (1982). *Computers and Privacy*. Cambridge, MA: Oelgeschlager, Gunn, & Hain Publishers, Inc.

Milne, G. R. (1997). Consumer participation in mailing lists: A field experiment. *Journal of Public Policy & Marketing*, 298-309.

Milne, G. R., & Boza, M.-E. (1999). Trust and concern in consumers' perceptions of marketing information management practices. *Journal of Interactive Marketing, 13*(1), 5-24.

Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing, 18*(3), 15-29.

Milne, G. R., & Gordon, M. E. (1993). Direct mail privacy-efficiency trade-offs within an implied social contract framework. *Journal of Public Policy & Marketing*, 206-215.

Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad Hoc Networks, 10*(7), 1497-1516.

Mishra, D., Angappa Gunasekaran, D. N. D., Gunasekaran, A., Childe, S. J., Papadopoulos, T., Dubey, R., & Wamba, S. (2016). Vision, applications and future challenges of Internet of Things. *Industrial Management & Data Systems, 116*(7), 1331-1355. doi:10.1108/imds-11-2015-0478

Mitchell, V.-W., & Harris, G. (2005). The importance of consumers' perceived risk in retail strategy. *European Journal of Marketing, 39*(7/8), 821-837.

Morwitz, V. G., Greenleaf, E. A., & Johnson, E. J. (1998). Divide and prosper: consumers' reactions to partitioned prices. *Journal of marketing research*, 453-463.

Nakyung, K., & Kim, J. (2015). Domestic smart home market, Low-priced products than high-priced products. Retrieved from http://www.lgeri.com/report/view.do?idx=19046

Narayanan, K. (2017). Addressing The Challenges Facing IoT Adoption. *Microwave Journal I, ,60*(1), 110-118.

Nowak, G. J., & Phelps, J. (1995). Direct marketing and the use of individual-level consumer information: Determining how and when "privacy" matters. *Journal of Direct Marketing, 9*(3), 46-60.

NTIA, N. T. a. I. A. (2002). *A nation online: how Americans are expanding their use of the internet.* Washington D.C.

Nysveen, H., Pedersen, P. E., & Thorbjørnsen, H. (2005). Intentions to use mobile services: Antecedents and cross-service comparisons. *Journal of the Academy of Marketing Science, 33*(3), 330.

O'Brien, J. (2017). The reality of IoT adoption *Big Data Quarterly, 3*(1), 12-16.

Oreg, S. (2003). Resistance to change: developing an individual differences measure. *Journal of applied psychology, 88*(4), 680.

Parasuraman, A. (2000). Technology Readiness Index (TRI) a multiple-item scale to measure readiness to embrace new technologies. *Journal of Service Research, 2*(4), 307-320.

Park, Y., & Chen, J. V. (2007). Acceptance and adoption of the innovative use of smartphone. *Industrial Management & Data Systems, 107*(9), 1349-1365. doi:10.1108/02635570710834009

Peppers, D., Rogers, M., & Dorf, B. (1999). Is your company ready for one-to-one marketing. *Harvard Business Review, 77*(1), 151-160.

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing, 19*(1), 27-41.

Piwek, L., Ellis, D. A., Andrews, S., & Joinson, A. (2016). The rise of consumer health wearables: promises and barriers. *PLoS Medicine, 13*(2), e1001953.

Poo, B., & Dalziel, N. (2016). Consumer Perceptions Towards Radical Innovation: Autonomous Cars. In: British Academy of Management (BAM).

Porter, C. E., & Donthu, N. (2006). Using the technology acceptance model to explain how attitudes determine Internet usage: The role of perceived access barriers and demographics. *Journal of Business Research, 59*(9), 999-1007.

Porter, M. E., & Heppelmann, J. E. (2014). How smart, connected products are transforming competition. *Harvard Business Review, 92*(11), 64-88.

Press, G. (2014). Internet of Things by the numbers: Market estimates and forecasts. *Forbes, Forbes Media, Jersey City, NJ*.

Price, L. L., Feick, L. F., & Guskey, A. (1995). Everyday market helping behavior. *Journal of Public Policy & Marketing*, 255-266.

Ram, S. (1987). A model of innovation resistance. *ACR North American Advances*.

Ram, S. (1989). Successful innovation using strategies to reduce consumer resistance: An empirical test. *Journal of Product Innovation Management, 6*(1), 20-34.

Ram, S., & Sheth, J. N. (1989). Consumer resistance to innovations: the marketing problem and its solutions. *Journal of Consumer Marketing, 6*(2), 5-14.

Rifkin, J. (2014). *The zero marginal cost society: The internet of things, the collaborative commons, and the eclipse of capitalism*: St. Martin's Press.

Risselada, H., Verhoef, P. C., & Bijmolt, T. H. (2014). Dynamic effects of social influence and direct marketing on the adoption of high-technology products. *Journal of Marketing, 78*(2), 52-68.

Rogers, E. M. (1976). New product adoption and diffusion. *Journal of consumer research, 2*(4), 290-301.

Rogers, E. M. (2010). *Diffusion of innovations*: Simon and Schuster.

Rogers, E. M., & Shoemaker, F. F. (1971). Communication of Innovations; A Cross-Cultural Approach.

Rojas-Méndez, J. I., Parasuraman, A., & Papadopoulos, N. (2015). Consumers' Technology Readiness in a Developing Country: The Role of Demographics and Attitudes. In *Marketing in Transition: Scarcity, Globalism, & Sustainability* (pp. 2-2): Springer.

Rojas-Méndez, J. I., Parasuraman, A., & Papadopoulos, N. (2017). Demographics, attitudes, and technology readiness: A cross-cultural analysis and model validation. *Marketing Intelligence & Planning, 35*(1), 18-39.

Rokeach, M. (1973). *The nature of human values*: Free press.

Romani, S., Grappi, S., Bagozzi, R. P., & Barone, A. M. (2018). Domestic food practices: A study of food management behaviors and the role of food preparation planning in reducing waste. *Appetite, 121*, 215-227.

Roselius, T. (1971). Consumer rankings of risk reduction methods. *The Journal of Marketing*, 56-61.

Rosenberg, M., Confessore, N., & Cadwalladr, C. (2018). How Trump Consultants Exploited the Facebook Data of Millions. *The New York Times*

Russo, G., Marsigalia, B., Evangelista, F., Palmaccio, M., & Maggioni, M. (2015). Exploring regulations and scope of the Internet of Things in contemporary companies: a first literature analysis. *Journal of Innovation and Entrepreneurship, 4*(1). doi:10.1186/s13731-015-0025-5

Salami, E. A. (2017). An Analysis of the General Data Protection Regulation (EU) 2016/679.

Sathye, M. (1999). Adoption of Internet banking by Australian consumers: an empirical investigation. *International Journal of Bank Marketing, 17*(7), 324-334. doi:10.1108/02652329910305689

Schwartz, S. H. (1992). Universals in the content and structure of values: Theoretical advances and empirical tests in 20 countries. In *Advances in experimental social psychology* (Vol. 25, pp. 1-65): Elsevier.

Shapiro, C., & Varian, H. R. (1998). *Information rules: a strategic guide to the network economy*: Harvard Business Press.

Sheehan, K. B., & Hoy, M. G. (2000). Dimensions of privacy concern among online consumers. *Journal of Public Policy & Marketing, 19*(1), 62-73.

Sheth, J. N. (1981). Psychology of Innovation Resistance. The less developed concept (LDC) in diffusion research. *Research in Marketing*, 273-282.

Sheth, J. N., & Stellner, W. H. (1979). *Psychology of innovation resistance: The less developed concept (LDC) in diffusion research*: College of Commerce and Business Administration, University of Illinois at Urbana-Champaign Urbana-Champaign, IL.

Shils, E. (1966). Privacy: Its constitution and vicissitudes. *Law and Contemporary Problems, 31*(2), 281-306.

Shin, D.-H. (2010). The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. *Interacting with computers, 22*(5), 428-438.

Shu, Q., Tu, Q., & Wang, K. (2011). The impact of computer self-efficacy and technology dependence on computer-related technostress: A social cognitive theory perspective. *International Journal of Human-Computer Interaction, 27*(10), 923-939.

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks, 76*, 146-164. doi:10.1016/j.comnet.2014.11.008

Smith, D. C., & Park, C. W. (1992). The effects of brand extensions on market share and advertising efficiency. *Journal of marketing research, 29*(3), 296.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: measuring individuals' concerns about organizational practices. *MIS quarterly*, 167-196.

Stone, E. F., Gueutal, H. G., Gardner, D. G., & McClure, S. (1983). A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. *Journal of applied psychology, 68*(3), 459.

Stone, R. N., & Grønhaug, K. (1993). Perceived risk: Further considerations for the marketing discipline. *European Journal of Marketing, 27*(3), 39-50.

Strebel, J., O'Donnell, K., & Myers, J. G. (2004). Exploring the connection between frustration and consumer choice behavior in a dynamic decision environment. *Psychology & Marketing, 21*(12), 1059-1076.

Szmigin, I., & Foxall, G. (1998). Three forms of innovation resistance: the case of retail payment methods. *Technovation, 18*(6), 459-468.

Szmigin, I. T., & Bourne, H. (1999). Electronic cash: a qualitative assessment of its adoption. *International Journal of Bank Marketing, 17*(4), 192-203.

Talke, K., & Heidenreich, S. (2014). How to Overcome Pro-Change Bias: Incorporating Passive and Active Innovation Resistance in Innovation Decision Models. *Journal of Product Innovation Management, 31*(5), 894-907. doi:10.1111/jpim.12130

Tam, E.-C., Hui, K.-L., & Tan, B. (2002). What do they want? Motivating consumers to disclose personal information to internet businesses. *ICIS 2002 Proceedings*, 2.

Teo, T. S., & Pok, S. H. (2003). Adoption of WAP-enabled mobile phones among Internet users. *Omega, 31*(6), 483-498.

Thibaut, J. W., & Walker, L. (1975). *Procedural justice: A psychological analysis*: L. Erlbaum Associates.

Trope, Y., & Liberman, N. (2003). Temporal construal. *Psychological review, 110*(3), 403.

Van de Ven, A. H. (2007). *Engaged scholarship: A guide for organizational and social research*: Oxford University Press

Van den Bulte, C., & Wuyts, S. H. K. (2007). Social networks in marketing. *MSI Relevant Knowledge Series*.

Van Doorn, J., Mende, M., Noble, S. M., Hulland, J., Ostrom, A. L., Grewal, D., & Petersen, J. A. (2017). Domo arigato Mr. Roboto: Emergence of automated social presence in organizational frontlines and customers' service experiences. *Journal of Service Research, 20*(1), 43-58.

Van Heerde, H. J., Mela, C. F., & Manchanda, P. (2004). The dynamic effect of innovation on market structure. *Journal of marketing research, 41*(2), 166-183.

Venkatesh, V., & Davis, F. D. (1996). A model of the antecedents of perceived ease of use: Development and test. *Decision Sciences, 27*(3), 451-481.

Venkatraman, M. P., & Price, L. L. (1990). Differentiating between cognitive and sensory innovativeness: Concepts, measurement, and implications. *Journal of Business Research, 20*(4), 293-315.

Vermesan, O., Friess, P., Guillemin, P., Gusmeroli, S., Sundmaeker, H., Bassi, A., & Doody, P. (2011). Internet of things strategic research roadmap. *Internet of Things-Global Technological and Societal Trends, 1*, 9-52.

Voorhees, C. M., Brady, M. K., & Horowitz, D. M. (2006). A voice from the silent masses: an exploratory and comparative analysis of noncomplainers. *Journal of the Academy of Marketing Science, 34*(4), 514-527.

Voss, K. E., Spangenberg, E. R., & Grohmann, B. (2003). Measuring the hedonic and utilitarian dimensions of consumer attitude. *Journal of marketing research, 40*(3), 310-320.

Wang, G., Dou, W., & Zhou, N. (2008). Consumption attitudes and adoption of new consumer products: a contingency approach. *European Journal of Marketing, 42*(1/2), 238-254. doi:10.1108/03090560810840998

Weber, R. H. (2010). Internet of Things – New security and privacy challenges. *Computer Law & Security Review, 26*(1), 23-30. doi:10.1016/j.clsr.2009.11.008

Weil, M. M., & Rosen, L. D. (1997). *Technostress: Coping with technology@ work@ home@ play*: Wiley New York.

Weinberg, B. D., Milne, G. R., Andonova, Y. G., & Hajjat, F. M. (2015). Internet of Things: Convenience vs. privacy and secrecy. *Business Horizons, 58*(6), 615-624. doi:10.1016/j.bushor.2015.06.005

Wells, J. D., Campbell, D. E., Valacich, J. S., & Featherman, M. (2010). The effect of perceived novelty on the adoption of information technology innovations: a risk/reward perspective. *Decision Sciences, 41*(4), 813-843.

Westin, A. F. (1967). Privacy and freedom, atheneum. *New York, 7*.

Whitmore, A., Agarwal, A., & Da Xu, L. (2014). The Internet of Things—A survey of topics and trends. *Information Systems Frontiers, 17*(2), 261-274. doi:10.1007/s10796-014-9489-2

Wood, S. L., & Moreau, C. P. (2006). From fear to loathing? How emotion influences the evaluation and early use of innovations. *Journal of Marketing, 70*(3), 44-57.

Wuenderlich, N. V., Heinonen, K., Ostrom, A. L., Patricio, L., Sousa, R., Voss, C., & Lemmink, J. G. (2015). "Futurizing" smart service: implications for service researchers and managers. *Journal of Services Marketing, 29*(6/7), 442-447.

Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2008). Examining the formation of individual's privacy concerns: Toward an integrative view. *ICIS 2008 proceedings*, 6.

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.

Xu, S., Fang, X., Chan, S., & Brzezinski, J. (2013). What tasks are suitable for handheld devices? . *Proceedings of HCI international 2003, human computer interaction: Theory and practice, 2*, 333-337.

Xu, Y., Tan, B., & Hui, K.-L. (2003). Consumer trust and online information privacy. *ICIS 2003 Proceedings*, 45.

Yang, Y., Liu, Y., Li, H., & Yu, B. (2015). Understanding perceived risks in mobile payment acceptance. *Industrial Management & Data Systems, 115*(2), 253-269.

Ziegeldorf, J. H., Morchon, O. G., & Wehrle, K. (2014). Privacy in the Internet of Things: threats and challenges. *Security and Communication Networks, 7*(12), 2728-2742. doi:10.1002/sec.795

LIBERA UNIVERSITÀ INTERNAZIONALE DEGLI STUDI SOCIALI

Department of Business and Management

Chair of Consumer Behavior

An exploration of barriers against IoT adoption across segments, and the influence of individual traits

Supervisor
Prof. Simona Romani

Co-Supervisor
Prof. Rumen Pozharliev

Candidate
Tina Marie Berg Toft

Student No.
700491

ACADEMIC YEAR

2017/2018

Acknowledgements

I would first like to thank my thesis supervisor Prof. Simona Romani at LUISS Guido Carli. I have received great support, help, and significant inputs throughout the entire thesis writing process. Her assistance cannot be appreciated enough.

I would also like to thank Ilaria Querci for her active interest and help. I have received great comments throughout the thesis writing process, which I am very grateful for.

Lastly, I am grateful for the managers who participated in my qualitative interviews, you provided great inputs from a practical perspective. I also want to thank everyone who participated in my research, especially people who conducted my first questionnaire as no rewards was given. Your participation provided the basis for this thesis' analyses which could not have been conducted without your participation.

Tina Marie Berg Toft
Roma, Italy
Thursday, June 14, 2018

Table of contents

Chapter 1: Introduction

Internet of Things (IoT) refers to the wireless connection of physical devices to the internet. Objects such as cars, kitchen appliances, and even heart monitors can be connected through IoT (Meola, 2016). A clear definition of IoT does not exist, as the term is continuously evolving. Still there have been many attempts in defining IoT. For instance, Madakam, Ramaswamy, and Tripathi (2015) define IoT as "an open and comprehensive network of intelligent objects that have the capacity to auto-organize, share information, data and resources, reacting and acting in face of situations and changes in the environment" (p.165). Furthermore, Smart Objects are seen as the building blocks to IoT. Smart Objects are referred to as objects that can communicate with other Smart Objects, objects that can make decisions about themselves and their interactions with external entities (López, Ranasinghe, Harrison, & McFarlane, 2011).

According to Hsu and Lin (2016), an increasing number of Smart Objects are connected to the internet. A large number of IoT services have been developed, and the global market for such services is growing rapidly. Despite the promising hype of IoT, adoption rates are low. Accenture's 2016 report, which studied 28 000 consumers in 28 countries, support this notion and state that consumer demand is slow across a number of categories. During 2015 there was only a brief increase in purchase intention (Björnsjö, Viglino, & Lovati, 2016). However, the industry is expecting a huge growth, a great example of this is Future Home. Sigbjorn Groven (personal communication, March 8, 2018), market and sales director at Future Home, a Norwegian Smart Home firm, said in an interview, that Future Home are expecting to sell 20 000 devices of smoke detectors in apartment blocks this year, until 08.03.18 the company had a sold 1650 devices.

Despite the slow growth of IoT, many are predicting that the economic impact of IoT will be huge. Estimates by many well-respected organizations range widely. For instance the Business Insider's report has forecasted that by 2020, 34 billion devices will be connected to the internet, whereas IoT devices will account for 24 billion (Greenough, 2016). Despite the many forecasts of the great growth in the IoT industry, consumers do not adopt these devices in the extent to which is expected. For the IoT industry to reach these forecasts, barriers against IoT must be solved. Before companies can solve barriers against IoT adoption, there needs to be conducted research in this field. This thesis contributes to the literature by further exploring and mapping barriers against IoT adoption. Additionally, it is expected that individual traits may influence a consumer's decision to adopt or not. This will be analyzed through Parasurman's (2000) Technology Readiness Index. Based on this, the following research question is presented: *What are the barriers against IoT adoption? And do individual traits affect the adoption decision?*

Relevance and contribution

Internet of Things has been identified as one of several emerging technologies in IT, and many initiatives are taken to bring IoT to market. IoT is evolving at a rapid pace and the impact it will have is likely to be profound. As a result, there has been more research in this field in recent years, with a boost in 2014 (Russo, Marsigalia, Evangelista, Palmaccio, & Maggioni, 2015). Still, it is a fairly new field of study and there exists several gaps to fill. This thesis aims to make the following contributions to the literature: (1) Study 1 aims to contribute with a further exploration of barriers against IoT adoption and in some cases replication of previous research. (2) This thesis employs a quantitative study, whereas previous research has mostly conducted qualitative studies (Balta-Ozkan, Davidson, Bicket, & Whitmarsh, 2013; Brody & Pureswaran, 2015), as this is a fairly new research topic. (3) Consumer's technology adoption and acceptance have gotten less attention where most researchers study implementation and use in the workplace (Laukkanen, 2016). (4) Few studies have focused on Smart Objects in general, whereas the current literature has focused on one part of the domain, such as smartwatches (Mani & Chouk, 2016), Smart Homes (Nakyung & Kim, 2015), and Smart Cars (Mallat, 2007). (5) To the best of my knowledge, there do not exist any previous scientific research that has tested the present of barriers against segments. This will therefore serve as a major contribution to the literature. (6) Additionally, a more thorough investigation of the privacy and security barrier will be provided, where the aim is to solve the collection problem. This will also contribute to the literature, since little attempt have been made to solve the collection problem before.

Hopefully, this thesis will also be useful to managers. Borgia (2014) points to the fact that IoT will bring tangible benefits to the environment, the society, individuals and business. It will lead to faster productivity growth and an increase of job creation. Additionally, it may lead to the delivering of services in a cheaper and better way and it will give the opportunity to innovate and offer new services and solutions to existing problems. IoT will also create the ability for companies to get closer to their customers and give an understanding of how customers interact with their products.

Outline

In the following sections, there will first be presented a literature review where previous research will be discussed as a basis for which factors that are going to be tested as barriers against IoT adoption. The barriers are divided into situational barriers and individual traits. Situational barriers are again divided into topic specific barriers, referring to barriers found in the IoT and Smart Device literature, and non-topic specific barriers, referring to barriers found in the innovation and technology literature. This thesis consists of two studies, whereas the first study explores barriers against IoT adoption. The second study will investigate one of the barriers found in Study 1 more thoroughly, namely collection which is one sub category of the privacy and security barrier. The analysis and discussion are followed by managerial and theoretical implications of the results. There will further be presented some limitations of the two studies conducted and avenues for future research. Lastly, a conclusion of the thesis will be provided.

Chapter 2: Theoretical Framework

Situational barriers

Situational barriers refer to obstacles directly and personally associated with a consumer. In this thesis, situational barriers consist of topic specific barriers and non-topic specific barriers.

Topic specific barriers

Topic specific barriers refer to barriers that are found in the IoT or Smart Object literature. These will be discussed in the following sections.

Security and privacy

Security refers to the risk that is associated with using a particular application (S. Xu, Fang, Chan, & Brzezinski, 2013). While privacy refers to the control and awareness individuals can have over the collection, processing, and subsequent use of personal information (Ziegeldorf, Morchon, & Wehrle, 2014). Prior research shows that privacy concerns is one major reason for why consumers do not buy IoT devices. Consumers are especially concerned for hacks and data breaches (Acquity Group, 2014; Björnsjö et al., 2016). Studies also show that the greater the perceived control of privacy information is for the consumer, the lower risk he or she feels (Hsu & Lin, 2016).

Dependence

The dependence barrier means that consumers are dependent on certain technology (D L. Hoffman, Novak, & Venkatesh, 2004). Several technologies such as mobile phone, increases consumers dependence (Licoppe & Heurtin, 2001). Mani and Chouk (2016) have analyzed if dependence positively influences consumer resistance to Smart Products. In which they did not find any significant effects, it will therefore be interesting to test if dependence influence adoption of IoT devices.

Intrusiveness

Intrusiveness means someone entering a consumer’s life without permission. Smart Products may be seen as intrusive (Mani & Chouk, 2016). Intrusiveness is found to have a negative effect on consumer adoption of RFID (Boeck, Roy, Durif, & Grégoire, 2011), and mobile location-based services (Hérault & Belvaux, 2014), as well as a positive effect on consumer resistance to Smart Products (Mani & Chouk, 2016).

Price

Price simply refers to the monetary value a consumer thinks a product or service is worth. Balta-Ozkan et al. (2013) suggests that consumers are concerned with cost of installation, repair, maintenance, learning and savings, not just the purchasing cost. Price is found to be a barrier against IoT adoption (Björnsjö et al., 2016), Smart Home product or services purchase (Nakyung & Kim, 2015), and Smart Product resistance (Mani & Chouk, 2016). Previous research also found that many consumers think Smart Devices are too expensive (Björnsjö et al., 2016). Price is often perceived as one of the barriers with highest impact in the innovation literature (Kleijnen, Lee, & Wetzels, 2009; Poo & Dalziel, 2016).

Ease of use

Ease of use refers to consumers perception of how difficult IoT devices are to understand and use (Mallat, 2007). Studies show that most consumers (64%) experience a challenge when using new IoT devices (Björnsjö et al., 2016). Mallat (2007) also found that ease of use contributes to low adoption of a variety of systems, such as Smart Cars and mobile banking. The innovation literature has also discussed the ease of use barrier, especially in relation to the Technology Acceptance Model (TAM) (Davis, 1989). Perceived ease of use also closely parallels to complexity (Hoeffler, 2003; Wood & Moreau, 2006), which has been proven to have a great importance on both adoption of innovations (Arts, Frambach, & Bijmolt, 2011) and resistance of innovation theory (Oreg, 2006; Ram & Sheth, 1989).

Self-efficiency

Compeau and Higgins (1995) defines self-efficiency as “consumers’ perception of their ability to use a technological innovative product” (p. 193). Several researchers have identified a positive link between self-efficacy and the willingness to adopt technology (Davis, Bagozzi, & Warshaw, 1989; Hill, Smith, & Mann, 1986) and consumers adoption of innovations (Park & Chen, 2007), as well as a negative effect on consumer resistance to technological innovations (Ellen, Bearden, & Sharma, 1991; Mani & Chouk, 2016).

Value perception

Value perception refers to consumers perception of the usage of a Smart Object to not be beneficial to them. It is argued that most consumers do not have the need for a IoT device (D L. Hoffman & Novak, 2015). Previous literature states that if consumers do not perceive the usage of a product as beneficial, they are unlikely to use it (Atzori, Iera, & Morabito, 2010). The most successful IoT solutions are powerful in their value proposition, simplicity and reliability (Brody & Pureswaran, 2015). Value perception is also a part of Ram and Sheth’s (1989) functional barriers against innovation resistance. It is demonstrated that a perceived lack of product value leads to a significantly lower chance of a consumer to adopt a technology (Antioco & Kleijnen, 2010). The value perception barrier is found to be a dominant barrier against both service innovation (Laukkanen, 2016) and technological innovation adoption (Kim, Chan, & Gupta, 2007). The value perception barrier also relates to Rogers’s (2010) relative advantage, where perceived relative advantage is found to be positively related to adoption behavior of an innovation (Arts et al., 2011).

Novelty

Novelty refers to consumers’ perception of a radical change in a product concept or an attribute of the product (Ram, 1987). The perception of novelty differs across individuals and types of innovations (Rogers, 2010). Previous research found a significant negative impact of novelty on consumer resistance to Smart Products (Mani & Chouk, 2016; Wells, Campbell, Valacich, & Featherman, 2010).

Non-topic specific barriers

Non-topic specific barriers are barriers found in the innovation or technology literature. These will be discussed in the following section.

Risk

Consumers evaluation of the likelihood of negative outcomes and their awareness of the perceived risk of adopting an innovation (Shoemaker & Shoaf, 1975), establish their perceived risk. Perceived risk is found to have a negative impact on intention to use an innovation (Martins, Oliveira, & Popovič, 2014; Yang, Liu, Li, & Yu, 2015) and resistance against innovations (Kang & Kim, 2009; Sheth & Stellner, 1979). On the other hand, previous research have also found that risk do not explain non-adoption or postponement of internet and mobile banking services (Laukkanen, 2016), as well as new product adoption (DelVecchio & Smith, 2005; Mitchell & Harris, 2005). Therefore, it will be interesting to test if risk is a barrier to IoT adoption. Furthermore, several risk dimensions have been discussed in previous research, such as performance, physical, financial, psychological, social risk (Kaplan, Szybillo, & Jacoby, 1974), and time risk, (Roselius, 1971). Among those, performance risk has been mentioned in relation to IoT, by Assurant Inc (2017). Their study found that reliability, risk and performance was the most frequent concerns for IoT adoption. As much as 61% of consumers who consider to buy a connected technology product would be more likely to buy it if they had longer warranties, on demand tech support or insurance. Piwek, Ellis, Andrews, and Joinson (2016) also points to the fact that there are concerns tied to reliability in using consumer wearables in healthcare. The majority of manufactures do not provide empirical evidence to support the effectiveness of their products. A study, comparing various wearables for tracking physical activity showed large variations in accuracy between different devices (Case, Burwick, Volpp, & Patel, 2015; Lee, 2013).

Network effect

Network effect for technology products is defined by Hall and Khan (2003) as “the value of a technology increases with the number of total users in the network” (p. 6). It is argued that network effect impacts technology adoption, since it effects the expected benefit from a new technology (Hall & Khan, 2003). Prior research has also stated that social influence effects adoption (Godes, 2011). When consumers do not have the assurance of other people in a network also having a given technology, it may lead to anxiety (Hirunyawipada & Paswan, 2006) Risselada, Verhoef, and Bijmolt (2014) further argue that the effect, for a potential adopter, of adding one additional adopter in a network decreases over time. Compatibility is discussed in relation to indirect network effect, and is found to be an important aspect of innovation’s desirability (Arts et al., 2011; Poo & Dalziel, 2016), adoption of innovations (Arts et al., 2011), and adoption of technological innovations (Zeithaml & Gilly, 1987).

Uncertainty

Uncertainty refers to the fact that consumers do not fully understand the functions and consequences of innovations. Also, it takes time before consumers know which technology that sets the standard, which leads to uncertainty (Van Heerde, Mela, & Manchanda, 2004). Uncertainty is widely documented as a barrier to innovation adoption (Castaño, Sujan, Kacker, & Sujan, 2008). uncertainty is found to have a negative effect on internet banking use (Littler & Melanthiou, 2006), adoption of new technology (Hall & Khan, 2003) and adoption of innovation (Van Heerde, Mela, & Manchanda, 2004). Uncertainty has also been discussed briefly in relation to high-tech products, whereas Yang et al. (2015) states that consumers perception of technological uncertainty may affect their purchase decisions. Hong, Nam, and Kim (2017) discuss uncertainty in relation to Smart Homes (topic specific) and states that consumers perception of technological uncertainty can lead to fear, and no adoption. If consumers feel uncertain about Smart Homes technology development, it may lead to concerns about its performance, expenses, and privacy invasion. However, Hong et al. (2017) discusses technology uncertainty as an antecedent of perceived risk, this thesis on the other hand identifies risk and uncertainty as two separate concepts.

Knowledge

The knowledge barrier refers to what consumers know about different Smart Devices. Previous research states that when consumers' knowledge of a product class is low, the level of perceived risk associated with a purchase is high (D. C. Smith & Park, 1992). Consumer's knowledge about Smart Devices is therefore important. On the other hand, consumers can also acquire too much knowledge and information about products. (Herbig & Day, 1992; Herbig & Kramer, 1994; Hirschman, 1987). The decision to adopt a new technology is related to the amount of knowledge consumers have (Rogers, 2010).

Individual traits

Individual traits are operationalized to measure consumers readiness to technology adoption, and will be analyzed as a moderator, effecting the independent variable-dependent variable relationship (Baron & Kenny, 1986). To analyze this moderating effect the Technology Readiness Index (TRI) developed by Parasuraman (2000) is used. According to Parasuraman (2000) the TRI index refers to "peoples' tendency to embrace and use new technologies for accomplishing goals in home life and at work" (p. 308). The TRI model consists of four distinct constructs, being: (1) *Optimism* which means that consumers have a positive view of technology. (2) *Innovativeness* which relates to consumers tending to be technological pioneers. (3) *Discomfort* which expresses a perceived lack of control over technological and a feeling of being overwhelmed by the technology. (4) *Insecurity* concerns consumers' distrusts of technological and skepticism about its ability to work properly. Optimism and innovativeness are drivers of technology readiness, while discomfort and insecurity are inhibitors of technology readiness (Parasuraman, 2000).

Chapter 3: Study 1

Study 1 explores barriers against IoT adoption across segments and analyses the influence of individual traits on barriers against IoT adoption.

Methodology

To explore barriers against IoT adoption in a quantitative and organized manner, descriptive design is used. The aim is therefore to detect association between the variables being investigated, namely, topic specific and non-topic specific barriers, adoption and individual traits. More specific, a questionnaire is developed to be able to analyze the perceptions of many consumers thoughts regarding Smart Devices. The questionnaire follows a normal and logical structure where respondents are provided with some general information at the beginning of the survey, thereafter the respondents answers questions related to the different barriers (discussed in the literature review). Furthermore, respondents are asked to answer questions related to individual traits, and lastly some demographic questions are given (Malhotra, 2009). Every scale included in the questionnaire – except from the demographic questions – are measured on a 7-point Likert scale, labeled strongly disagree to strongly agree. To minimize missing values, each question in the survey has "force response", meaning that all questions in the survey need to be answered for the respondents to complete the survey. The question wording has also been evaluated to avoid leading and biasing questions. Ordinary and unambiguous words have been used, and issues have been defined, such as the definition of Smart Devices in the beginning of the survey (Malhotra, 2009). Some questions are reversed meaning that they have a different direction than the rest of the questions in the survey. When the reversed scale has a high score (7) it entails a bad thing, and not a good thing.

Sampling

The target population for this thesis is people above 18 years from the general population. The population is not restricted to any geographical area as there may be differences in barriers across countries. There might be some differences in countries, such as the accessibility of Smart Devices etc. These potential differences are not considered as influential since a convenience sample technique is used, and therefore the respondents would most likely be people from the developed world. The minimum age is 18, since all the respondents need to be legal. Since the sample is drawn from the population, the sample will be: the general population above 18 years. The sample is targeted online, mainly through Facebook, but also on forums and survey swap websites. The survey was distributed from 23.03.2018 to 12.04.2018. During the same period (17.03.2018) the Facebook-Cambridge Analytica data scandal was extensively discussed in media. This might have influenced the results in this thesis as the study addresses privacy and security barriers. However, it is expected that some consumers have concern over privacy and security in general, and that the Facebook-Cambridge Analytica data scandal have not influenced every respondent.

The sampling method used in Study 1 is a non-probability sampling method, meaning that the selection of elements from the population is non-random, rather the selection relay on the personal judgment of the researcher. From several types of non-probability sample techniques, convenience sampling is chosen, which attempts to obtain a sample of convenient elements, and the selection of sampling units is left primarily to the researcher (Malhotra, 2009). This sampling method is chosen because of limited resources available, such as time and budget. Several qualitative methods to determine sample size have been used. These are, nature of analyses, number of variables, completion rates, and resource constraints (Malhotra, 2009). In line with previous research (Littler & Melanthiou, 2006; Ram, 1989), the sample size of this thesis is 150 respondents. Initially, the aim was to collect 200 respondents, however as the survey was quite long (15 minutes), and because limited time and budget was available, this proved itself to be difficult.

Reliability and validity

According to Malhotra (2009), researchers have the ethical responsibility to use scales that have reasonable reliability, validity and generalizability. Accordingly, this thesis will include reliability and validity checks of the studies performed in both Study 1 and Study 2. Several methods exist to asses' reliability, this thesis uses internal consistency and Cronbach alpha to test the scale's reliability. Additionally, where a scale only consists of two questions a correlation study will be conducted to check for the scale's reliability. To asses' validity in Study 1, exploratory factor analyses are conducted on the scales which have been changed from the source they were found.

Analyses

After making the dataset ready, some preliminary analyses were performed, namely *Cronbach alpha* and *correlation* studies for reliability and *factor analyses* for validity checks. Further, some *descriptive statistics* are conducted to gain knowledge about the respondents. The descriptive analyses were mainly conducted on demographic questions included in the survey. The main analyses in Study 1 were a *cluster analysis*, performed to classify objects into relatively homogenous groups. A tandem method combining hierarchical and non-hierarchical clustering analysis was performed. K-means was used as the non- hierarchical clustering method to create an improved solution. Before conducting the analysis, all variables were transformed to aggregated variables, meaning average scores for every scale and subscale for each of the 150 responses, these were used in the cluster analysis (Malhotra, 2009).

Results

Preliminary analyses showed that novelty and value perception consists of two factors each instead of one. This is not surprising, especially for novelty as this scale was merged with the uncertainty scale. Since two factors were found for novelty and value, new scales were developed (Malhotra, 2009). In terms of reliability checks, Cronbach alpha and correlation tests were conducted for evert scale included in the survey. In some cases, items were deleted from scales to increase the reliability, afterword every scale had a satisfactory alpha. As for the correlational test, every scale had significant and high correlation coefficients.

Conducting cluster analyses – both hierarchical and non-hierarchal – consisting of all metric variables needed to be performed multiple times as the results always showed a cluster solution where one cluster had very few respondents and the rest of the clusters consisted of several respondents. This result was consistent through any number of cluster solutions that were tested. Further, doing the same analysis without the dependent variables (adoption, measured through purchase intention and WOM intention) gave the same result. A more thorough analysis of the descriptive statistics showed the evidence of a special sample, as respondents are very similar in terms of knowledge, they have high purchase intention, high positive WOM intention in general, and own many Smart Devices. This made the clustering difficult, as it was hard to detect differences between segments. Conducting cluster analysis with only some of the variables, solved the problem with the special sample. As Study 1 is a preliminary study, used in an explorational way, it was decided to analyze the special sample instead of collecting new data to be able to proceed to the second study.

Because of the special sample, the final cluster analysis was conducted with only some of the scales measuring barriers. These are: privacy concern, collection, unauthorized secondary use, and improper access, as well as intrusiveness, dependency, price, novelty 1, novelty 2, value perception 1, and value perception 2. The variables included in the analysis are viewed as the most important barriers against IoT adoption. The hierarchical clustering method conducted on the 11 barriers, gave a 2-cluster solution. This is based on the agglomeration schedule and the dendrogram. Therefore, the non- hierarchical, K-means technique was used to develop a 2-cluster solution. The K-means clustering analysis supported the hierarchical clustering method, and the final cluster solution is therefore two. The 15 variables not i in the cluster analysis will serve as descriptive variables, still explaining differences between segments. To asses' the descriptive variables a *one-way ANOVA analysis* is conducted, based on the analysis' robust design, and because it decreases random variability. A post hoc test (Turkey) is included, to be able to examine which levels are responsible for any factor effect (Janssens, De Pelsmacker, & Van Kenhove, 2008).

Discussion

It is important for companies to understand why the expected growth of IoT has not happened, to be able to facilitate growth. The aim of Study 1 was therefore to acquire an understanding of possible consumer barriers against IoT adoption. There was not found any evidence for a moderating effect of individual traits. However, there has been found evidence for some barriers, and an important contribution to the literature was to examine barriers across clusters. A description of the two segments created is therefore given in the following part.

Cluster 1: Smart Device Likers

The first segment is called Smart Device Likers as they have great knowledge about Smart Devices, they own many Smart devices, they are not insecure when dealing with these devices, and they do not associate a lot of risk with Smart Devices. However, these consumers have privacy and security concerns in general, are concerned for collection, unauthorized secondary use, and improper access of personal information. In addition, dependency and price is found to be IoT adoption barriers to this segment. These findings are in line with previous research (Hsu & Lin, 2016; Licoppe & Heurtin, 2001; Mani & Chouk, 2016; Nakyung & Kim, 2015). This means that Smart Device Likers purchase a lot of Smart Devices and are knowledgeable about these products, however, they have more concerns regarding Smart Devices and privacy compared to cluster 2. Other factors that characterize Smart Device Likers are that these consumers are older than cluster 2 and some of these are employees, compared to cluster 2 where most consumers are students.

Cluster 2: Smart Device Lovers

The second segment is called Smart Device Lovers as they think of Smart Devices as very advantageous and attractive. These consumers have a high WOM intention and high purchase intention, meaning that they simply love Smart Devices. Furthermore, they do not have problems related to the use of devices and they own a lot of Smart Devices. Compared to cluster 1, cluster 2 consist of many young consumers, which are students. While cluster 1 is concerned for every aspect of the privacy and security barrier, cluster 2 are only concerned for unauthorized secondary use and improper access of personal information.

Interestingly these findings show that only some consumers have concerns for collection of personal information while other consumers do not find this to be a barrier against IoT adoption. Let us call this the collection problem, referring to why some consumers allow companies to collect their personal information while other consumers do not. Study 2 looks more deeply into this collection problem, and the aim of Study 2 is to solve the collection problem.

Chapter 4: Study 2

Study 2 tries to solve the collection problem by examining if benefits to consumers will influence collection of consumers personal information. Additionally, it is being tested if consumers having control (high/low) over their personal information will moderate the effect of benefit on collection. In terms of benefit, it is examined if consumers are more willing to disclose personal information if they receive self-benefit compared to others-benefit. Control of personal information is measured as high, or low control. It is assumed that self-benefit will affect collection of personal information in a positive way, and that self-benefit also will be better than others-benefit. Further, it is predicted that high control is better than low control, and that the moderating effect of control positively affect the benefit-collection relationship. In the following, collection, benefit and control is discussed respectively. Study 2 aims to test three hypotheses, presented in the discussion below.

Collection

Collection is referred to as the degree to which a person is concerned about the amount of personal information that is being possessed by others compared to the value of benefits received (Malhotra, Kim, & Agarwal, 2004). Previous litterature presents a perception of there being too much data collected in the society (Miller, 1982; H. J. Smith, Milberg, & Burke, 1996). It is also stated that consumers have observed the great quantities of personal data that are being collected, which they often resent (H. J. Smith et al., 1996). More specifically, previous research has found that the majority (85,6%) of consumers want to limit the amount of personal information collected by marketers (Phelps, Nowak, & Ferrell, 2000). Previous literature also points to the fact that some consumers actually avoid the use of services which requires collection of personal information (Harris & Westin, 1990; Milne & Gordon, 1993).

Benefit

Prior research states that providing the right rewards may induce consumers do disclose personal information (Tam, Hui, & Tan, 2002). Building on this, benefit is included in this thesis as a variable that could influence collection of personal information. In this thesis, benefit involves consumers giving personal information to a firm, and in return the consumers get a benefit based on the personal information they disclosed. Following Fisher, Vandenbosch, and Antia (2008), there is made a distinction between self-benefit and others-benefit. This thesis will examine if consumers share their personal information for self-interest or altruism (others-benefit), this is possible as benefit is divided into self and others. Others-benefit may be seen as an altruistic behavior, meaning that consumers act unselfish to enhance welfare of others (Price, Feick, & Guskey, 1995). While self-benefit is a type of personalization, which is extensively discussed in previous research. Personalization is defined by Chellappa and Sin (2005) as "the ability to proactively tailor products and product purchasing experiences to tastes of individual consumers based upon their personal and preference information" (p. 181). It is expected that benefit will influence consumers to disclose their personal information to companies, as the right reward may induce consumers to disclose personal information (Tam et al., 2002). Furthermore, intrinsic reward (e.g. altruism) has been found to be useful to induce information disclosure (Tam et al., 2002), and personalization (self-benefit) can lead to positive customer response. The following hypothesis is therefore developed: *H1: Benefit has a positive effect on collection*

Control

A common thread throughout the literature is to explain control as, consumers having control over disclosure of personal information (Johnson, 1974; Shils, 1966; Westin, 1967). Control is often exercised through approval, modification, and opportunity to exit. Additionally, consumers should be allowed to add, delete, and modify the information in the organization's database (Malhotra et al., 2004). The newly implemented General Data Protection Regulation (GDPR) includes some of these aspects (Salami, 2017). Previous research has found that 85% of adults believe that controlling access to their personal information is very important (Bélanger & Crossler, 2011). In line with previous research high control is predicted to be better than low control on collection of personal information (Ziegeldorf et al., 2014). This implies that it is also expected that control will influence collection of consumers personal information, therefore the following hypothesis is developed: *H2: Control has a positive effect on collection*

It is expected that control will change the relationship between benefit and collection in a positive way, meaning that control is a moderator. This means that the effect of benefit (IV) on collection (DV) differs at different values (high/low) of control (moderator). The following hypothesis is therefore developed: *H3: The positive effect of benefit on collection is positively moderated by control*

Methodology

The research type used in Study 2 is a causal design, which can infer causal relationship between the independent and dependent variables. This thesis examines if benefit (self/others), and level of control (high/low) is the cause and if collection is the effect of the collection problem. As Study 2 tests the effect of two independent variables on one dependent variable, a factorial design is used. More specific, a 2 x 2 between subject factorial design is used to test for interaction between the two independent variables (benefit and control). The main method of causal research is experimentation, which is also used in this thesis. More specifically an experimentation survey is used. An experimentation survey is classified as a laboratory experiment rather than a field experiment. A laboratory experiment is an artificial setting for experimentation in which the researcher constructs the desired conditions (Malhotra, 2009). The experimentation survey used in this thesis consisted of scenarios, were respondents were randomly assigned to one of four scenarios. Every scenario consisted of the same general information, explaining the context that were used, this general information stated that the training center respondents normally train at had developed an app. Respondents were asked to give their personal information to the fictive training center through the app. A fictive training center was used so people's judgements and perceptions of a brand would not affect the participants answers. After, respondents in the self-benefit condition learned that they could receive personalized training and nutrition plans. Respondents in the others-benefit condition learned that other members at the training center received tutorials regarding new training methods if the participant disclosed his/her personal information. In combination with the benefit manipulation respondents also received either low or high control over their personal information. Low control means that the training center will manage the personal information and the participants will be unaware of what it will be used for. While high control means that participants could decide which information the training center receives, how it is used, and it is easy to change the privacy settings. After being exposed to the scenarios, respondents were asked the same questions regarding benefit, control, collection, improper access, intention to use, WOM intention, and demographic questions. The manipulations were also pretested to test if the manipulations were perceived in the correct way. Amazon Mechanical Turk (Mturk) was used to gather the data both from the pretests and experiment, as this data collection method is perceived to be satisfactory in terms of data quality (Buhrmester, Kwang, & Gosling, 2011; Goodman, Cryder, & Cheema, 2013).

Sampling

The target population for Study 2 is: people above 18 from general the population. The population is not restricted to any geographical areas as there is a wish to generalize the study to more than one country. However, since the data is collected through MTurk, which is from USA, most people answering the experimental survey is from USA. Since the sample is drawn from the population, the sample will be: the general population above 18 years. Furthermore, when determining the sample size, a great effort was made to find the balance between an inadequate and excessive number of respondents. There was not used any quantitative methods to determine the sample size, however multiple qualitative methods have been used. These are, nature of analyses, number of variables, completion rates, and resource constraints (Malhotra, 2009). In line with these methods of sample size determination, 269 respondents were collected, meaning approximately 67 respondents in each of the four groups.

Reliability and validity

Similar to Study 1, reliability and validly tests have also been conducted in Study 2. To measure reliability, internal consistency and Cronbach alpha analysis are being conducted for the five scales used in the experiment. To asses validity, exploratory factor analysis are being conducted on the scales that are changed, in the experiment the only variable that is changed is collection (Malhotra, 2009).

Analyses

After making the dataset ready and performing preliminary analysis, a univariate linear regression is performed to examine if there exist any main or interaction effects. In this thesis the difference in average collection of personal information between self and others benefit, and between high and low control is tested. Further, it is also tested if this difference is statistical meaningful. As the data's measurement level is metric and the sample consist of four independent groups, the univariate technique one-way ANOVA is conducted (Malhotra, 2009). Furthermore, to assess the interaction effect more closely two *independent sample t-tests* are conducted, one for control on collection and one t-test for benefit on collection. The aim of this analysis is to assess the contracts of the interaction effect. The sample will be split based on control, to be able to verify the different effect of benefit on collection under each specific control condition (high/low).

Results and discussion

First, the pretest measuring the control manipulations show that there is a significant difference between low and high control, $F(1,39) = 8.48$, $p = .006$. Second, the pretest measuring the benefit manipulations show that others-benefit is perceived different from self-benefit and the control group, $F(2,36) = 3.77$, $p = .033$, and that self-benefit is perceived different from others-benefit and the control group, $F(2,36) = 3.83$, $p = .031$. Results from the preliminary analysis, show that the reliability of the scales used in the experiment is satisfactory, therefore no items were deleted and summated scales were calculated. The control group in the benefit condition is deleted before further analysis is conducted.

Results from the univariate linear regression show a significant main effect of benefit on collection, $F(1,265) = 13.72$, $p < .001$, indicating a significant difference between self-benefit ($M = 4.38$, $SD = 1.78$) and others-benefit ($M = 5.10$, $SD = 1.53$). This means that if consumers receive self-benefit from a company, they would be more likely to share their personal information with that company. This is in line with prior research, which states that providing consumers with valuable benefits to obtain personal information is consistent with the benefit congruency principle of marketing (Chandon, Wansink, & Laurent, 2000; Y. Xu, Tan, & Hui, 2003). Furthermore, the main effect of control on collection was not significant, $F(1,265) = .57$, $p = .45$, the reason for this may be that respondents expresses their attitudes toward high or low control which may not reflect their actual behavior. More important than the main effect, is the interaction effect. The results show that the interaction effect between control and benefit is moderately significant, $F(1,265) = 2.99$, $p = .085$. This means that the effect of benefit (independent variable) on collection (dependent variable) is different for different categories of control (independent variable) (Malhotra, 2009). The moderately significant interaction effect is confirmed graphically, as the two lines in the “estimated marginal means” figure are not parallel to each other (Janssens et al., 2008). These results mean that if consumers have low control over their personal information they will need self-benefits to justify the collection.

To assess the contracts of the interaction effect, an independent sample t-test analysis is conducted. The sample is split based on control (moderator variable), therefore the different effects of benefit on collection can be verified under each specific control condition (high/low). Under low control of personal information, the collection scores differ in case of self-benefit versus others-benefit. Self-benefit ($M = 4.28$, $SD = 1.85$) allows for more collection of personal information than others-benefit ($M = 5.38$, $SD = 1.27$), $t(115.77) = -3.85$, $p < .001$. This means that if consumers have low control over their personal information companies will need to provide self-benefits to the consumers in order to justify the collection. Assessing high control secondly, there was not found a significant difference in collection of personal information between self-benefit ($M = 4.48$, $SD = 1.73$) and others-benefit ($M = 4.88$, $SD = 1.67$), $t(141) = -1.40$, $p = .163$.

Implications

Overall the results provide important insights in consumers barriers against IoT adoption. This serves as a scientific contribution to previous literature, even when the sample used in Study 1 was a special sample. Additionally, applying quantitative research in the exploration of barriers against IoT adoption, is a major contribution. An understanding of barriers for adoption is important, as companies need to understand the problem before they can solve it. Growth in the IoT industry will create increased revenues for companies. As Mazhelis, Luoma, and Warma (2012) stated, IoT represent a tremendous opportunity for various types of firms. Furthermore, price was only found to be a barrier in cluster 1 and not cluster 2. Managers can therefore implement price discrimination and offer lower prices to cluster 1, but keep a higher price for cluster 2. Alternatively, managers can keep a high price but offer better value to ignite growth. This is in line with the recommendations given in Accenture’s 2016 report (Björnsjö et al., 2016). This thesis also contributes with a suggestion of how to solve the collection problem. This is important for managers as it is suggested that firms can use customers information to generate productivity and profit gains that are five to six percent higher than competitors (Biesdorf, Court, & Willmott, 2013). The main finding in Study 2 is that companies need to provide consumers with self-benefit when they have low control, to justify the collection of personal information. However, this does not mean that companies can prevent consumers of having control and use consumers personal information as wanted as long as the company provide consumers with self-benefit. In fact, companies that commit to authentic data privacy practices in long-term will experience positive performance including customer loyalty and engagement (Martin & Murphy, 2017).

Limitations

Due to the data collection method used in Study 1, the sample is small and homogeneous, which have been referred to as a special sample in this thesis. Due to this special sample, the generalizability of the results is most likely limited. The scenarios used in Study 2 could have been developed better so the differences between the scenarios would have been perceived stronger. This lead to the need to delete the control condition for benefit in the analyses, as this manipulation was not perceived as natural.

Future research

Future research could examine if there exist other barriers against IoT adoption, such as awareness of Smart Devices. Alternatively, researchers could replicate Study 1 with a better sample. There is also a need to examine consumers actual behavior in relation to barriers. Future research could also analyze the influence of individual traits on barriers, which could give a better understanding of why barriers differ across segments. Lastly, researchers could try to solve other barriers against IoT adoption, such as dependency. This could be a major contribution to the literature, which also would be very relevant for companies.

Chapter 5: Conclusion

In this thesis Study 1 contributes to a better understanding of factors that explain why consumers do not adopt IoT devices. An exploration of barriers from the IoT literature (topic-specific barriers) and the innovation literature (non-topic specific barriers) was introduced and tested across segments. Findings of Study 1 show – despite a special sample – that price, dependency and all sub categories of privacy and security are barriers for the first cluster named Smart Device Likers. Further, only improper access and unauthorized secondary use was found to be barriers that hinder IoT adoption in the second cluster, named Smart Device Lovers. Detecting these barriers against IoT adoption serves as an important contribution to the existing literature. Study 2 aims to solve the collection problem. The findings show that the collection problem can be solved by providing self-benefits to consumers when they have low control. The interaction effect which indicates these findings is moderately significant, however, these findings indicates some interesting results. The understanding of how to influence more consumers to disclose personal information is a contribution to previous literature.

References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*(6221), 509-514.

Acquity Group. (2014). *Acquity Group 2014 Internet of Things study, part of Accenture Interactive*. Retrieved from https://acquitygroup.wordpress.com/2014/08/21/acquity-group-2014-internet-of-things-study/

Agarwal, S., & Teas, R. K. (2001). Perceived value: mediating role of perceived risk. *Journal of Marketing theory and Practice, 9*(4), 1-14.

Ajzen, I., & Fishbein, M. (1980). Understanding attitudes and predicting social behaviour. *Michigan: Prentice-Hall*.

Alba, J., Lynch, J., Weitz, B., Janiszewski, C., Lutz, R., Sawyer, A., & Wood, S. (1997). Interactive home shopping: consumer, retailer, and manufacturer incentives to participate in electronic marketplaces. *The Journal of Marketing*, 38-53.

Altman, I. (1975). The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding.

Andersson, P., & Heinonen, K. (2002). Acceptance of mobile services-insights from the Swedish market for mobile telephony. *Working Paper Series in Business Administration, 2002*(16).

Antioco, M., & Kleijnen, M. (2010). Consumer adoption of technological innovations. *European Journal of Marketing, 44*(11/12), 1700-1724. doi:10.1108/03090561011079846

Arnett, D. B., German, S. D., & Hunt, S. D. (2003). The identity salience model of relationship marketing success: The case of nonprofit marketing. *Journal of Marketing, 67*(2), 89-105.

Arts, J. W. C., Frambach, R. T., & Bijmolt, T. H. A. (2011). Generalizations on consumer innovation adoption: A meta-analysis on drivers of intention and behavior. *International Journal of Research in Marketing, 28*(2), 134-144. doi:10.1016/j.ijresmar.2010.11.002

Assurant Inc. (2017). *The Connected Future. Navigating promise and risk*. Retrieved from https://www.assurant.com/documents/assurant/publications/aiz-news-connectedfuturereportbrief-2017-01-05.pdf?sfvrsn=8

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks, 54*(15), 2787-2805. doi:10.1016/j.comnet.2010.05.010

Balta-Ozkan, N., Davidson, R., Bicket, M., & Whitmarsh, L. (2013). Social barriers to the adoption of smart homes. *Energy Policy, 63*, 363-374.

Bandyopadhyay, D., & Sen, J. (2011). Internet of things: Applications and challenges in technology and standardization. *Wireless Personal Communications, 58*(1), 49-69.

Barnett, H. G. (1953). *Innovation: the basis of cultural change*. New York, US: McGraw-Hill.

Baron, R. M., & Kenny, D. A. (1986). The moderator–mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. *Journal of personality and social psychology, 51*(6), 1173.

Bearden, W. O., & Shimp, T. A. (1982). The use of extrinsic cues to facilitate product adoption. *Journal of marketing research*, 229-239.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in information systems. *MIS quarterly, 35*(4), 1017-1042.

Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. *The Journal of Strategic Information Systems, 11*(3-4), 245-270.

Biesdorf, S., Court, D., & Willmott, P. (2013). Big data: What's your plan. *Mckinsey Quarterly 2013*.

Björnsjö, A., Viglino, M., & Lovati, G. (2016). *Accenture Igniting Growth in Consumer Technology. Digital Consumer Survey 2016*. Retrieved from https://www.accenture.com/_acnmedia/PDF-3/Accenture-Igniting-Growth-in-Consumer-Technology.pdf

Blau, P. (1964). *Exchange and power in social life*. New York John Wiley & Sons.

Boeck, H., Roy, J., Durif, F., & Grégoire, M. (2011). The effect of perceived intrusion on consumers' attitude towards using an RFID-based marketing program. *Procedia Computer Science, 5*, 841-848.

Borgia, E. (2014). The Internet of Things vision: Key features, applications and open issues. *Computer Communications, 54*, 1-31. doi:10.1016/j.comcom.2014.09.008

Bradley, J., Barbier, J., & Handler, D. (2013). *Embracing the Internet of Everything To Capture Your Share of $14.4 Trillion* Retrieved from https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoE_Economy.pdf

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced confidences: Privacy and the control paradox. *Social Psychological and Personality Science, 4*(3), 340-347.

Brody, P., & Pureswaran, V. (2015). The next digital gold rush: how the internet of things will create liquid, transparent markets. *Strategy & Leadership, 43*(1), 36-41.

Buhrmester, M., Kwang, T., & Gosling, S. D. (2011). Amazon's Mechanical Turk: A new source of inexpensive, yet high-quality, data? *Perspectives on psychological science, 6*(1), 3-5.

Campbell, M. C., & Goodstein, R. C. (2001). The moderating effect of perceived risk on consumers' evaluations of product incongruity: Preference for the norm. *Journal of consumer research, 28*(3), 439-449.

Castaño, R., Sujan, M., Kacker, M., & Sujan, H. (2008). Managing consumer uncertainty in the adoption of new products: Temporal distance and mental simulation. *Journal of marketing research, 45*(3), 320-336.

Castellion, G., & Markham, S. K. (2013). Perspective: new product failure rates: influence of argumentum ad populum and self interest. *Journal of Product Innovation Management, 30*(5), 976-979.

Cavoukian, A., Polonetsky, J., & Wolf, C. (2010). Smartprivacy for the smart grid: embedding privacy into the design of electricity conservation. *Identity in the Information Society, 3*(2), 275-294.

Cespedes, F. V., & Smith, H. J. (1993). Database marketing: New rules for policy and practice. *Sloan Management Review, 34*(4), 7.

Chandon, P., Wansink, B., & Laurent, G. (2000). A benefit congruency framework of sales promotion effectiveness. *Journal of Marketing, 64*(4), 65-81.

Chang, M. K., & Cheung, W. (2001). Determinants of the intention to use Internet/WWW at work: a confirmatory study. *Information & Management, 39*(1), 1-14.

Chang, Y., Dong, X., & Sun, W. (2014). Influence of characteristics of the Internet of Things on consumer purchase intention. *Social Behavior and Personality: an international journal, 42*(2), 321-330.

Charlton, J. P. (2002). A factor analytic investigation of computer 'addiction'and engagement. *British journal of psychology, 93*(3), 329-344.

Chellappa, R. K., & Sin, R. G. (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information technology and management, 6*(2-3), 181-202.

Chui, M., Markus, L., & Roger, R. (2010). The Internet of things. *McKinsey Quarterly*.

Cohen, R. L. (1987). Distributive justice: Theory and research. *Social justice research, 1*(1), 19-40.

Compeau, D. R., & Higgins, C. A. (1995). Computer self-efficacy: Development of a measure and initial test. *MIS quarterly*, 189-211.

Conner, K. R. (1995). Obtaining strategic advantage from being imitated: When can encouraging "clones" pay? *Management Science, 41*(2), 209-225.

Cox, D., & Cox, A. D. (2002). Beyond first impressions: The effects of repeated exposure on consumer liking of visually complex and simple product designs. *Journal of the Academy of Marketing Science, 30*(2), 119-130.

Cox, D. S., & Cox, A. D. (1988). What does familiarity breed? Complexity as a moderator of repetition effects in advertisement evaluation. *Journal of consumer research, 15*(1), 111-116.

Cranor, L. F., Reagle, J., & Ackerman, M. S. (2000). Beyond concern: Understanding net users' attitudes about online privacy. *The Internet upheaval: raising questions, seeking answers in communications policy*, 47-70.

Culnan, M. J. (1993). " How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use. *MIS quarterly*, 341-363.

Culnan, M. J. (1995). Consumer awareness of name removal procedures: Implications for direct marketing. *Journal of Interactive Marketing, 9*(2), 10-19.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly,* 319-340.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: a comparison of two theoretical models. *Management Science, 35*(8), 982-1003.

DelVecchio, D., & Smith, D. C. (2005). Brand-extension price premiums: the effects of perceived fit and extension product category risk. *Journal of the Academy of Marketing Science, 33*(2), 184-196.

Desarnauts, B. (2015, November 30). Dissatisfaction Learnings. First insights into unsatisfied Apple Watch owners. Retrieved from https://medium.com/wristly-thoughts/dissatisfaction-learnings-48c26d564bc1

Dhir, A., Chen, S., & Nieminen, M. (2015). Predicting adolescent Internet addiction: The roles of demographics, technology accessibility, unwillingness to communicate and sought Internet gratifications. *Computers in Human Behavior, 51*, 24-33.

Dholakia, U. M. (2001). A motivational process model of product involvement and consumer risk perception. *European Journal of Marketing, 35*(11/12), 1340-1362.

Dimofte, C. V., Forehand, M. R., & Deshpande, R. (2003). Ad schema incongruity as elicitor of ethnic self-awareness and differential advertising response. *Journal of Advertising, 32*(4), 7-17.

Dowling, G. R., & Staelin, R. (1994). A model of perceived risk and intended risk-handling activity. *Journal of consumer research, 21*(1), 119-134.

Easterby-Smith, M., Thorpe, R., & Jackson, P. R. (2012). Management research. *Sage*, pp. 95-97.

Edwards, S. M., Li, H., & Lee, J.-H. (2002). Forced exposure and psychological reactance: Antecedents and consequences of the perceived intrusiveness of pop-up ads. *Journal of Advertising*, *31*(3), 83-95.

Ellen, P. S., Bearden, W. O., & Sharma, S. (1991). Resistance to technological innovations: an examination of the role of self-efficacy and performance satisfaction. *Journal of the Academy of Marketing Science, 19*(4), 297-307.

Engel, J. F., Kegerreis, R. J., & Blackwell, R. D. (1969). Word-of-mouth communication by the innovator. *The Journal of Marketing*, 15-19.

Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-services adoption: a perceived risk facets perspective. *International journal of human-computer studies, 59*(4), 451-474.

Fenech, T. (2002). Exploratory study into wireless application protocol shopping. *International Journal of Retail & Distribution Management, 30*(10), 482-497.

Ferreira, J. B., da Rocha, A., & da Silva, J. F. (2014). Impacts of technology readiness on emotions and cognition in Brazil. *Journal of Business Research, 67*(5), 865-873.

Fisher, R. J., Vandenbosch, M., & Antia, K. D. (2008). An empathy-helping perspective on consumers' responses to fund-raising appeals. *Journal of consumer research, 35*(3), 519-531.

Garcia, R., & Atkin, T. (2006). Coopetition for the diffusion of resistant innovations: a case study in the global wine industry using an agent-based model. *Agent-Based Models of Market Dynamics and Consumer Behaviour, Institute of Advanced Studies, University of Surrey, Guildford*.

Garcia, R., Bardhi, F., & Friedrich, C. (2007). Overcoming consumer resistance to innovation. *MIT Sloan management review, 48*(4), 82.

Gartner, I. (2014). *"Gartner Says 4.9 Billion Connected 'Things' Will Be in Use in 2015; In 2020, 25 Billion Connected 'Things' Will Be in Use," Press Release, Gartner*. Retrieved from http://www.gartner.com/newsroom/id/2905717

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS quarterly, 27*(1), 51-90.

Gilliland, S. W. (1993). The perceived fairness of selection systems: An organizational justice perspective. *Academy of management review, 18*(4), 694-734.

Godes, D. (2011). Commentary—Invited Comment on "Opinion Leadership and Social Contagion in New Product Diffusion". *Marketing Science, 30*(2), 224-229.

Goodman, J. K., Cryder, C. E., & Cheema, A. (2013). Data collection in a flat world: The strengths and weaknesses of Mechanical Turk samples. *Journal of Behavioral Decision Making, 26*(3), 213-224.

Goodwin, C. (1991). Privacy: Recognition of a consumer right. *Journal of Public Policy & Marketing*, 149-166.

GreenJinn. (2018). GreenJinn.com. Retrieved from https://www.greenjinn.com/

Greenough, J. (2016). *How the 'Internet of Things' will impact consumers, businesses, and governments in 2016 and beyond. Business insider*. Retrieved from http://www.businessinsider.com/how-the-internet-of-things-market-will-grow-2014-10?IR=T

Grewal, D., Monroe, K. B., & Krishnan, R. (1998). The effects of price-comparison advertising on buyers' perceptions of acquisition value, transaction value, and behavioral intentions. *The Journal of Marketing*, 46-59.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems, 29*(7), 1645-1660. doi:10.1016/j.future.2013.01.010

Hadlington, L. J. (2015). Cognitive failures in daily life: Exploring the link with Internet addiction and problematic mobile phone use. *Computers in Human Behavior, 51*, 75-81.

Hall, B. H., & Khan, B. (2003). Adoption of new technology. *UC Berkeley Working Papers Departent of Economics*.

Harris, L., & Westin, A. F. (1990). The Equifax Report on Consumers in the Information Age. *Atlanta, GA: Equifax Inc*.

Haws, K. L., & Bearden, W. O. (2006). Dynamic pricing and consumer fairness perceptions. *Journal of consumer research, 33*(3), 304-311.

Heidenreich, S., Kraemer, T., & Handrich, M. (2016). Satisfied and unwilling: Exploring cognitive and situational resistance to innovations. *Journal of Business Research, 69*(7), 2440-2447. doi:10.1016/j.jbusres.2016.01.014

Hérault, S., & Belvaux, B. (2014). Privacy paradox et adoption de technologies intrusives Le cas de la géolocalisation mobile/Privacy paradox and the adoption of intrusive technologies. The case of mobile location-based services. *Décisions Marketing*(74), 67.

Herbig, P. A., & Day, R. L. (1992). Customer acceptance: the key to successful introductions of innovations. *Marketing Intelligence & Planning, 10*(1), 4-15.

Herbig, P. A., & Kramer, H. (1994). The effect of information overload on the innovation choice process: Innovation overload. *Journal of Consumer Marketing, 11*(2), 45-54.

Herzenstein, M., Posavac, S. S., & Brakus, J. J. (2007). Adoption of new and really new products: The effects of self-regulation systems and risk salience. *Journal of marketing research, 44*(2), 251-260.

Hilgard, E. R., & Bower, G. H. (1975). *Theories of learning*.

Hill, T., Smith, N. D., & Mann, M. F. (1986). Communicating innovations: Convincing computer phobics to adopt innovative technologies. *ACR North American Advances*.

Hirschman, E. C. (1987). Adoption of an incredibly complex innovation: propositions from a humanistic vantage point. *ACR North American Advances*.

Hirunyawipada, T., & Paswan, A. K. (2006). Consumer innovativeness and perceived risk: implications for high technology product adoption. *Journal of Consumer Marketing*, *23*(4), 182-198. doi:10.1108/07363760610674310

Hoeffler, S. (2003). Measuring preferences for really new products. *Journal of marketing research, 40*(4), 406-420.

Hoffman, D. L., & Novak, T. (2015). Emergent experience and the connected consumer in the smart home assemblage and the internet of things. *The center of the connected consumer, the George Washington University School of Business*.

Hoffman, D. L., Novak, T. P., & Venkatesh, A. (2004). Has the Internet become indispensable? *Communications of the ACM, 47*(7), 37-42.

Hong, A., Nam, C., & Kim, S. (2017). Analysis of the barriers that consumers encounter when smart home service is introduced in South Korea.

Hoyer, W. D., & MacInnis, D. J. (1997). Consumer Behavior. Boston. *NY: Houghton Mifflin Company*.

Hsu, C. L., & Lin, J. C. C. (2016). An empirical examination of consumer adoption of Internet of Things services: Network externalities and concern for information privacy perspectives. *Computers in Human Behavior, 62*, 516-527. doi:10.1016/j.chb.2016.04.023

Hurter, J. A. P., & Rubenstein, A. H. (1978). Market penetration by new innovations: the technological literature. *Technological Forecasting and Social Change, 11*(3), 197-221.

IDC. (2014). Retrieved from http://www.zdnet.com/article/internet-of-things-market-to-hit-7-1-trillion-by-2020-idc/.Iimi

Inquiry, W. (1997). Financial System Inquiry Final Report. In: Canberra: Commonwealth of Australia.

Jacoby, J., & Kaplan, L. B. (1972). The components of perceived risk. *ACR Special Volumes*.

Janssens, W., De Pelsmacker, P., & Van Kenhove, P. (2008). *Marketing research with SPSS*: Pearson Education.

Jansson, J., Marell, A., & Nordlund, A. (2010). Green consumer behavior: determinants of curtailment and eco-innovation adoption. *Journal of Consumer Marketing, 27*(4), 358-370.

Jarvenpaa, S. L., Lang, K. R., Takeda, Y., & Tuunainen, V. K. (2003). Mobile commerce at crossroads. *Communications of the ACM, 46*(12), 41-44.

John, A., & Klein, J. (2003). The boycott puzzle: consumer motivations for purchase sacrifice. *Management Science, 49*(9), 1196-1209.

Johnson, C. A. (1974). Privacy as personal control. *Man-environment interactions: evaluations and applications: part, 2*, 83-100.

Kahneman, D., & Tversky, A. (1979). Prospect Theory: An Analysis of Decision under Risk. *Econometrica, 47*(2), 263-291.

Kang, Y., & Kim, S. (2009). Understanding user resistance to participation in multihop communications. *Journal of Computer-Mediated Communication, 14*(2), 328-351.

Kaplan, L. B., Szybillo, G. J., & Jacoby, J. (1974). Components of perceived risk in product purchase: A cross-validation. *Journal of applied psychology, 59*(3), 287.

Karahanna, E., & Limayem, M. (2000). E-mail and v-mail usage: Generalizing across technologies. *Journal of organizational computing and electronic commerce, 10*(1), 49-66.

Karahanna, E., Straub, D. W., & Chervany, N. L. (1999). Information technology adoption across time: a cross-sectional comparison of pre-adoption and post-adoption beliefs. *MIS quarterly*, 183-213.

Katz, M. L., & Shapiro, C. (1985). Network externalities, competition, and compatibility. *The American economic review, 75*(3), 424-440.

Kelvin, P. (1973). A social psychological examination of privacy. *British Journal of Clinical Psychology, 12*(3), 248-261.

Kim, H. W., Chan, H. C., & Gupta, S. (2007). Value-based adoption of mobile internet: an empirical investigation. *Decision support systems, 43*(1), 111-126.

Kleijnen, M., De Ruyter, K., & Wetzels, M. (2007). An assessment of value creation in mobile service delivery and the moderating role of time consciousness. *Journal of retailing, 83*(1), 33-46.

Kleijnen, M., Lee, N., & Wetzels, M. (2009). An exploration of consumer resistance to innovation and its antecedents. *Journal of Economic Psychology, 30*(3), 344-357.

Klerck, D., & Sweeney, J. C. (2007). The effect of knowledge types on consumer perceived risk and adoption of genetically modified foods. *Psychology & Marketing, 24*(2), 171-193.

Kolodinsky, J. M., Hogarth, J. M., & Hilgert, M. A. (2004). The adoption of electronic banking technologies by US consumers. *International Journal of Bank Marketing, 22*(4), 238-259. doi:10.1108/02652320410542536

Kuisma, T., Laukkanen, T., & Hiltunen, M. (2007). Mapping the reasons for resistance to Internet banking: A means-end approach. *International Journal of Information Management, 27*(2), 75-85.

Laroche, M., Yang, Z., McDougall, G. H. G., & Bergeron, J. (2005). Internet versus bricks-and-mortar retailers: An investigation into intangibility and its consequences. *Journal of retailing, 81*(4), 251-267.

Lassar, W. M., Manolis, C., & Lassar, S. S. (2005). The relationship between consumer innovativeness, personal characteristics, and online banking adoption. *International Journal of Bank Marketing, 23*(2), 176-199. doi:10.1108/02652320510584403

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*(7), 2432-2439. doi:10.1016/j.jbusres.2016.01.013

Laukkanen, T., & Lauronen, J. (2005). Consumer value creation in mobile banking services. *International journal of mobile Communications, 3*(4), 325-338.

Laukkanen, T., Sinkkonen, S., Kivijärvi, M., & Laukkanen, P. (2007). Innovation resistance among mature consumers. *Journal of Consumer Marketing, 24*(7), 419-427. doi:10.1108/07363760710834834

Lazar, A., Koehler, C., Tanenbaum, J., & Nguyen, D. H. (2015, 2015). *Why we use and abandon smart devices.* Paper presented at the In Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing

Lee, C. H., & Cranage, D. A. (2011). Personalisation–privacy paradox: The effects of personalisation and privacy assurance on customer responses to travel Web sites. *Tourism Management, 32*(5), 987-994.

Liao, Z., & Cheung, M. T. (2001). Internet-based e-shopping and consumer attitudes: an empirical study. *Information & Management, 38*(5), 299-306.

Licoppe, C., & Heurtin, J. P. (2001). Managing one's availability to telephone communication through mobile phones: A French case study of the development dynamics of mobile phone use. *Personal and Ubiquitous Computing, 5*(2), 99-108.

Lin, J.-S. C., & Hsieh, P.-L. (2007). The influence of technology readiness on satisfaction and behavioral intentions toward self-service technologies. *Computers in Human Behavior, 23*(3), 1597-1615.

Littler, D., & Melanthiou, D. (2006). Consumer perceptions of risk and uncertainty and the implications for behaviour towards innovative retail services: The case of Internet Banking. *Journal of Retailing and Consumer Services, 13*(6), 431-443. doi:10.1016/j.jretconser.2006.02.006

Lo, S.-K., Wang, C.-C., & Fang, W. (2005). Physical interpersonal relationships and social anxiety among online game players. *Cyberpsychology & behavior, 8*(1), 15-20.

Locander, W. B., & Hermann, P. W. (1979). The effect of self-confidence and anxiety on information seeking in consumer risk reduction. *Journal of marketing research*, 268-274.

López, T. S., Ranasinghe, D. C., Harrison, M., & McFarlane, D. (2011). Adding sense to the Internet of Things. *Personal and Ubiquitous Computing, 16*(3), 291-308. doi:10.1007/s00779-011-0399-8

Lu, H.-P., Hsu, C.-L., & Hsu, H.-Y. (2005). An empirical study of the effect of perceived risk upon intention to use online applications. *Information Management & Computer Security, 13*(2), 106-120.

Lu, J., Yao, J. E., & Yu, C.-S. (2005). Personal innovativeness, social influences and adoption of wireless Internet services via mobile technology. *The Journal of Strategic Information Systems, 14*(3), 245-268.

Madakam, S., Ramaswamy, R., & Tripathi, S. (2015). Internet of Things (IoT): A Literature Review. *Journal of Computer and Communications, 03*(05), 164-173. doi:10.4236/jcc.2015.35021

Malhotra, N. K. (2009). *Marketig Research. An applied orientation* (Vol. 6). New Jersey, USA.

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.

Malina, L., Hajny, J., Fujdiak, R., & Hosek, J. (2016). On perspective of security and privacy-preserving solutions in the internet of things. *Computer Networks, 102*, 83-95. doi:10.1016/j.comnet.2016.03.011

Mallat, N. (2007). Exploring consumer adoption of mobile payments–A qualitative study. *The Journal of Strategic Information Systems, 16*(4), 413-432.

Mani, Z., & Chouk, I. (2016). Drivers of consumers’ resistance to smart products. *Journal of Marketing Management, 33*(1-2), 76-97. doi:10.1080/0267257x.2016.1245212

Mano, H., & Oliver, R. L. (1993). Assessing the dimensionality and structure of the consumption experience: evaluation, feeling, and satisfaction. *Journal of consumer research, 20*(3), 451-466.

Manyika, J., Chui, M., Bisson, P., Woetzel, J., Dobbs, R., Bughin, J., & Aharon, D. (2015). *Unlocking the potential of the Internet of Things. McKinsey Global Institute*. Retrieved from https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world

Margulis, S. T. (1977). Conceptions of privacy: Current status and next steps. *Journal of Social Issues, 33*(3), 5-21.

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing, 81*(1), 36-58.

Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science, 45*(2), 135-155.

Martins, C., Oliveira, T., & Popovič, A. (2014). Understanding the Internet banking adoption: A unified theory of acceptance and use of technology and perceived risk application. *International Journal of Information Management, 34*(1), 1-13.

Mazhelis, O., Luoma, E., & Warma, H. (2012). Defining an internet-of-things ecosystem. In *Internet of Things, Smart Spaces, and Next Generation Networking* (pp. 1-14): Springer.

McPherson, M., Smith-Lovin, L., & Cook, J. M. (2001). Birds of a feather: Homophily in social networks. *Annual review of sociology, 27*(1), 415-444.

Meola, A. (2016). *What is the Internet of Things (IoT)?* Retrieved from http://www.businessinsider.com/internet-of-things-definition?IR=T

Meyers-Levy, J., & Peracchio, L. A. (1995). Understanding the effects of color: How the correspondence between available and required resources affects attitudes. *Journal of consumer research, 22*(2), 121-138.

Midgley, D. F., & Dowling, G. R. (1978). Innovativeness: The concept and its measurement. *Journal of consumer research, 4*(4), 229-242.

Miller, A. (1982). *Computers and Privacy*. Cambridge, MA: Oelgeschlager, Gunn, & Hain Publishers, Inc.

Milne, G. R. (1997). Consumer participation in mailing lists: A field experiment. *Journal of Public Policy & Marketing*, 298-309.

Milne, G. R., & Boza, M.-E. (1999). Trust and concern in consumers' perceptions of marketing information management practices. *Journal of Interactive Marketing, 13*(1), 5-24.

Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing, 18*(3), 15-29.

Milne, G. R., & Gordon, M. E. (1993). Direct mail privacy-efficiency trade-offs within an implied social contract framework. *Journal of Public Policy & Marketing*, 206-215.

Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad Hoc Networks, 10*(7), 1497-1516.

Mishra, D., Angappa Gunasekaran, D. N. D., Gunasekaran, A., Childe, S. J., Papadopoulos, T., Dubey, R., & Wamba, S. (2016). Vision, applications and future challenges of Internet of Things. *Industrial Management & Data Systems, 116*(7), 1331-1355. doi:10.1108/imds-11-2015-0478

Mitchell, V.-W., & Harris, G. (2005). The importance of consumers' perceived risk in retail strategy. *European Journal of Marketing, 39*(7/8), 821-837.

Morwitz, V. G., Greenleaf, E. A., & Johnson, E. J. (1998). Divide and prosper: consumers' reactions to partitioned prices. *Journal of marketing research*, 453-463.

Nakyung, K., & Kim, J. (2015). Domestic smart home market, Low-priced products than high-priced products. Retrieved from http://www.lgeri.com/report/view.do?idx=19046

Narayanan, K. (2017). Addressing The Challenges Facing IoT Adoption. *Microwave Journal I, ,60*(1), 110-118.

Nowak, G. J., & Phelps, J. (1995). Direct marketing and the use of individual-level consumer information: Determining how and when "privacy" matters. *Journal of Direct Marketing, 9*(3), 46-60.

NTIA, N. T. a. I. A. (2002). *A nation online: how Americans are expanding their use of the internet.* Washington D.C.

Nysveen, H., Pedersen, P. E., & Thorbjørnsen, H. (2005). Intentions to use mobile services: Antecedents and cross-service comparisons. *Journal of the Academy of Marketing Science, 33*(3), 330.

O'Brien, J. (2017). The reality of IoT adoption *Big Data Quarterly, 3*(1), 12-16.

Oreg, S. (2003). Resistance to change: developing an individual differences measure. *Journal of applied psychology, 88*(4), 680.

Parasuraman, A. (2000). Technology Readiness Index (TRI) a multiple-item scale to measure readiness to embrace new technologies. *Journal of Service Research, 2*(4), 307-320.

Park, Y., & Chen, J. V. (2007). Acceptance and adoption of the innovative use of smartphone. *Industrial Management & Data Systems, 107*(9), 1349-1365. doi:10.1108/02635570710834009

Peppers, D., Rogers, M., & Dorf, B. (1999). Is your company ready for one-to-one marketing. *Harvard Business Review, 77*(1), 151-160.

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing, 19*(1), 27-41.

Piwek, L., Ellis, D. A., Andrews, S., & Joinson, A. (2016). The rise of consumer health wearables: promises and barriers. *PLoS Medicine, 13*(2), e1001953.

Poo, B., & Dalziel, N. (2016). Consumer Perceptions Towards Radical Innovation: Autonomous Cars. In: British Academy of Management (BAM).

Porter, C. E., & Donthu, N. (2006). Using the technology acceptance model to explain how attitudes determine Internet usage: The role of perceived access barriers and demographics. *Journal of Business Research, 59*(9), 999-1007.

Porter, M. E., & Heppelmann, J. E. (2014). How smart, connected products are transforming competition. *Harvard Business Review, 92*(11), 64-88.

Press, G. (2014). Internet of Things by the numbers: Market estimates and forecasts. *Forbes, Forbes Media, Jersey City, NJ*.

Price, L. L., Feick, L. F., & Guskey, A. (1995). Everyday market helping behavior. *Journal of Public Policy & Marketing*, 255-266.

Ram, S. (1987). A model of innovation resistance. *ACR North American Advances*.

Ram, S. (1989). Successful innovation using strategies to reduce consumer resistance: An empirical test. *Journal of Product Innovation Management, 6*(1), 20-34.

Ram, S., & Sheth, J. N. (1989). Consumer resistance to innovations: the marketing problem and its solutions. *Journal of Consumer Marketing, 6*(2), 5-14.

Rifkin, J. (2014). *The zero marginal cost society: The internet of things, the collaborative commons, and the eclipse of capitalism*: St. Martin's Press.

Risselada, H., Verhoef, P. C., & Bijmolt, T. H. (2014). Dynamic effects of social influence and direct marketing on the adoption of high-technology products. *Journal of Marketing, 78*(2), 52-68.

Rogers, E. M. (1976). New product adoption and diffusion. *Journal of consumer research, 2*(4), 290-301.

Rogers, E. M. (2010). *Diffusion of innovations*: Simon and Schuster.

Rogers, E. M., & Shoemaker, F. F. (1971). Communication of Innovations; A Cross-Cultural Approach.

Rojas-Méndez, J. I., Parasuraman, A., & Papadopoulos, N. (2015). Consumers' Technology Readiness in a Developing Country: The Role of Demographics and Attitudes. In *Marketing in Transition: Scarcity, Globalism, & Sustainability* (pp. 2-2): Springer.

Rojas-Méndez, J. I., Parasuraman, A., & Papadopoulos, N. (2017). Demographics, attitudes, and technology readiness: A cross-cultural analysis and model validation. *Marketing Intelligence & Planning, 35*(1), 18-39.

Rokeach, M. (1973). *The nature of human values*: Free press.

Romani, S., Grappi, S., Bagozzi, R. P., & Barone, A. M. (2018). Domestic food practices: A study of food management behaviors and the role of food preparation planning in reducing waste. *Appetite, 121*, 215-227.

Roselius, T. (1971). Consumer rankings of risk reduction methods. *The Journal of Marketing*, 56-61.

Rosenberg, M., Confessore, N., & Cadwalladr, C. (2018). How Trump Consultants Exploited the Facebook Data of Millions. *The New York Times*

Russo, G., Marsigalia, B., Evangelista, F., Palmaccio, M., & Maggioni, M. (2015). Exploring regulations and scope of the Internet of Things in contemporary companies: a first literature analysis. *Journal of Innovation and Entrepreneurship, 4*(1). doi:10.1186/s13731-015-0025-5

Salami, E. A. (2017). An Analysis of the General Data Protection Regulation (EU) 2016/679.

Sathye, M. (1999). Adoption of Internet banking by Australian consumers: an empirical investigation. *International Journal of Bank Marketing, 17*(7), 324-334. doi:10.1108/02652329910305689

Schwartz, S. H. (1992). Universals in the content and structure of values: Theoretical advances and empirical tests in 20 countries. In *Advances in experimental social psychology* (Vol. 25, pp. 1-65): Elsevier.

Shapiro, C., & Varian, H. R. (1998). *Information rules: a strategic guide to the network economy*: Harvard Business Press.

Sheehan, K. B., & Hoy, M. G. (2000). Dimensions of privacy concern among online consumers. *Journal of Public Policy & Marketing, 19*(1), 62-73.

Sheth, J. N. (1981). Psychology of Innovation Resistance. The less developed concept (LDC) in diffusion research. *Research in Marketing*, 273-282.

Sheth, J. N., & Stellner, W. H. (1979). *Psychology of innovation resistance: The less developed concept (LDC) in diffusion research*: College of Commerce and Business Administration, University of Illinois at Urbana-Champaign Urbana-Champaign, IL.

Shils, E. (1966). Privacy: Its constitution and vicissitudes. *Law and Contemporary Problems, 31*(2), 281-306.

Shin, D.-H. (2010). The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. *Interacting with computers, 22*(5), 428-438.

Shu, Q., Tu, Q., & Wang, K. (2011). The impact of computer self-efficacy and technology dependence on computer-related technostress: A social cognitive theory perspective. *International Journal of Human-Computer Interaction, 27*(10), 923-939.

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks, 76*, 146-164. doi:10.1016/j.comnet.2014.11.008

Smith, D. C., & Park, C. W. (1992). The effects of brand extensions on market share and advertising efficiency. *Journal of marketing research, 29*(3), 296.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: measuring individuals' concerns about organizational practices. *MIS quarterly*, 167-196.

Stone, E. F., Gueutal, H. G., Gardner, D. G., & McClure, S. (1983). A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. *Journal of applied psychology, 68*(3), 459.

Stone, R. N., & Grønhaug, K. (1993). Perceived risk: Further considerations for the marketing discipline. *European Journal of Marketing, 27*(3), 39-50.

Strebel, J., O'Donnell, K., & Myers, J. G. (2004). Exploring the connection between frustration and consumer choice behavior in a dynamic decision environment. *Psychology & Marketing, 21*(12), 1059-1076.

Szmigin, I., & Foxall, G. (1998). Three forms of innovation resistance: the case of retail payment methods. *Technovation, 18*(6), 459-468.

Szmigin, I. T., & Bourne, H. (1999). Electronic cash: a qualitative assessment of its adoption. *International Journal of Bank Marketing, 17*(4), 192-203.

Talke, K., & Heidenreich, S. (2014). How to Overcome Pro-Change Bias: Incorporating Passive and Active Innovation Resistance in Innovation Decision Models. *Journal of Product Innovation Management, 31*(5), 894-907. doi:10.1111/jpim.12130

Tam, E.-C., Hui, K.-L., & Tan, B. (2002). What do they want? Motivating consumers to disclose personal information to internet businesses. *ICIS 2002 Proceedings*, 2.

Teo, T. S., & Pok, S. H. (2003). Adoption of WAP-enabled mobile phones among Internet users. *Omega, 31*(6), 483-498.

Thibaut, J. W., & Walker, L. (1975). *Procedural justice: A psychological analysis*: L. Erlbaum Associates.

Trope, Y., & Liberman, N. (2003). Temporal construal. *Psychological review, 110*(3), 403.

Van de Ven, A. H. (2007). *Engaged scholarship: A guide for organizational and social research*: Oxford University Press

Van den Bulte, C., & Wuyts, S. H. K. (2007). Social networks in marketing. *MSI Relevant Knowledge Series*.

Van Doorn, J., Mende, M., Noble, S. M., Hulland, J., Ostrom, A. L., Grewal, D., & Petersen, J. A. (2017). Domo arigato Mr. Roboto: Emergence of automated social presence in organizational frontlines and customers' service experiences. *Journal of Service Research, 20*(1), 43-58.

Van Heerde, H. J., Mela, C. F., & Manchanda, P. (2004). The dynamic effect of innovation on market structure. *Journal of marketing research, 41*(2), 166-183.

Venkatesh, V., & Davis, F. D. (1996). A model of the antecedents of perceived ease of use: Development and test. *Decision Sciences, 27*(3), 451-481.

Venkatraman, M. P., & Price, L. L. (1990). Differentiating between cognitive and sensory innovativeness: Concepts, measurement, and implications. *Journal of Business Research, 20*(4), 293-315.

Vermesan, O., Friess, P., Guillemin, P., Gusmeroli, S., Sundmaeker, H., Bassi, A., & Doody, P. (2011). Internet of things strategic research roadmap. *Internet of Things-Global Technological and Societal Trends, 1*, 9-52.

Voorhees, C. M., Brady, M. K., & Horowitz, D. M. (2006). A voice from the silent masses: an exploratory and comparative analysis of noncomplainers. *Journal of the Academy of Marketing Science, 34*(4), 514-527.

Voss, K. E., Spangenberg, E. R., & Grohmann, B. (2003). Measuring the hedonic and utilitarian dimensions of consumer attitude. *Journal of marketing research, 40*(3), 310-320.

Wang, G., Dou, W., & Zhou, N. (2008). Consumption attitudes and adoption of new consumer products: a contingency approach. *European Journal of Marketing, 42*(1/2), 238-254. doi:10.1108/03090560810840998

Weber, R. H. (2010). Internet of Things – New security and privacy challenges. *Computer Law & Security Review, 26*(1), 23-30. doi:10.1016/j.clsr.2009.11.008

Weil, M. M., & Rosen, L. D. (1997). *Technostress: Coping with technology@ work@ home@ play*: Wiley New York.

Weinberg, B. D., Milne, G. R., Andonova, Y. G., & Hajjat, F. M. (2015). Internet of Things: Convenience vs. privacy and secrecy. *Business Horizons, 58*(6), 615-624. doi:10.1016/j.bushor.2015.06.005

Wells, J. D., Campbell, D. E., Valacich, J. S., & Featherman, M. (2010). The effect of perceived novelty on the adoption of information technology innovations: a risk/reward perspective. *Decision Sciences, 41*(4), 813-843.

Westin, A. F. (1967). Privacy and freedom, atheneum. *New York, 7*.

Whitmore, A., Agarwal, A., & Da Xu, L. (2014). The Internet of Things—A survey of topics and trends. *Information Systems Frontiers, 17*(2), 261-274. doi:10.1007/s10796-014-9489-2

Wood, S. L., & Moreau, C. P. (2006). From fear to loathing? How emotion influences the evaluation and early use of innovations. *Journal of Marketing, 70*(3), 44-57.

Wuenderlich, N. V., Heinonen, K., Ostrom, A. L., Patricio, L., Sousa, R., Voss, C., & Lemmink, J. G. (2015). “Futurizing” smart service: implications for service researchers and managers. *Journal of Services Marketing, 29*(6/7), 442-447.

Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2008). Examining the formation of individual's privacy concerns: Toward an integrative view. *ICIS 2008 proceedings*, 6.

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.

Xu, S., Fang, X., Chan, S., & Brzezinski, J. (2013). What tasks are suitable for handheld devices? . *Proceedings of HCI international 2003, human computer interaction: Theory and practice, 2,* 333-337.

Xu, Y., Tan, B., & Hui, K.-L. (2003). Consumer trust and online information privacy. *ICIS 2003 Proceedings*, 45.

Yang, Y., Liu, Y., Li, H., & Yu, B. (2015). Understanding perceived risks in mobile payment acceptance. *Industrial Management & Data Systems, 115*(2), 253-269.

Ziegeldorf, J. H., Morchon, O. G., & Wehrle, K. (2014). Privacy in the Internet of Things: threats and challenges. *Security and Communication Networks*, *7*(12), 2728-2742. doi:10.1002/sec.795